

# Privacy Protection and Incentive for AI-Driven IoT

Lead Guest Editor: Zhuojun Duan

Guest Editors: Yingjie Wang, Yaguang Lin, and Donghyun Kim





---

# **Privacy Protection and Incentive for AI-Driven IoT**



Wireless Communications and Mobile Computing

---

## **Privacy Protection and Incentive for AI-Driven IoT**

Lead Guest Editor: Zhuojun Duan

Guest Editors: Yingjie Wang, Yaguang Lin, and  
Donghyun Kim




---




Copyright © 2021 Hindawi Limited. All rights reserved.

This is a special issue published in “Wireless Communications and Mobile Computing.” All articles are open access articles distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

# Chief Editor

Zhipeng Cai , USA

## Associate Editors

Ke Guan , China  
Jaime Lloret , Spain  
Maode Ma , Singapore

## Academic Editors

Muhammad Inam Abbasi, Malaysia  
Ghufran Ahmed , Pakistan  
Hamza Mohammed Ridha Al-Khafaji ,  
Iraq  
Abdullah Alamoodi , Malaysia  
Marica Amadeo, Italy  
Sandhya Aneja, USA  
Mohd Dilshad Ansari, India  
Eva Antonino-Daviu , Spain  
Mehmet Emin Aydin, United Kingdom  
Parameshchhari B. D. , India  
Kalapaveen Bagadi , India  
Ashish Bagwari , India  
Dr. Abdul Basit , Pakistan  
Alessandro Bazzi , Italy  
Zdenek Becvar , Czech Republic  
Nabil Benamar , Morocco  
Olivier Berder, France  
Petros S. Bithas, Greece  
Dario Bruneo , Italy  
Jun Cai, Canada  
Xuesong Cai, Denmark  
Gerardo Canfora , Italy  
Rolando Carrasco, United Kingdom  
Vicente Casares-Giner , Spain  
Brijesh Chaurasia, India  
Lin Chen , France  
Xianfu Chen , Finland  
Hui Cheng , United Kingdom  
Hsin-Hung Cho, Taiwan  
Ernestina Cianca , Italy  
Marta Cimitile , Italy  
Riccardo Colella , Italy  
Mario Collotta , Italy  
Massimo Condoluci , Sweden  
Antonino Crivello , Italy  
Antonio De Domenico , France  
Floriano De Rango , Italy

Antonio De la Oliva , Spain  
Margot Deruyck, Belgium  
Liang Dong , USA  
Praveen Kumar Donta, Austria  
Zhuojun Duan, USA  
Mohammed El-Hajjar , United Kingdom  
Oscar Esparza , Spain  
Maria Fazio , Italy  
Mauro Femminella , Italy  
Manuel Fernandez-Veiga , Spain  
Gianluigi Ferrari , Italy  
Luca Foschini , Italy  
Alexandros G. Fragkiadakis , Greece  
Ivan Ganchev , Bulgaria  
Óscar García, Spain  
Manuel García Sánchez , Spain  
L. J. García Villalba , Spain  
Miguel Garcia-Pineda , Spain  
Piedad Garrido , Spain  
Michele Girolami, Italy  
Mariusz Glabowski , Poland  
Carles Gomez , Spain  
Antonio Guerrieri , Italy  
Barbara Guidi , Italy  
Rami Hamdi, Qatar  
Tao Han, USA  
Sherief Hashima , Egypt  
Mahmoud Hassaballah , Egypt  
Yejun He , China  
Yixin He, China  
Andrej Hrovat , Slovenia  
Chunqiang Hu , China  
Xuexian Hu , China  
Zhenghua Huang , China  
Xiaohong Jiang , Japan  
Vicente Julian , Spain  
Rajesh Kaluri , India  
Dimitrios Katsaros, Greece  
Muhammad Asghar Khan, Pakistan  
Rahim Khan , Pakistan  
Ahmed Khattab, Egypt  
Hasan Ali Khattak, Pakistan  
Mario Kolberg , United Kingdom  
Meet Kumari, India  
Wen-Cheng Lai , Taiwan



Jose M. Lanza-Gutierrez, Spain  
Pavlos I. Lazaridis , United Kingdom  
Kim-Hung Le , Vietnam  
Tuan Anh Le , United Kingdom  
Xianfu Lei, China  
Jianfeng Li , China  
Xiangxue Li , China  
Yaguang Lin , China  
Zhi Lin , China  
Liu Liu , China  
Mingqian Liu , China  
Zhi Liu, Japan  
Miguel López-Benítez , United Kingdom  
Chuanwen Luo , China  
Lu Lv, China  
Basem M. ElHalawany , Egypt  
Imadeldin Mahgoub , USA  
Rajesh Manoharan , India  
Davide Mattera , Italy  
Michael McGuire , Canada  
Weizhi Meng , Denmark  
Klaus Moessner , United Kingdom  
Simone Morosi , Italy  
Amrit Mukherjee, Czech Republic  
Shahid Mumtaz , Portugal  
Giovanni Nardini , Italy  
Tuan M. Nguyen , Vietnam  
Petros Nicolitidis , Greece  
Rajendran Parthiban , Malaysia  
Giovanni Pau , Italy  
Matteo Petracca , Italy  
Marco Picone , Italy  
Daniele Pinchera , Italy  
Giuseppe Piro , Italy  
Javier Prieto , Spain  
Umair Rafique, Finland  
Maheswar Rajagopal , India  
Sujan Rajbhandari , United Kingdom  
Rajib Rana, Australia  
Luca Reggiani , Italy  
Daniel G. Reina , Spain  
Bo Rong , Canada  
Mangal Sain , Republic of Korea  
Praneet Saurabh , India

Hans Schotten, Germany  
Patrick Seeling , USA  
Muhammad Shafiq , China  
Zaffar Ahmed Shaikh , Pakistan  
Vishal Sharma , United Kingdom  
Kaize Shi , Australia  
Chakchai So-In, Thailand  
Enrique Stevens-Navarro , Mexico  
Sangeetha Subbaraj , India  
Tien-Wen Sung, Taiwan  
Suhua Tang , Japan  
Pan Tang , China  
Pierre-Martin Tardif , Canada  
Sreenath Reddy Thummaluru, India  
Tran Trung Duy , Vietnam  
Fan-Hsun Tseng, Taiwan  
S Velliangiri , India  
Quoc-Tuan Vien , United Kingdom  
Enrico M. Vitucci , Italy  
Shaohua Wan , China  
Dawei Wang, China  
Huaqun Wang , China  
Pengfei Wang , China  
Dapeng Wu , China  
Huaming Wu , China  
Ding Xu , China  
YAN YAO , China  
Jie Yang, USA  
Long Yang , China  
Qiang Ye , Canada  
Changyan Yi , China  
Ya-Ju Yu , Taiwan  
Marat V. Yuldashev , Finland  
Sherali Zeadally, USA  
Hong-Hai Zhang, USA  
Jiliang Zhang, China  
Lei Zhang, Spain  
Wence Zhang , China  
Yushu Zhang, China  
Kechen Zheng, China  
Fuhui Zhou , USA  
Meiling Zhu, United Kingdom  
Zhengyu Zhu , China



# Contents

## **An Efficient Network Security Situation Assessment Method Based on AE and PMU**

Xiao-ling Tao , Zi-yi Liu , and Chang-song Yang 




Research Article (9 pages), Article ID 1173065, Volume 2021 (2021)

## **Network Threat Detection Based on Group CNN for Privacy Protection**

Yanping Xu , Xia Zhang, Chengdan Lu , Zhenliang Qiu, Chunfang Bi, Yuping Lai, Jian Qiu, and Hua Zhang

Research Article (18 pages), Article ID 3697536, Volume 2021 (2021)

## **Blockchain-Based Privacy Protection Scheme for IoT-Assisted Educational Big Data Management**

Xiaoshuang He , Hechuan Guo , and Xueyu Cheng 



Research Article (11 pages), Article ID 3558972, Volume 2021 (2021)

## **A Framework to Test Resistency of Detection Algorithms for Stepping-Stone Intrusion on Time-Jittering Manipulation**

Lixin Wang , Jianhua Yang, Michael Workman, and Peng-Jun Wan



Research Article (8 pages), Article ID 1807509, Volume 2021 (2021)

## **Aspect-Level Sentiment Analysis Approach via BERT and Aspect Feature Location Model**

Guangyao Pang , Keda Lu, Xiaoying Zhu, Jie He, Zhiyi Mo, Zizhen Peng , and Baoxing Pu

Research Article (13 pages), Article ID 5534615, Volume 2021 (2021)

## **Temporal Index Scheme of Hyperledger Fabric System in IoT**

Yongqiang Lu , Zhaobin Liu , Shaoqi Wang, Zhiyang Li, Weijiang Liu, and Xuhui Chen


Research Article (15 pages), Article ID 9945530, Volume 2021 (2021)

## **A Face Occlusion Removal and Privacy Protection Method for IoT Devices Based on Generative Adversarial Networks**

Wenqiu Zhu, Xiaoyi Wang, Yuezhong Wu , and Guang Zou

Research Article (14 pages), Article ID 6948293, Volume 2021 (2021)

## **A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection**

Yingwen Chen, Linghang Meng, Huan Zhou , and Guangtao Xue







Research Article (12 pages), Article ID 6685762, Volume 2021 (2021)

## **AI-Driven Multiobjective Scheduling Algorithm of Flood Control Materials Based on Pareto Artificial Bee Colony**

Banteng Liu , Junjie Lu, Yourong Chen, Ping Sun, Kehua Zhao, Meng Han , Rengong Zhang, and Zegao Yin




Research Article (15 pages), Article ID 5557543, Volume 2021 (2021)

## **Multiscale Anchor-Free Region Proposal Network for Pedestrian Detection**


Zhiwei Cao , Huihua Yang , Weijin Xu , Juan Zhao , Lingqiao Li , and Xipeng Pan 

Research Article (12 pages), Article ID 5590895, Volume 2021 (2021)

**Traceable Multiauthority Attribute-Based Encryption with Outsourced Decryption and Hidden Policy for CIoT**

Suhui Liu , Jiguo Yu , Chunqiang Hu , and Mengmeng Li  
Research Article (16 pages), Article ID 6682580, Volume 2021 (2021)

**Participant Recruitment Method Aiming at Service Quality in Mobile Crowd Sensing**

Weijin Jiang, Junpeng Chen , Xiaoliang Liu, Yuehua Liu, and Sijian Lv  
Research Article (14 pages), Article ID 6621659, Volume 2021 (2021)


**Anti-Attack Scheme for Edge Devices Based on Deep Reinforcement Learning**

Rui Zhang , Hui Xia , Chao Liu , Ruo-bing Jiang , and Xiang-guo Cheng   
Research Article (9 pages), Article ID 6619715, Volume 2021 (2021)

**A Hybrid Alarm Association Method Based on AP Clustering and Causality**

Xiao-ling Tao , Lan Shi , Feng Zhao , Shen Lu , and Yang Peng   
Research Article (10 pages), Article ID 5576504, Volume 2021 (2021)


**D-(DP)<sup>2</sup>SGD: Decentralized Parallel SGD with Differential Privacy in Dynamic Networks**

Yuan Yuan, Zongrui Zou, Dong Li, Li Yan, and Dongxiao Yu   
Research Article (14 pages), Article ID 6679453, Volume 2021 (2021)




**A High-Quality Authenticatable Visual Secret Sharing Scheme Using SGX**

Denghui Zhang  and Zhaoquan Gu   
Research Article (12 pages), Article ID 6660709, Volume 2021 (2021)






**Certificateless-Based Anonymous Authentication and Aggregate Signature Scheme for Vehicular Ad Hoc Networks**

Xin Ye , Gencheng Xu , Xueli Cheng , Yuedi Li , and Zhiguang Qin  
Research Article (16 pages), Article ID 6677137, Volume 2021 (2021)




**Dynamic Network Security Mechanism Based on Trust Management in Wireless Sensor Networks**

Guiping Zheng , Bei Gong , and Yu Zhang   
Research Article (10 pages), Article ID 6667100, Volume 2021 (2021)

**BSSPD: A Blockchain-Based Security Sharing Scheme for Personal Data with Fine-Grained Access Control**

Hongmin Gao , Zhaofeng Ma , Shoushan Luo , Yanping Xu , and Zheng Wu   
Research Article (20 pages), Article ID 6658920, Volume 2021 (2021)

**Trustworthy Jammer Selection with Truth-Telling for Wireless Cooperative Systems**

Yingkun Wen , Tao Jing , and Qinghe Gao   
Research Article (17 pages), Article ID 6626355, Volume 2021 (2021)



# Contents

---





## **Histogram Publication over Numerical Values under Local Differential Privacy**

Xu Zheng , Ke Yan , Jingyuan Duan, Wenyi Tang, and Ling Tian  
Research Article (11 pages), Article ID 8886255, Volume 2021 (2021)


## **A Transaction Trade-Off Utility Function Approach for Predicting the End-Price of Online Auctions in IoT**

Xiaohui Li  and Hongbin Dong   
Research Article (10 pages), Article ID 6656421, Volume 2021 (2021)


## **On Constructing $t$ -Spanner in IoT under SINR**

Xiujuan Zhang , Yongcai Wang , Wenping Chen, Yuqing Zhu, Deying Li , and Guangshun Li   
Research Article (13 pages), Article ID 6643810, Volume 2021 (2021)





## **A Survey of Cooperative Jamming-Based Secure Transmission for Energy-Limited Systems**

Yuandong Wu and Yan Huo   
Research Article (11 pages), Article ID 6638405, Volume 2021 (2021)

## **Emotional Dialogue Generation Based on Conditional Variational Autoencoder and Dual Emotion Framework**

Zhenrong Deng, Hongquan Lin, Wenming Huang , Rushi Lan, and Xiaonan Luo  
Research Article (10 pages), Article ID 8881616, Volume 2020 (2020)

## **Service Recommendation with High Accuracy and Diversity**

Shengqi Wu , Huaizhen Kou , Chao Lv, Wanli Huang , Lianyong Qi, and Hao Wang   
Research Article (10 pages), Article ID 8822992, Volume 2020 (2020)

## Research Article

# An Efficient Network Security Situation Assessment Method Based on AE and PMU

Xiao-ling Tao <sup>1,2</sup>, Zi-yi Liu <sup>1,2</sup> and Chang-song Yang <sup>1,2</sup>

<sup>1</sup>Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin 541004, China

<sup>2</sup>Guangxi Cooperative Innovation Centre of Cloud Computing and Big Data, Guilin University of Electronic Technology, Guilin 541004, China

Correspondence should be addressed to Chang-song Yang; [csyang@guet.edu.cn](mailto:csyang@guet.edu.cn)

Received 22 June 2021; Accepted 23 August 2021; Published 13 September 2021

Academic Editor: Zhuojun Duan

Copyright © 2021 Xiao-ling Tao et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Network security situation assessment (NSSA) is an important and effective active defense technology in the field of network security situation awareness. By analyzing the historical network security situation awareness data, NSSA can evaluate the network security threat and analyze the network attack stage, thus fully grasping the overall network security situation. With the rapid development of 5G, cloud computing, and Internet of things, the network environment is increasingly complex, resulting in diversity and randomness of network threats, which directly determine the accuracy and the universality of NSSA methods. Meanwhile, the indicator data is characterized by large scale and heterogeneity, which seriously affect the efficiency of the NSSA methods. In this paper, we design a new NSSA method based on the autoencoder (AE) and parsimonious memory unit (PMU). In our novel method, we first utilize an AE-based data dimensionality reduction method to process the original indicator data, thus effectively removing the redundant part of the indicator data. Subsequently, we adopt a PMU deep neural network to achieve accurate and efficient NSSA. The experimental results demonstrate that the accuracy and efficiency of our novel method are both greatly improved.

## 1. Introduction

Network security situation assessment (NSSA) technology is one of the most effective active defense technologies to evaluate the threats of network security, by which the network administrators not only can comprehensively understand the security risk situation but also can understand the security threats which are faced by the current network and information system. Hence, the network administrators can manage the dynamic network security situation and judge the development trend of the network security situation [1, 2]. As a result, NSSA attracts increasing attention.

Nowadays, plenty of NSSA methods have been proposed, while there still exist many inherent deficiencies in the existing methods, resulting in a lot of severe challenges that need to be solved solidly. Firstly, most of the existing

NSSA methods pay too much attention to subjective judgment and prior knowledge. Meanwhile, they ignore plenty of other external factors and the time sequence property of the indicator data. As a result, they are not suitable for the long-term assessment over the network security situation. Secondly, the existing NSSA methods are not efficiency attractive. Specifically, the current indicator data is characterized by large scale, multifeature, heterogeneity, high dimensionality, and nonlinearity. Hence, the existing NSSA methods need to pay very expensive computational overhead to process these indicator data before evaluating the network security situation. Last but not least, some existing NSSA methods only consider part of the network security threats and attacks. However, the current network threats and attacks are characterized by diversity and randomness, resulting in very low accuracy in some existing methods.

Therefore, how to design a novel method to effectively and accurately achieve NSSA has become one of the most important problems in the field of network security.

*1.1. Contributions.* We study an essential but challenging problem in this paper, i.e., accurate and efficient NSSA in large-scale network environment. Then, we design a novel NSSA method based on the autoencoder (AE) and parsimonious memory unit (PMU), which can efficiently and accurately achieve NSSA. Therefore, the main contributions of this paper can be described as the following two aspects.

- (1) In the current large-scale network environment, the indicator data is characterized by heterogeneity, large scale, multifeature, high dimensionality, and nonlinearity. Therefore, we design an AE-based data dimensionality reduction method to process the original indicator data, thus reducing the dimensions of the indicator data. Subsequently, we can efficiently extract the situation assessment elements on the premise of guaranteeing the integrity of the data features
- (2) We adopt PMU to design a novel NSSA method for the current large-scale network environment, in which PMU is utilized for feature representation and time-varying learning of situation assessment elements. Meanwhile, we offer the theoretical computational complexity comparison. Finally, we implement our novel method and provide the performance evaluation, which can intuitively demonstrate the high efficiency and accuracy of our novel method

*1.2. Related Work.* NSSA has been extensively studied in both academia and industry, resulting in a rich body of solutions. Generally speaking, the existing NSSA methods can be summarized into three categories: mathematical statistics-based assessment method, knowledge reasoning-based assessment method [3], and machine learning-based assessment method [4, 5].

Wang et al. [6] designed a hierarchical NSSA method based on an analytic hierarchy process (AHP), which used the hierarchical cyber threat situation assessment (CSA) indicator system constructed by AHP to decide the network threat weight values. Wang et al. [7] proposed an AHP-based NSSA and quantification method, which utilized the AHP and hierarchical situation assessment model to simplify the NSSA problem. Li et al. [8] adopted fuzzy optimal clustering criteria combined with  $c$ -means clustering to process the indicator data, thus getting the number of clusters and the optimal clustering center. Then, they got the final NSSA results by utilizing AHP to construct an assessment model. Zhang et al. [9] presented a distributed denial of service (DDoS) attack NSSA model based on fuzzy clustering algorithm fusion features, which can effectively evaluate the security status of DDoS attack. Although the above methods can effectively implement NSSA, they not only need a lot of subjective judgments but also are not conducive to long-term assessment.

Yi et al. [10] designed a NSSA method based on fuzzy theory. Their method used fuzzy theory to weaken the index factors with low credibility and eliminate the uncertainty, thus making the assessment results more accurate. Liu et al. [11] utilized D-S evidence theory to fuse the measured indexes for obtaining the device threat value. Then, they utilized AHP to calculate the weights for different devices and finally obtained the network threat situation value by the weighting method. Codetta-Raiteri et al. [12] designed a NSSA method based on decision networks (DN), which can achieve a reasonable tradeoff between computational complexity and analysis efficiency. To quantitatively assess the network security risk, Wang et al. [13] designed a NSSA model based on the Bayesian approach. Fan et al. [14] presented a security evaluation method based on a software-defined network (SDN), which used multiple observation hidden Markov model (HMM) to obtain the security evaluation value of SDN, by quantifying the network state. To more completely describe the network security situation, Liao et al. [15] designed a NSSA method based on the extended HMM. Although the above knowledge reasoning-based methods can improve the NSSA accuracy, they rely on too much prior knowledge and have no advantages in efficiency.

Nowadays, the support vector machine (SVM) [16] and neural network [17, 18] are also widely used in NSSA. Chen et al. [19] adopted the SVM and gravitational search algorithm (GSA) to design a NSSA method, which has a better global optimization function. Qiang et al. [20] utilized an optimized cuckoo search back propagation neural network (BPNN) to design a new NSSA method. In their method, they used a cuckoo search (CS) algorithm based on conjugate gradient to optimize the initial parameters of BPNN and increase the training efficiency of the neural network. Shi and Chen [21] utilized a dual-SVM model for data learning and parameter estimation in command information system security situation samples, thus evaluating the command information system security situation. Gao et al. [22] designed the SVM information system security risk assessment model, which was optimized by an artificial fish swarm algorithm (AFSA). In their method, the AFSA was used to optimize the SVM, resulting in great accuracy and fast convergence. Han et al. [23] adopted convolutional neural networks (CNN) to design a quantitative network security situation evaluation method for an intelligent robot cluster under the wireless connection. Yang et al. [24] adopted a deep autoencoder (DAE) and deep neural networks (DNN) to study NSSA. Subsequently, they designed a new method to improve the network attack identification accuracy and the NSSA flexibility. Although the above methods can improve the accuracy, they cannot learn the correlation of time series. Therefore, they cannot be suitable for the NSSA over the indicator data which is characterized by the time sequence.

*1.3. Organization.* The rest of the structure of this paper is as follows. In Section 2, we describe the AE and PMU. In Section 3, we adopt AE and PMU to propose a novel NSSA method. Then, we implement the proposed method and



provide the experiment results in Section 4. Finally, we simply summarize this paper in Section 5.

## 2. Preliminaries

**2.1. Autoencoder.** An autoencoder (AE) [25, 26] is a common unsupervised learning algorithm, which utilizes the original input data as a reference for self-supervised learning to reduce dimension. AE generates information elements with more obvious features and lower dimensions than the original data element. AE maps the original data to the encoding layer to achieve encoding, then maps the encoded data to the decoding layer for decoding, and takes the final decoded data as the output data (see Figure 1).

We utilize  $X = [X_1, X_2, \dots, X_l]^T \in R^{l \times 1}$  and  $W_e = [W_e^{(1)}, W_e^{(2)}, \dots, W_e^{(n)}]^T \in R^{n \times 1}$  to represent the input data and the weight of the encoder, respectively. At the same time, we denote by  $h_e = [h_e^{(1)}, h_e^{(2)}, \dots, h_e^{(n)}]^T \in R^{n \times 1}$  the output of the encoding layer. Then, we could utilize  $W_d = [W_d^{(1)}, W_d^{(2)}, \dots, W_d^{(n)}]^T \in R^{n \times 1}$  to represent the weight of the decoder. The output result can be expressed as  $X' = [X'_1, X'_2, \dots, X'_l]^T \in R^{l \times 1}$ , where  $l$  represents the data dimensions. Note that the AE requires that the final input result is almost equal to the output result, that is,  $X = X'$ .

The encoding process of the AE can be expressed as follows:

$$h_e = f^e(W_e X + b^e), \quad (1)$$

where the bias of the encoding part can be represented as  $b^e$  and the activation function of the encoding part can be represented as  $f^e$ .

The decoding process of the AE decoding layer can be expressed as follows:

$$X' = f^d(W_d h_e + b^d), \quad (2)$$

where the bias of the decoding part can be represented as  $b^d$  and the activation function of the decoding part can be represented as  $f^d$ .

The MSE loss function is usually used in AE training, and it can be expressed as

$$L(X, X') = \frac{1}{2k} \sum_{j=1}^k (X_j - X'_j)^2, \quad (3)$$

where  $X$  represents the input variable,  $X'$  represents the output variable,  $L(X, X')$  represents the loss function, and  $k$  represents the number of samples.

**2.2. Parsimonious Memory Unit.** A parsimonious memory unit (PMU) is a new recurrent neural network, which can be viewed as an improved version of a gated recurrent unit (GRU) [27]. PMU is characterized by better managing the latent relations between short- and long-term dependencies

[28]. Note that there are two gate structures in the GRU model, i.e., reset gate and update gate. However, there is only one gate structure in PMU, i.e., unit gate, as seen in Figure 2. Specifically, PMU integrates the update gate and the reset gate of GRU into a new unit gate, resulting in fewer parameters in PMU. Moreover, due to the fact that the PMU can better manage the latent relations between short- and long-term dependencies, PMU has better convergence and speed in training.

In Figure 2, we utilize  $U_t$  to represent the unit gate, which is used to control the learning of long-term correlation and short-term correlation of the data. When  $U_t$  is 1, PMU learns the long-term dependence of the data, while when  $U_t$  is 0, PMU learns the short-term dependence of the data. The learning mode of PMU can be described as follows.

Firstly, the state of the unit gate is obtained by the evaluation state  $h_{t-1}$  transmitted from the previous node and the input  $x_t$  of the current node:

$$U_t = \sigma(W_u \bullet [h_{t-1}, x_t]). \quad (4)$$

Secondly, the state of the current time memorized on the current candidate set  $\tilde{h}_t$  can be expressed as

$$\tilde{h}_t = \tanh(W_{\tilde{h}} \bullet [U_t \times h_{t-1}, x_t]). \quad (5)$$

Thirdly, in the stage of updating memory, PMU updates  $h_t$  through the following formula:

$$h_t = (1 - U_t) \times h_{t-1} + \tilde{h}_t. \quad (6)$$

Finally, the output of forward propagation is

$$y_t = \text{softmax}(W_o \bullet h_t). \quad (7)$$

In the forward propagation process of PMU, we need to learn the following three parameters:  $W_u$ ,  $W_{\tilde{h}}$ , and  $W_o$ , where

$$\begin{aligned} W_u &= W_{ux} + W_{uh}, \\ W_{\tilde{h}} &= W_{\tilde{h}x} + W_{\tilde{h}h}, \\ W_o &= W_o. \end{aligned} \quad (8)$$

Then, the output  $y_t$  is the network domain security situation score value.

## 3. Method

In this section, we initially describe the system structure. Then, we introduce our AE-PMU-based NSSA method in detail.

**3.1. System Structure.** With the rapid development of modern network technology, the complexity of the current network environment is continuously increasing. In particular, with the development of cloud computing [29–31] and

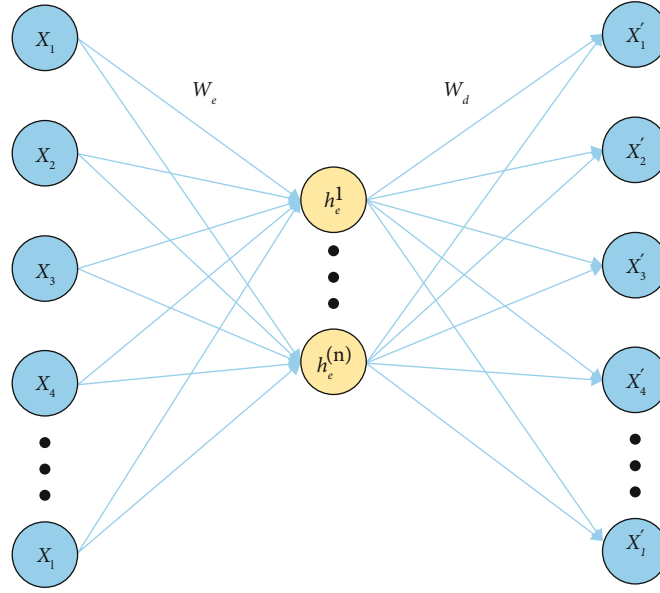


FIGURE 1: Basic structure of AE.

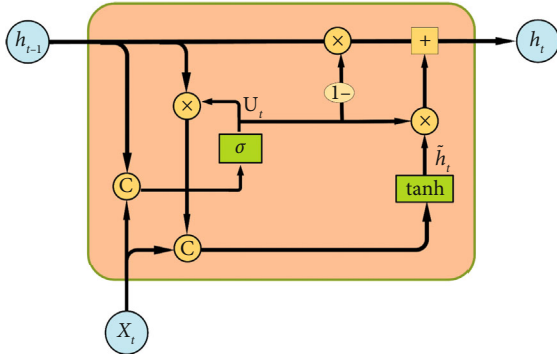


FIGURE 2: The construction of PMU.

Internet of things [32, 33], the modern network is characterized by new features, such as dynamic virtualized management methods and multilevel service models. As a result, the network threats have the characteristics of diversity and randomness. Meanwhile, the indicator data is large-scale and has heterogeneity, resulting in plenty of new problems in NSSA. Specifically, the large volume of indicator data seriously affects the efficiency of the assessment method. Moreover, the diversity and randomness of network threats directly determine the accuracy and the universality of the assessment method. To handle the above challenges, we propose a novel NSSA method (as seen in Figure 3), which is mainly composed of AE-based data dimensionality reduction and PMU-based assessment method. Specifically, we first adopt AE to process the original indicator data to achieve data dimension reduction. Then, we extract the situation assessment elements efficiently. By taking AE, our method can greatly improve the efficiency and reduce the data loss. Then, we adopt PMU to design an efficient NSSA method. Compared with other deep neural networks (e.g., GRU), PMU is more suitable for managing the latent rela-

tions between short- and long-term dependencies. Meanwhile, our PMU-based assessment method is more efficient than the GRU-based assessment method.

**3.2. AE-PMU-Based NSSA Method.** In this part, we provide the detailed description of our proposed AE-PMU-based NSSA method. The algorithm pseudocode is shown in Algorithm 1.

As described in Algorithm 1,  $M$  represents the dimension of data dimensionality reduction,  $n$  represents the training period, and  $C$  represents the situation value after the evaluation of the test set. The main processes are as follows.

- (1) Initialize the data dimension reduction dimension  $M$  and the number of training period  $n$
- (2) Use AE to extract the situation assessment elements from the initialized overall indicator dataset to achieve data dimensionality reduction
- (3) Input the situation assessment elements of the training set into the PMU-based NSSA training model to implement the model training
- (4) Input the situation assessment elements of the testing set into the PMU-based NSSA model to get the situation value  $C$

## 4. Time Complexity Analysis and Experiment

We initially analyze the time complexity in this section. Then, we implement our AE-PMU-based NSSA method and provide the experimental results, including the precision, the efficiency, and the fit between the assessed indicator value and the real indicator value.

**4.1. Time Complexity Analysis.** Time complexity is a significant index to judge the merits of the algorithm. We will

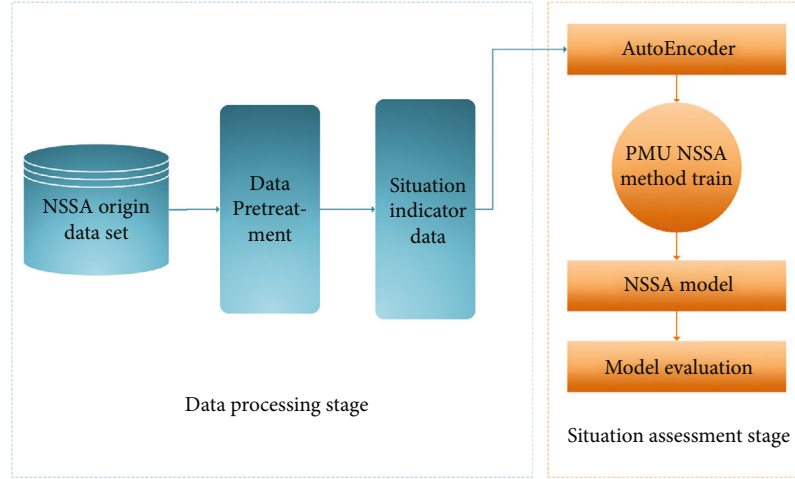


FIGURE 3: The system model.

**Input:** X-train dataset, Y-test dataset, Real-label, M-dimension, n-number of epoch.  
**Output:** evaluation results.

```

1 Initialize the size of M and n.
2  $X \leftarrow \text{AutoEncoder}(X\text{-train}, M)$ 
3  $Y \leftarrow \text{AutoEncoder}(Y\text{-test}, M)$ 
4 for  $i = 0$  to  $n$  do
5    $PMU_i \leftarrow PMU_i(X)$ 
6 end for
7  $C \leftarrow PMU(Y)$ 
8 return result  $\leftarrow C$ 

```

ALGORITHM 1: AE-PMU-based NSSA method.

analyze and compare the forward propagation time complexity of the GRU-based NSSA method and the PMU-based NSSA method.

We can assume that the dimension of the data input is  $m$  and the number of PMU hidden units is  $n$ . Firstly, according to formula (4), the number of operations for  $U_t$  can be represented as  $T(n \times m + n^2 + n)$ . Secondly, according to formula (5), the number of operations for calculating the current state candidate set is  $T(n \times m + 2 \times n^2 + n)$ . Thirdly, according to formula (6), the number of operations in the memory update phase is  $T(n^2 + 2 \times n)$ . Finally, the total number of operations of PMU is  $T(2 \times n \times m + 4 \times n^2 + 4 \times n)$ . Overall, the time complexity is  $O(n^2)$ .

Compared with PMU, GRU has one more gate structure, which has the same number of operations as the  $U_t$  gate of PMU. In addition, the memory update phase of the GRU is different from that of PMU. GRU uses  $Z_t$  to control whether the candidate set state is added to the memory update phase in this state. Therefore, the number of operations in the memory update phase of the GRU is  $T(2 \times n^2 + n)$ . The operation time of other parts of GRU is the same as that of PMU. Therefore, the total number of GRU operations is  $T(3 \times n \times m + 6 \times n^2 + 4 \times n)$ . In summary, the time complexity is  $O(n^2)$ .

As shown in Table 1, in general, although the time complexity of PMU is the same as that of the GRU, the total

number of operations in PMU is much less than that in GRU. Therefore, the PMU-based NSSA is much more efficient.

## 4.2. Experimental Settings

**4.2.1. Experimental Environment and Dataset.** In our simulation experiment, the public dataset UNSW-NB15 is utilized as the experimental dataset [34, 35]. In UNSW-NB15, there are 9 different modern attacks. Meanwhile, every data record contains 43 elements and a corresponding label. UNSW-NB15 is divided into 4 different Comma-Separated Values (CSV) files, which contain a total of 2540044 data records. Moreover, there are 300000 abnormal traffic data records, as shown in Table 2.

As shown in Table 2, the dataset covers 9 different attack categories; the detailed categories are as follows:

- (1) Analysis: an intrusion method that penetrates web applications through email, web scripts, ports, etc.
- (2) Backdoors: an intrusion method that bypasses the system security mechanism through technical secrets to evaluate the computer or its data
- (3) DoS: a method of deliberately attacking the implementation defects of the network protocol or directly



TABLE 1: PMU and GRU time complexity.

	Total number of operations	Time complexity
PMU	$T(2 \times n \times m + 4 \times n^2 + 4 \times n)$	$O(n^2)$
GRU	$T(3 \times n \times m + 6 \times n^2 + 4 \times n)$	$O(n^2)$

TABLE 2: UNWS-NB15 dataset data type.

Type	Quantity
Normal	2218761
Analysis	2677
Backdoors	2329
DoS	16353
Exploits	44525
Fuzzers	24246
Generic	215481
Reconnaissance	13987
Shellcode	1511
Worms	174

using brute force to exhaust the resources of the attacked object, so as to achieve an attack that makes the target network unable to use services or resources

- (4) Exploits: a type of attack that exploits the attacker's knowledge of security vulnerabilities in the operating system or software
- (5) Fuzzers: an attack type in which an attacker provides a large number of random numbers to the program or the network to make it down
- (6) Generic: use hash functions for conflicts regardless of password configuration
- (7) Reconnaissance: attacks used to collect computer information, also called probes
- (8) Shellcode: the attacker uses shell commands and a small amount of code to control the attack mode of the attacked host
- (9) Worms: worm attack, a virus attack that can replicate itself to the control host without any operation

For the convenience of experiment, we make statistics every ten minutes according to the time stamp in all the extracted dataset. A total of 144 sample data composed of the situation value is generated; among them, 100 are intercepted as the training set and 44 as the testing set. In addition, the network security situation value is 0-10. In the process of establishing the situation risk level, we will denote the situation value of 0-2 as safe, the situation value of 3-4 as low risk, and the situation value of 5-6 as medium risk. The situation value of 7-8 indicates a high risk, and the situation value of 9-10 indicates an emergency.

TABLE 3: Confusion matrix.

	Positive	Negative
True	TP	FP
False	FN	TN

4.2.2. *Experimental Criteria.* In this experiment, Accuracy, Precision, Recall, and  $F1\_score$  are used to evaluate the effectiveness of our NSSA method and some of these concepts are defined as follows.

True positive (TP): TP means that the positive samples are evaluated as positive samples

False positive (FP): FP means that the negative samples are evaluated as positive samples

True negative (TN): TN means that the negative samples are evaluated as negative samples

False negative (FN): FN means that the positive samples are evaluated as negative samples

We use a confusion matrix to represent TP, FP, TN, and FN, as shown in Table 3.

Then, the Accuracy, Precision, Recall, and  $F1\_score$  are defined as follows:

$$\begin{aligned}
 \text{Accuracy} &= \frac{\text{TN} + \text{TP}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}, \\
 \text{Precision} &= \frac{\text{TP}}{\text{FP} + \text{TP}}, \\
 \text{Recall} &= \frac{\text{TP}}{\text{FN} + \text{TP}}, \\
 F1_{\text{score}} &= 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}.
 \end{aligned} \tag{9}$$

Accuracy represents the proportion of the number of correctly identified samples in the total sample. Precision represents the proportion of actual positive samples among the number of positive samples identified. Recall represents the percentage of positive examples in the sample that are predicted to be correct. However, it is unreasonable to evaluate the performance of the model only from Precision or Recall. To make the evaluation be more convincing, except for Precision and Recall, it is generally necessary to use  $F1\_score$  as the model evaluation standard.

4.3. *Evaluation Experimental Result.* In this part, we evaluate the proposed AE-PMU-based assessment method, the PMU-based assessment method, the GRU-based assessment method, and BPNN-based assessment method from the points of effectiveness, fitting degree, and efficiency.

4.3.1. *Effectiveness Evaluation.* We compare the effectiveness of our AE-PMU-based assessment method, PMU-based assessment method, GRU-based assessment method, and BPNN-based assessment method, as shown in Figure 4.

Figure 4 measures the effectiveness of four different assessment methods from the Accuracy rate, Precision rate, Recall rate, and  $F1\_score$ . Among them, the AE-PMU-based assessment method has the best performance. This is

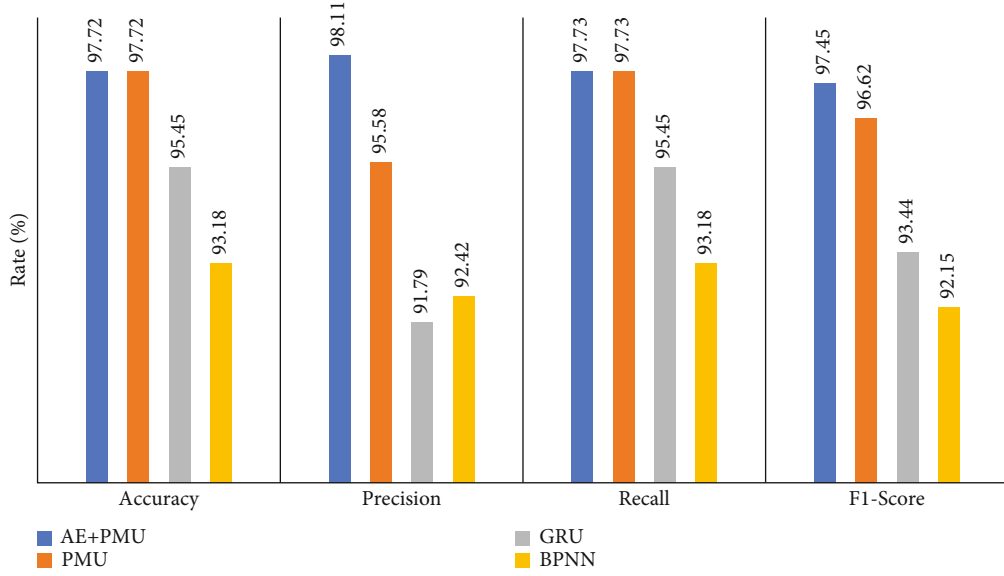


FIGURE 4: Comparison of evaluation effectiveness of different algorithms.

because BPNN-based assessment method does not consider the time sequence of the indicator data; thus, it could not evaluate the indicator data better. Although the GRU-based assessment method can consider the timing of the indicator data, compared with the PMU-based assessment method, GRU cannot effectively manage gates based on the latent relation between short- and long-term dependencies, so its effectiveness is inferior to that of the PMU-based assessment method. Because the data after AE dimensionality reduction removes the redundant part, the effectiveness of the AE-PMU-based assessment method is better than that of the PMU-based assessment method. This shows that the AE-based dimensionality reduction data fully retains the effectiveness of the indicator data, and the effectiveness of the PMU-based assessment method is better than that of the GRU-based assessment method.

4.3.2. *Goodness of Fit.* We utilize a polyline graph to intuitively show the comparison of the fit between the assessment value and the real value, as shown in Figure 5.

From Figure 5, we can see that when the sample numbers are 3, 13, 31, and 33, the network situation value fluctuates significantly, indicating that the network threats are relatively strong at these moments. In the third sample, a warning of “medium-risk” level appeared, indicating that the network is being threatened by a higher level attack, and security defense countermeasures should be taken. The “high-risk” level warnings appeared in the samples no. 13 and no. 31, indicating that the network suffers from extremely great security threats, and timely protection or rescue is required. According to the two fitting curves of the real value and the assessment value, it can be seen that the situation assessment result obtained by the proposed method basically fits the real security situation. Except for sample no. 31, which misjudged “high risk” as “safety,” all other samples were correctly judged, which can more accurately fit the real security situation of the current network.

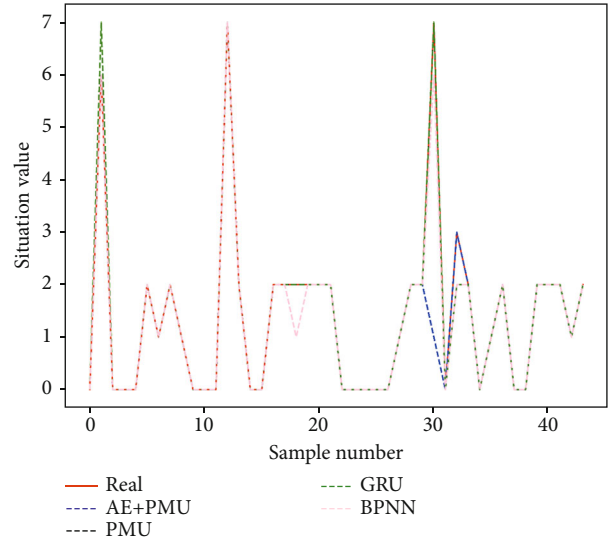


FIGURE 5: The fitted polyline of the assessment value and the real value.

Among other methods, the PMU-based assessment method makes a mistake once, the GRU-based assessment method makes a mistake twice, and the BPNN-based assessment method makes a mistake three times.

Our analysis of the reasons is consistent with the above “effectiveness evaluation” reasons. According to the above experimental results, it can be shown that the AE-PMU-based NSSA method can adapt to the NSSA under the modern network environment and can more accurately fit the real network security situation changes.

4.3.3. *Performance Evaluation.* Among the above four methods, although the network structure of BPNN is simple, it is rarely used in practical applications because it cannot fully characterize the data characteristics by using the time

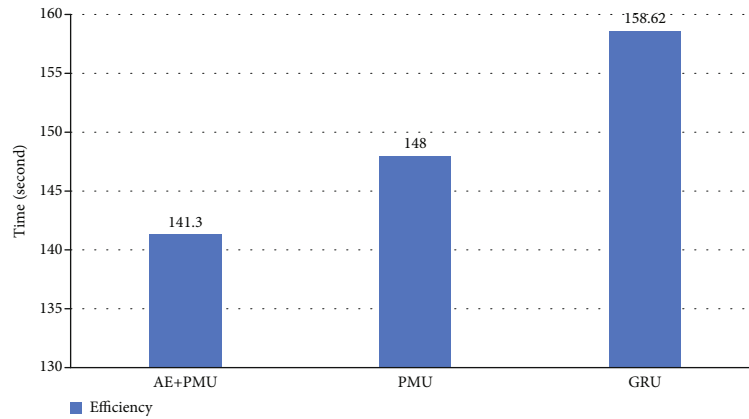


FIGURE 6: Efficiency comparison of different methods.

sequence of the data. Therefore, here we only compare the performance (assessment time) of NSSA methods based on PMU, GRU, and AE+PMU, as seen in Figure 6.

We can see from Figure 6 that the running time of the AE-PMU-based assessment method is the smallest, the running time of the PMU-based assessment method is the second, and the running time of the GRU-based assessment method is the longest. This is because the GRU has two gate structures. The reset gate helps the GRU decide which past information needs to be forgotten, and the update gate helps the GRU decide which past information needs to be passed to the future. However, PMU uses a gate to complete the calculation tasks of the GRU update gate and reset gate, thus reducing the amount of calculation. Meanwhile, AE reduces the dimension of the original indicator data. Hence, the computational efficiency of the AE-PMU-based assessment method is the best.

## 5. Conclusions

In large-scale network environment, the diversity of network threats and the high dimensionality of indicator data make the NSSA become more difficult. In this paper, we studied the NSSA in large-scale network environment and then proposed a novel NSSA method based on AE and PMU. Specifically, we first used AE for data dimensionality reduction to remove the redundant data. Then, we utilized PMU to achieve NSSA. By taking the advantage of PMU, the proposed method can effectively improve the performance of the model. Finally, we implemented the proposed method and provided the performance evaluation. The experimental results can show that compared with the existing methods, our method had significant advantages in efficiency, accuracy, and fit degree.

## Data Availability

The dataset UNSW-NB15 can be got by sending e-mail to the corresponding author or downloaded from <https://research.unsw.edu.au/projects/unsw-nb15-dataset>.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. 61962015), the Natural Science Foundation of Guangxi (No. 2020GXNSFBA297132), the Science and Technology Program of Guangxi (No. AD20297028), the Innovation Project of GUET Graduate Education (No. 2021YCX061), and the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security (No. AGK2020005).



## References

- [1] Y. B. Leau, S. Manickam, and Y. W. Chong, "Network security situation assessment: a review and discussion," in *Information Science and Applications*, K. Kim, Ed., vol. 339 of Lecture Notes in Electrical Engineering, pp. 407–4414, Springer, Berlin, Germany, 2015.
- [2] X. Tao, Y. Liu, F. Zhao, C. Yang, and Y. Wang, "Graph database-based network security situation awareness data storage method," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, 2018.
- [3] P. Thagard, "Frames, knowledge, and inference," *Synthese*, vol. 61, no. 2, pp. 233–259, 1984.
- [4] T. M. Mitchell, *Machine Learning*, McGraw Hill, Burr Ridge, IL, 1997.
- [5] M. I. Jordan and T. M. Mitchell, "Machine learning: trends, perspectives, and prospects," *Science*, vol. 349, no. 6245, pp. 255–260, 2015.
- [6] Y. F. Wang, J. Wang, Z. B. Xu, and H. Li, "Assessing cyber-threats situation for electric power information networks," in *2013 Ninth International Conference on Natural Computation (ICNC)*, pp. 1557–1562, Shenyang, China, 2013.
- [7] H. Wang, Z. F. Chen, Z. Feng et al., "Research on network security situation assessment and quantification method based on analytic hierarchy process," *Wireless Personal Communications*, vol. 102, no. 2, pp. 1401–1420, 2018.
- [8] F. W. Li, S. C. Yang, and J. Zhu, "Improved network security situation assessment method based on fuzzy hierarchy

- method,” *Journal of Computer Applications*, vol. 42, no. 9, pp. 2622–2626, 2014.
- [9] R. Zhang, J. Cheng, X. Tang, Q. Liu, and X. He, “DDoS attack security situation assessment model using fusion feature based on fuzzy C-means clustering algorithm,” in *International Conference on Cloud Computing and Security (ICCCS)*, X. Sun, Z. Pan, and E. Bertino, Eds., vol. 11064 of Lecture Notes in Computer Science, pp. 654–669, Springer, Cham, 2018.
- [10] B. Yi, Y. P. Cao, and Y. Song, “Network security risk assessment model based on fuzzy theory,” *Journal of Intelligent & Fuzzy Systems*, vol. 38, no. 4, pp. 3921–3928, 2020.
- [11] Z. H. Liu, Z. Bin, Z. Ning, and L. Li, “Hierarchical network threat situation assessment method for DDoS based on DS evidence theory,” in *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 49–53, Beijing, China, 2017.
- [12] D. Codetta-Raiteri and L. Portinale, “Decision networks for security risk assessment of critical infrastructures,” *ACM Transactions on Internet Technology*, vol. 18, no. 3, pp. 1–22, 2018.
- [13] J. Wang, M. Neil, and N. Fenton, “A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model,” *Computers & Security*, vol. 89, article 101659, 2020.
- [14] Z. Fan, Y. Xiao, A. Nayak, and C. Tan, “An improved network security situation assessment approach in software defined networks,” *Peer-to-Peer Networking and Applications*, vol. 12, no. 2, pp. 295–309, 2019.
- [15] Y. W. Liao, G. S. Zhao, J. Wang, and S. Li, “Network security situation assessment model based on extended hidden Markov,” *Mathematical Problems in Engineering*, vol. 2020, Article ID 1428056, 13 pages, 2020.
- [16] W. S. Noble, “What is a support vector machine?,” *Nature Biotechnology*, vol. 24, no. 12, pp. 1565–1567, 2006.
- [17] Y. Liang, Z. P. Cai, J. G. Yu, Q. L. Han, and Y. S. Li, “Deep learning based inference of private information using embedded sensors in smart devices,” *IEEE Network Magazine*, vol. 32, no. 4, pp. 8–14, 2018.
- [18] Y. Lecun, Y. Bengio, and G. Hinton, “Deep learning,” *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.
- [19] X. Y. Chen, X. C. Yin, and A. Sun, “Network security situation assessment model based on GSA-SVM,” in *Proceedings of 2018 International Conference on Computer, Communication and Network Technology (CCNT)*, pp. 414–420, Zhejiang, China, June 2018.
- [20] J. Qiang, F. Wang, and X. L. Dang, “Network security based on DS evidence theory optimizing CS-BP neural network situation assessment,” in *2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, pp. 153–159, Shanghai, China, June 2018.
- [21] L. L. Shi and J. Chen, “Assessment model of command information system security situation based on twin support vector machines,” in *2017 International Conference on Network and Information Systems for Computers (ICNISC)*, pp. 135–139, Shanghai, China, April 2017.
- [22] Y. Y. Gao, Y. J. Shen, G. D. Zhang, and S. Zheng, “Information security risk assessment model based on optimized support vector machine with artificial fish swarm algorithm,” in *2015 6th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, pp. 599–602, Beijing, China, September, 2015.
- [23] W. H. Han, Z. H. Tian, Z. Z. Huang, D. Q. Huang, and Y. Jia, “Quantitative assessment of wireless connected intelligent robot swarms network security situation,” *IEEE Access*, vol. 7, no. 99, pp. 134293–134300, 2019.
- [24] H. Y. Yang, R. Y. Zeng, G. Q. Xu, and L. Zhang, “A network security situation assessment method based on adversarial deep learning,” *Applied Soft Computing*, vol. 102, no. 8, article 107096, 2021.
- [25] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, “Learning representations by back-propagating errors,” *Nature*, vol. 323, no. 6088, pp. 533–536, 1986.
- [26] G. E. Hinton, S. Osinder, and Y. W. Teh, “A fast learning algorithm for deep belief nets,” *Neural Computation*, vol. 18, no. 7, pp. 1527–1554, 2006.
- [27] M. Mohamed, “Parsimonious memory unit for recurrent neural networks with application to natural language processing,” *Neurocomputing*, vol. 314, no. 7, pp. 48–64, 2018.
- [28] L. Landberg, G. Giebel, H. A. Nielsen, T. Nielsen, and H. Madsen, “Short-term prediction? An overview,” *Wind Energy*, vol. 6, no. 3, pp. 273–280, 2003.
- [29] C. Yang, X. Tao, F. Zhao, and Y. Wang, “Secure data transfer and deletion from counting bloom filter in cloud computing,” *Chinese Journal of Electronics*, vol. 29, no. 2, pp. 273–280, 2020.
- [30] C. Yang, X. Tao, F. Zhao, and Y. Wang, “A new outsourced data deletion scheme with public verifiability,” in *Wireless Algorithms, Systems, and Applications. WASA 2019*, E. Biagioni, Y. Zheng, and S. Cheng, Eds., vol. 11604 of Lecture Notes in Computer Science, pp. 631–638, Springer, Cham, 2019.
- [31] C. Yang, F. Zhao, X. Tao, and Y. Wang, “Publicly verifiable outsourced data migration scheme supporting efficient integrity checking,” *Journal of Network and Computer Applications*, vol. 192, article 103184, 2021.
- [32] X. Zheng and Z. P. Cai, “Privacy-preserved data sharing towards multiple parties in industrial IoTs,” *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.
- [33] K. Y. Li, G. C. Luo, Y. Ye, W. Li, S. Ji, and Z. Cai, “Adversarial privacy-preserving graph embedding against inference attack,” *IEEE Internet of Things*, vol. 8, no. 8, pp. 6904–6915, 2021.
- [34] N. Moustafa and J. Slay, “UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),” in *Military Communications and Information Systems Conference 2015 (MilCIS)*, pp. 1–6, Canberra, Australia, November 2015.
- [35] N. Moustafa and J. Slay, “The evaluation of network anomaly detection systems: statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set,” *Information Security Journal: A Global Perspective*, vol. 25, no. 1, pp. 18–31, 2016.

## Research Article

# Network Threat Detection Based on Group CNN for Privacy Protection

Yanping Xu <sup>1</sup>, Xia Zhang,<sup>1</sup> Chengdan Lu <sup>2</sup>, Zhenliang Qiu,<sup>1</sup> Chunfang Bi,<sup>3</sup> Yuping Lai,<sup>4</sup> Jian Qiu,<sup>5</sup> and Hua Zhang<sup>6</sup>

<sup>1</sup>School of Cyberspace, Hangzhou Dianzi University, Hangzhou, China

<sup>2</sup>Zhejiang Electronic Information Product Inspection and Research Institute (Key Laboratory of Information Security of Zhejiang Province), Hangzhou, China

<sup>3</sup>Chengzhong Primary School, Zibo, China

<sup>4</sup>School of Cyberspace, Beijing University of Post and Telecommunications, Beijing, China

<sup>5</sup>Center for Undergraduate Education, Westlake University, Hangzhou, China

<sup>6</sup>School of Computer Science, Hangzhou Dianzi University, Hangzhou, China

Correspondence should be addressed to Chengdan Lu; [lcd@zdjy.org.cn](mailto:lcd@zdjy.org.cn)

Received 8 June 2021; Revised 15 July 2021; Accepted 3 August 2021; Published 3 September 2021

Academic Editor: Yaguang Lin

Copyright © 2021 Yanping Xu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The Internet of Things (IoT) contains a large amount of data, which attracts various types of network attacks that lead to privacy leaks. With the upgrading of network attacks and the increase in network security data, traditional machine learning methods are no longer suitable for network threat detection. At the same time, data analysis techniques and deep learning algorithms have developed rapidly and have been successfully applied to a variety of tasks for privacy protection. Convolutional neural networks (CNNs) are typical deep learning models that can learn and reconstruct features accurately and efficiently. Therefore, in this paper, we propose a group CNN models that is based on feature correlations to learn features and reconstruct security data. First, feature correlation coefficients are computed to measure the relationships among the features. Then, we sort the correlation coefficients in descending order and group the data by columns. Second, a 1D group CNN model with multiple 1D convolution kernels and 1D pooling filters is built to address the grouped data for feature learning and reconstruction. Third, the reconstructed features are input to shadow machine learning models for network threat prediction. The experimental results show that features reconstructed by the group CNN can reduce the dimensions and achieve the best performance compared to the other present dimension reduction algorithms. At the same time, the group CNN can decrease the floating point of operations (FLOP), parameters, and running time compared to the basic 1D CNN.

## 1. Introduction

Application scenarios for the IoT are becoming increasingly mature, which brings people to a new digital lifestyle by connecting everything [1]. However, as the IoT scope and scale continue to expand, the threat of network intrusion has become more serious than ever before [2, 3]. Malicious software, DDoS attacks, vulnerability attacks, and other attacks always occur in the IoT cyberspace, which inevitably leads to privacy leaks [4–6]. These attacks harm not only physical terminal equipment but also people's lives and property [7].

In the IoT, there are three major security and privacy challenges: terminal authentication, network attack prevention, and personal data protection [8, 9]. In terms of privacy challenges, blockchain-enabled technology using encryption algorithm will not cause privacy data leakage [10–12]. In terms of network attack prevention, network threat detection technology is required to find network intrusions and meet the demand of IoT assurance. In this situation, intrusion detection [13], malicious code detection [14], malware detection [15], malicious URL detection [16], and vulnerability mining [17] based on machine learning algorithms are



considered to be effective network threat behavior detection measures. With the upgrading of attacks and the increase in network security data, traditional machine learning methods are no longer suitable. At the same time, data analysis techniques and deep learning algorithms have developed rapidly and have been successfully applied to natural language processing, image recognition, and video detection [18, 19]. In the field of network security, many research studies have used deep learning technology to detect network threats and have garnered many achievements [13, 20].

Big data analysis techniques include oversampling imbalanced datasets, dimension reduction of high-dimensional data, and correlation analysis between features [21]. Correlation analysis studies the correlation coefficients among two or more random variables [22]. In probability theory, the correlation coefficient can reflect that there is a close relationship between variables. The range of the correlation coefficient is  $[-1, 1]$ . The closer the absolute value of the correlation coefficient is to 1, the closer the linear relationship between the two variables is. In contrast, the closer the absolute value of the correlation coefficient approaches to 0, the weaker the linear relationship between the two variables will be. Therefore, we use a correlation coefficient matrix to measure the relationships among the column vectors in the data matrix.

Machine learning algorithms are divided into shallow learning and deep learning [13, 22, 23]. Shallow learning is treated as a traditional machine learning technique that achieves desirable effects to address a small amount of data. Shallow learning algorithms, including support vector machines (SVMs), random forests (RFs), decision trees (DTs), and  $K$ -means algorithms, have been employed to distinguish abnormal data from network activities [13, 20]. Comparing rule-based intrusion detection systems (IDSs), shallow learning methods do not rely on the domain knowledge and can extend their generalization ability to detect the attack variants and unknown attacks. However, shallow learning is no longer suitable to address the complexity of the dataset and the diversity of the features [13]. In this situation, it emerges that deep learning is required.

Deep learning, also known as deep neural networks (DNNs), is designed from hierarchical structures composed of multiple neural layers [24]. Deep learning can extract and learn information to generate the reconstruction features from the input raw data through layer-by-layer neural processing. Benefitting from their feature reconstruction characteristics, deep learning algorithms, including CNNs, recurrent neural network (RNNs), and generative adversarial networks (GANs) [25–31] have been widely used not only for visual recognition and language understanding but also for network threat detection. Studies in [32] show that deep learning algorithm-based methods can achieve better performance when working on reconstructed features.

CNN, as one of the typical DNN models, was first proposed to solve the problem of 2D image recognition. 2D CNNs have been successfully used to learn and reconstruct features from raw data and have developed into the dominant approach for accomplishing recognition and detection tasks of image and speech analysis [33]. Due to the good characteristics of CNN learning, 1D CNN has been proposed

to address 1D signals based on 2D CNN and has achieved superior performance with high efficiency [34, 35]. To adapt to the data characteristics of 1D signals, comparing 2D CNNs, the hierarchical architecture of 1D CNNs is simplified [36]. For example, in the structure of 1D CNN, the data of the convolution kernels and pooling filters are 1D. In the structure of 2D CNN, the data of the convolution kernels and pooling filters are 2D. Therefore, in the structure and running process, 1D CNN is simpler than 2D CNN [34]. Therefore, we build a 1D CNN for analyzing network security data.

However, with the deepening of the network layers, the number of parameters increases exponentially [37]. For example, in a traditional basic 2D CNN, if the size of the input image feature is  $C * H * W$ , the number of convolution kernels is  $N$ , the size of each convolution kernel is  $K * K$ , and the size of the feature map is  $M * M$ . The total number of parameters in all convolution layers is  $C * N * (K * K + 1) * (M * M)$ . Obviously, the number of parameters is large. To reduce the number of parameters and improve the efficiency of the CNN, a group CNN is proposed to group the convolution kernels separately [38]. Suppose that the convolution kernels are divided into  $T$  groups, the number of convolution kernels in each group is  $N/T$ , the size of each convolution kernel is  $K' * K'$ , and the size of the feature map is  $M' * M'$ . The total number of parameters in the convolution layers is  $C * (N/T) * (K' * K' + 1) * (M' * M')$ . When grouping, the sizes of the convolution kernel and the feature maps are considered to be smaller, and the total number of parameters of all of the convolution layers is reduced. At the same time, the performance of the algorithm is improved. Therefore, we use a group CNN to address the big network data.

When analyzing the security data for network threat detection, we determined that each threat behavior had 1D characteristics, which makes the threats similar to 1D signals. Additionally, the group CNN can improve the efficiency. Therefore, learning from the successful experience of using 1D CNN to process 1D signals, we build a 1D group CNN model to perform feature learning and reconstruction of the security dataset. In this paper, we combine shadow learning and deep learning algorithms to build a network threat detection model. First, correlation coefficients are computed to measure the relationships of the features. Then, we sort the correlation coefficients in descending order and group the data by the columns. Second, a 1D group CNN model with multiple 1D convolution kernels and 1D pooling filters is built for feature learning and reconstruction. In each convolution layer and pooling layer, the convolution kernels and pooling filters are grouped. Third, the reconstructed features are input to the shadow learning models for threat prediction.

The proposed method includes the following advantages:

- (1) Compared with the traditional basic 1D CNN, the proposed group CNN model with grouped convolution kernels and pooling filters reconstructs the features layer by layer and reduces the FLOP, parameters, and running time
- (2) The proposed data grouping, which is based on correlation coefficients between the features, can

enhance the structural information used by group CNN to address the data

- (3) The proposed group CNN model can reduce the dimensions by generating fewer reconstructed features and can achieve high performance
- (4) The FLOP and parameter counts of the group CNN are calculated and are less than those of the basic 1D CNN

The remainder of this paper is organized as follows. Section 2 discusses the related work using shallow learning algorithms and deep learning technology in network threat detection. A description of the 1D group CNN model is provided in Section 3. Experimental results and analysis are presented in Section 4. The work is concluded in Section 5.

## 2. Related Work

Machine learning techniques, including shallow learning and deep learning algorithms, have been used for anomaly detection since the early 2000s and can automatically mine hidden information on the differences between normal and malicious behaviors.

Shallow learning algorithms, such as traditional machine learning algorithms, were previously applied to analyze system logs, malicious software, and network traffic and to output the predicted labels of the input data. By comparing the predicted labels with the true labels, the performance of the shallow learning algorithms can be achieved. The most widely used algorithms include SVM, DT, NB, and K-means [39, 40]. Buczak et al. [39] provided a summary as a survey to describe some machine learning and data mining methods, such as DT, SVM, RF, and NB, which were used for cybersecurity intrusion detection. Kruczkowski and Szykiewicz [41] used SVM with kernels to build a malware detection model. The results revealed that SVM was a robust and efficient method for data analysis and it increased the efficiency of malware detection. Bilge et al. [42] presented the EXPOSURE system to analyze large-scale and passive domain name service (DNS) data. The classifier is built by J48 DT. The experimental results suggested that the minimum error was achieved by a decision tree. Aung and Min [43] used K-means and classification and regression tree (CART) algorithms to mine the KDD'99 dataset for intrusion detection. The experimental results showed that the hybrid data mining method could achieve good accuracy in performance analysis with time complexity. Mo et al. [44] discussed three data clustering algorithms, including K-means, fuzzy C means (FCM), and expectation maximization (EM), to capture abnormal behavior in communication networks. The experimental results showed that FCM was more accurate.

More recently, deep learning technology is developing rapidly and has been successfully been applied to a variety of tasks, such as natural language processing, image recognition, and computer vision [45]. CNNs, as typical DNN models, have feedforward neural networks with convolution calculations and deep structures, which can learn and reconstruct features more accurately and efficiently. According to

the type of raw data, 1D CNN and 2D CNN models should be built. A 1D CNN is constructed to process one-dimensional sequence signal data and natural language, and a 2D CNN is constructed to address two-dimensional image and video data [36]. Because the CNN can learn and reconstruct features, both 1D CNN and 2D CNN are used for network threat detection.

Xiao et al. [46] proposed a network intrusion detection model based on a CNN. The original traffic data were reduced in dimensions through principal component analysis (PCA) and an autoencoder (AE), and then, the data were converted into a 2D image format. Next, the 2D data were input to the CNN model to evaluate the performance. Wang et al. [47] proposed a method that represented raw flow data as an image and used the CNN for classification and identification without manually selecting and extracting features. Experimental results showed that this method had high availability and high accuracy in malicious traffic identification. Zhang et al. [48] proposed a feature-hybrid malware variant detection approach based on 2D CNN and 1D BPNN. A 2D CNN was designed to compute the dot product and compress the dimension of the PCA-initialized opcode matrix. Experimental results showed that the method achieved more than 95% malware detection accuracy. Zhang et al. [49] proposed converting opcodes into a 2D matrix and adopted the CNN to train the 2D opcode matrix for malware recognition. Experimental results showed that their approach could significantly improve the detection accuracy by 15%. Yan et al. [50] proposed converting Android opcode into 2D gray images with fixed size and adopted a CNN to train and detect Android malware. Through the above literature, we can determine that the input data of the 2D CNN model must be converted into 2D data first.

Ma et al. [51] proposed a hybrid neural network comprised of 1D CNN and DNN to learn the characteristics of high-dimension network flows for network anomaly detection. Experimental results showed that the proposed method was better than those of other algorithms on the comprehensive performances. Azizjon et al. [52] proposed a 1D CNN model to serialize the TCP/IP packets in a predetermined time range as an invasion Internet traffic model for the IDS. Experimental results showed that 1D CNN and its variant architectures had the capability to extract high-level feature representations and outperformed the traditional machine learning classifiers. Wei et al. [53] proposed a 1D CNN-based model to identify phishing websites on a URL address text, which was converted to one-hot character-level representation. This mode liked the 1D CNN to analyze natural language. Experimental results showed that the method was faster to detect zero-day attacks. Zhang et al. [54] designed a flow-based intrusion detection model called SGM-CNN, which first integrated SMOTE and GMM to make an imbalanced class process and used 1D CNN to detect the network traffic data with high accuracy. Experimental results showed that SGM-CNN was superior to the state-of-the-art methods, and effective for large-scale imbalanced intrusion detection.

The group convolution was first proposed and used in AlexNet by Krizhevsky et al. [37] for distributing the model over two GPUs to handle the memory insufficient issue.



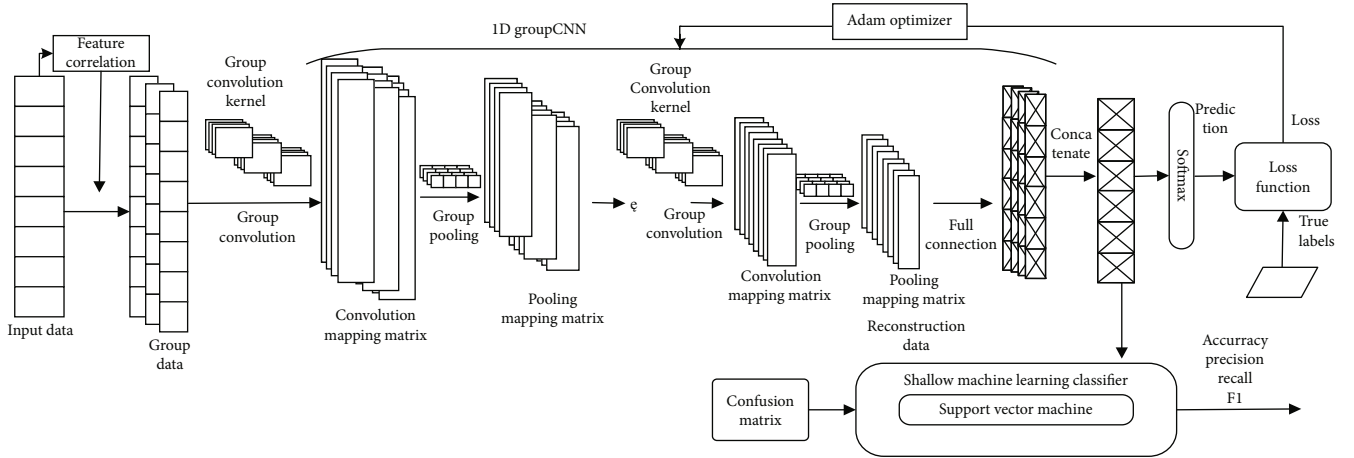


FIGURE 1: The architecture of the 1D group CNN.

AlexNet was designed as a the group convolution method could increase the diagonal correlations between the convolution kernels, reduce the training parameters, and be not easy to overfit. Zhang et al. [38] proposed interleaved group CNNs called IGCNets, which contained a pair of successive interleaved group convolutions, i.e., the primary group convolution and the secondary group convolution. IGCNets was wider than a regular convolution. Experimental results demonstrated that IGCNets was more efficient in parameters and computation complexity. Xie and Girshick [55] proposed a simple, highly modularized network architecture named ResNeXt, which was based on AlexNet and constructed by repeating a building block. The idea of ResNeXt was consistent of group convolutions. Without increasing the complexity of the parameters, the accuracy of the model could be improved, and the number of super parameters could be reduced. Lu et al. [39] proposed a novel repeated group convolutional kernel (RGC) to remove the filter's redundancy from group extent. SRGC-Nets worked well in not only reducing the model size and computational complexity, but also decreasing the testing and training running time.

In the 2D CNN-based model, the input data are converted to the image format. In the 1D CNN-based model, the input data are treated as timing serial signals, similar to natural language. Compared with a 2D CNN, the structure of a 1D CNN is simpler, which makes the computational complexity lower. Therefore, we intend to learn from the experience of applying the 1D CNN to address the data and to construct a network threat detection model for feature learning and reconstruction.

### 3. Proposed Solution

The architecture of the proposed network threat detection model, which combines the 1D group CNN algorithm and machine learning classification methods, is shown in Figure 1. First, correlation coefficients are computed to measure the relationships between the features. Then, we sort the correlation coefficients in descending order and group the data. Second, a group CNN model with multiple groups of

convolution kernels and pooling filters is built for feature learning and reconstruction. In the group CNN model, the input data are divided into multiple groups. Similarly, convolution kernels and pooling filters in each layer are divided into multiple groups. Each group of data is computed by each convolution kernel and is then computed by each pooling filter.

Finally, a concatenating layer is used to concatenate multiple groups of data to form one group of reconstructed data. Third, the reconstructed data are input to the shadow machine learning model for threat prediction. In the shadow machine learning model, traditional machine learning algorithms are used to identify normal or abnormal samples from reconstruction data. Then, the accuracy, precision, recall, and F1, which are the detection performance indicators, are computed according to the statistics of the confusion matrix.

*3.1. Group Convolutional Neural Network for Feature Reconstruction.* The convolutional neural network (CNN) is one of the representative algorithms for deep learning. It is a type of deep feed forward neural network that has convolution calculations [56]. CNNs have the capability of representation learning to generate reconstruction features. At the same time, by the convolution operation and pooling operation, a CNN can achieve the purpose of reducing the dimensions of the input data [57]. Additionally, grouped convolution kernels and pooling filters can reduce the number of parameters and improve the performance [39]. Therefore, we use 1D group convolution kernels to build a 1D group CNN model in this work.

The 1D group CNN includes multiple convolutional layers, multiple pooling layers, a full connection layer, a concatenating layer, and an output layer. In each convolutional layer, the convolutional kernels are divided into multiple groups. At the same time, in each pooling layer, the pooling filters are divided into multiple groups. The fully connected layer determines the dimensions of the reconstruction features of each group. The concatenating layer is used to concatenate the reconstruction features of each group to form the final results. The combination of multiple layers makes the group CNN output the low-dimensional

reconstruction features, which can not only strengthen the original data's features but also relatively reduce the dimension.

**3.2. Feature Correlation.** In this work, we assume that the input data are  $X = (x_1, x_2, \dots, x_n, \dots, x_N)$ ,  $x_n = (x_{n1}, x_{n2}, \dots, x_{nD})^T$ ,  $n = (1, 2, \dots, N)$ , containing  $N$  independent  $D$ -dimensional samples. Usually, the malicious samples have some similar values of the same features and so are the benign samples. Thus, there are certain correlations between the features and the labels. We calculate the correlations between the data features and labels based on the correlation coefficients.

First, we calculate the correlations between the data features and labels based on the correlation coefficients to form a correlation coefficient matrix  $\mathbf{R}$ . Then, we randomly select one row vector  $\mathbf{R}_i$  and rank the correlation elements in descending order. Furthermore, we divide the data into  $T$  groups by columns equally according to the descending correlations. Usually, each group has the same number of features, which is  $D/T$ . The input data in the  $t$ th ( $0 < t \leq T$ ) group are expressed as  $X_t = (x_{1,t}, x_{2,t}, \dots, x_{n,t}, \dots, x_{N,t})$ . So the correlation coefficients of the first group data are the biggest, and that of the last group data are the smallest.

**3.3. Group CNN.** After the data are grouped, we start to establish the group CNN model, which contains  $L$  convolution layers,  $L$  pooling layers, a full connection layer, a concatenating layer, and an output layer. Like the group counts of the input data, the convolution kernels and pooling filters in each layer are also divided into  $T$  groups. Further, there are  $M$  convolution kernels in each group.

Suppose that the  $m$ th ( $0 < m \leq M$ ) convolution kernel in the  $t$ th ( $0 < t \leq T$ ) group of the  $l$ th ( $0 < l \leq L$ ) convolution layer is expressed as  $K_l^{m,t}$ . Convolution operations are conducted between the grouped data  $X_t$  and the convolution kernel, or the output  $R_{l-1}^{m,t}$  of the previous pooling layer. Then, activation function is working to generate the feature maps. Suppose the feature map in the  $t$ th group of the  $l$ th convolution layer by the  $m$ th convolution kernel is  $S_l^{m,t}$ , which is expressed as follows:

$$S_l^{m,t} = \begin{cases} \text{Re } LU(\text{conv1D}(K_l^{m,t}, X_t) + b_l^{m,t}), & l = 1, \\ \text{Re } LU(\text{conv1D}(K_l^{m,t}, R_{l-1}^{m,t}) + b_l^{m,t}), & 1 < l \leq L, \end{cases} \quad (1)$$

where  $\text{Re } LU(\cdot)$  is the nonlinear activation function.  $\text{conv1D}(\cdot)$  is the 1D convolution function.  $R_{l-1}^{m,t}$  is the output of the  $m$ th pooling filter in  $t$ th group of the  $(l-1)$ th pooling layer.  $b_l^{m,t}$  is the bias of the  $t$ th group in the  $l$ th convolution layer.

After the convolution layer, a pooling layer not only reduces the dimensions of feature maps from the upper convolution layer to reduce the computational cost but also provides basic translation invariance. The  $l$ th pooling layer is immediately after the  $l$ th convolution layer. Suppose the  $m$ th pooling filter of the  $t$ th group in the  $l$ th pooling layer is  $P_l^{m,t}$ . The input data of the  $l$ th pooling layer is the output of the  $l$ th convolution layer, and the output data of the  $t$ th group

in the  $l$ th pooling layer is  $R_l^{m,t}$ , which is expressed as follows:

$$R_l^{m,t} = \text{Re } LU(\text{max pooling}(S_l^{m,t}, P_l^{m,t})), \quad (2)$$

where  $\text{max pooling}(\cdot)$  is the pooling function. The max pooling is adopted in this paper.

After the last pooling layer is the full connection layer. Last pooling layer is connected to a fully connected layer. After the convolution operations and pooling operations, the original data is converted into the feature maps. In the full connection layer, the  $t$ th feature map is mapped to the group reconstruction features  $X_t'$  by a global convolution operation:

$$X_t' = \text{Re } LU\left(\sum_m (\text{conv1D}(K_{full}^{m,t}, R_L^{m,t}) + b_L^{m,t})\right), \quad (3)$$

where  $K_{full}^{m,t}$  is the convolution kernel of the full connection layer.  $b_L^{m,t}$  is the bias of the full connection layer.

Further, the fully connected layer is connected to the concatenating layer. The  $T$  groups of the reconstructed features  $X_t'$  are concatenated to form the final reconstructed features  $X'$ :

$$X' = \text{concatenate}(X_t'), \quad (4)$$

where  $\text{concatenate}(\cdot)$  is the reconstruction features' concatenated function.

The size of  $X'$  is  $N \times D'$ . When  $D'$  is less than  $D$ , it means that the dimension of  $D'$  is less than that of  $D$ . In other words, 1D CNN realizes the generation of reconstruction features and the dimension reduction of features.

**3.4. Floating Point of Operations and Parameters.** Floating point of operations (FLOP) is used to calculate the times of multiplications and additions, which are related to the overall running time of the model [58]. In this section, we want to calculate the FLOP and parameter counts of the group CNN. However, the group CNN is proposed on the basic 1D CNN. So, we first calculate the FLOP and parameter counts of the basic 1D CNN. Then, we calculate the FLOP and parameter counts of the group CNN based on that of the basic 1D CNN.

**3.4.1. FLOP and Parameter Counts of the Basic 1D CNN.** Suppose that the basic 1D CNN with fully connected layers is used for feature reconstructed. First, FLOP is computed. We assume that the input data are  $X$ , containing  $N$  independent  $D$ -dimensional samples. In the basic 1D CNN, the number of the input convolution channels is  $C_{in}$ , the number of the convolution kernels is  $M'$ , and the size of the convolution kernels is  $1 * W'_1$ . The size of the feature map of the convolution operation is  $1 * W'_2$ . The numbers of the output convolution channels are  $C_{out}$ . The FLOP performed by a

convolution layer is as follows:

$$N * C_{in} * M' * (1 * W_1' + 1) * W_2' * M' * W_1' * C_{out}, \quad (5)$$

where  $(1 * W_1' + 1)$  means that a multiplication is performed by one convolutional kernel sampling the input data.  $(+1)$  is to add the bias.

$*W_2'$  means the number of multiplications performed by one convolutional kernel to get the feature maps of the output convolution operation. The definition of  $W_2'$  is  $W_2' = (D + 2padding - W_1')/stride + 1$ , where padding = 0, stride = 1.

$*M'$  means multiple convolutional kernels computing in the operation.

$*M' * W_1'$  means the number of addition from the feature map of the convolution operation to the output feature map of the convolution layer.

It is noted that the operations of  $Re\ LU(\cdot)$  and the pooling layers do not contain multiplication and addition operations. Therefore, the FLOP does not consider the operations of  $Re\ LU(\cdot)$  and the pooling layers.

$*C_{in}$  and  $*C_{out}$  means repeating calculation in multiple input channels and output channels.

$*N$  means repeating calculation of all the samples.

Basic 1D CNN has  $L$  convolution layers, so the FLOP of the basic 1D CNN model equals the sum of the FLOP of each convolution layer, which can be computed as follows:

$$\sum_{l=1}^L N * C_{l,in} * M_l' * (1 * W_{l,1}' + 1) * W_{l,2}' * M_l' * W_{l,1}' * C_{l,out}. \quad (6)$$

Then, the bias term is ignored and the FLOP calculation formula (6) is written as follows:

$$o\left(\sum_{l=1}^L N * C_{l,in} * M_l'^2 * W_{l,1}'^2 * W_{l,2}' * C_{l,out}\right). \quad (7)$$

It can be seen that FLOP is determined by the number of the samples, the number of the convolutional layers, the number of the convolutional kernels per layer, the size of each convolutional kernel, the length of the feature map of the convolution operation, and the number of the input and output convolution channels.

Next, we computed the parameter count of basic 1D CNN. The parameter count is to get the statistics of the parameters during the basic 1D CNN operating, containing weighting parameters and bias parameters, which appear in the running process of the model. In the above basic 1D CNN, in the case of a single channel and a single convolution kernel, the number of the parameters is  $(W_1' + 1)$ . When the number of the convolution kernels is  $M'$  and the number of the convolution layers is  $L$ , the parameter count of each layer is  $\sum_{l=1}^L N * C_{l,in} * M_l' * (W_{l,1}' + 1) * C_{l,out}$ . Then, the bias term is ignored and the parameter count calculation formula is

written as follows:

$$o\left(\sum_{l=1}^L N * C_{l,in} * M_l' * W_{l,1}' * C_{l,out}\right). \quad (8)$$

It can be seen that the parameter count is determined by the number of the samples, the number of the convolutional layers, the number of the convolutional kernels per layer, the size of each convolutional kernel, and the number of the input and output convolution channels.

**3.4.2. FLOP and Parameter Counts of the Group CNN.** Like basic 1D CNN, the FLOP and parameter count of group CNN can be computed. Suppose that the input data is  $X$ , containing  $N$  independent  $D$ -dimensional samples, which are grouped to  $T$  groups. It means that the dimension of each group data is  $D/T$ . The numbers of the input and output convolution channels are  $C_{in}$  and  $C_{out}$ . The structure of group CNN contains  $L$  convolution layers and  $L$  pooling layers. There are  $T$  group convolution kernels in each convolution layer. The pooling layer is the same. There are  $M$  convolution kernels in each group convolution kernels. The size of each convolution kernel is  $1 * W_1$ . The size of the feature map of the convolution operation is  $1 * W_2$ . Therefore, the FLOP of each group is

$$N * C_{in} * M * (1 * W_1 + 1) * W_2 * M * W_1 * C_{out}, \quad (9)$$

where  $W_2 = ((D/T) + 2padding - W_1)/stride + 1$ , where padding = 0, stride = 1.

Total FLOP of the model equals the sum of the FLOP of each convolution layer, which can be computed as follows:

$$\sum_{l=1}^L \sum_{t=1}^T N * C_{l,t,in} * M_{l,t} * (1 * W_{l,t,1} + 1) * W_{l,t,2} * M_{l,t} * W_{l,t,1} * C_{l,t,out}. \quad (10)$$

Then, the bias term is ignored and the FLOP in formula (6) is optimized as follows:

$$o\left(\sum_{l=1}^L \sum_{t=1}^T N * C_{l,t,in} * M_{l,t}^2 * W_{l,t,1}^2 * W_{l,t,2} * C_{l,t,out}\right). \quad (11)$$

Similarly, the parameter count of group CNN can be computed as follows:

$$o\left(\sum_{l=1}^L \sum_{t=1}^T N * C_{l,t,in} * M_{l,t} * W_{l,t,1} * C_{l,t,out}\right). \quad (12)$$

It can be seen that the FLOP and parameter count are determined not only by the number of the samples, the number of the convolutional layers, the number of the convolutional kernels per layer, the size of each convolutional kernel, and the number of the input and output convolution channels, but also by the number of groups.

Now, let us compare the FLOP and parameter count of group CNN with that of basic 1D CNN. From formula (7), formula (8), formula (11), and formula (12), we can find that there are many parameters to decide the FLOP and parameter count. We cannot compare them directly. But we can assume some comparison conditions. Because the length of input data in group CNN to that of basic 1D CNN is  $1/T$ , we assume that the length of convolutional kernels in each layer of group CNN to that of basic 1D CNN is  $1/T$ , that is,  $W'_1 = T * W_1$ . Similarly,  $W'_2 \approx T * W_2$ . According to the comparison of formula (7) and formula (11), it can roughly be seen that the FLOP of group CNN is smaller than that of 1D CNN. Similarly, according to the comparison of formula (8) and formula (12), it can roughly be seen that the parameter count of group CNN is smaller than that of 1D CNN. Actually, in experiments, we set completely different values of the parameters for the two models to achieve the best feature representation effect. More specifically, a comparison of the results are seen in Section 4.3.5.

**3.5. Shallow Machine Learning Classifier.** Shallow machine learning has good performance and high efficiency. Therefore, in this work, we use SVM as a shallow machine learning algorithm to build the classification model and identify the malicious samples in the dataset.

Shallow machine learning is consisted of two stages: training stage and testing stage [59]. In the training stage, the high-dimensional original dataset is reconstructed to the low-dimensional features by the training of the group CNN. Then, the dataset containing low-dimensional reconstruction features is input to the shallow machine learning classifier to train and obtain the optimal model structure. In the testing stage, the high-dimensional original testing dataset is input to the trained group CNN model to obtain the low-dimensional reconstructed features [60, 61]. Then, the dataset containing low-dimensional reconstructed features is input to the trained shallow machine learning classifier to get the labels of the predicted testing data.

In the experiment, the true labels of the testing dataset have been known, so the performance of the shallow machine learning models, such as accuracy, precision, recall, and F1, can be obtained by comparing the true labels with the predicted labels and calculating the confusion matrix.

The confusion matrix for binary classification includes four index items, such as true positive (TP), false negative (FN), false positive (FP), and true negative (TN). Then, other evaluation metrics as performance are defined as follows:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FN} + \text{FP} + \text{TN}}, \quad (13)$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}, \quad (14)$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}, \quad (15)$$

TABLE 1: Details of the datasets.

Dataset	Number of features	Number of samples (normal/abnormal)
KDDCUP99	41	10200 (5000/5200)
CICMalDroid2020-139	139	3795 (1795/2100)
CICMalDroid2020-470	470	3795 (1795/2100)

$$F1 = \frac{(1 + \beta^2) \times \text{precision} \times \text{recall}}{\beta^2 \times \text{precision} + \text{recall}} = \frac{2 \times \text{TP}}{2 \times \text{TP} + \text{FN} + \text{FP}} (\beta = 1). \quad (16)$$

## 4. Experiments

**4.1. Dataset.** The data come from the public datasets in cyberspace and contain the data of the network threat behavior. The details of the datasets are shown in Table 1.

KDDCUP99 [61] is the most famous and frequently cited dataset on intrusion detection. The whole dataset is very big and classified to 5 classes. In our work, we just randomly extract a small part, and only use them in 2 classes consisting of the normal and abnormal samples. The data set contains 41 features, which are divided into 4 categories: 9 basic features of the TCP, 13 content features of the TCP, 9 statistical features of the traffic based on time, and 10 statistical features of the traffic based on host.

CICMalDroid2020 [62] is downloaded from the website of Canadian Institute for Cybersecurity datasets. The original dataset contains 5 categories of Android samples. In our work, we just use the whole banking dataset, which contains 2100 malware samples, and the whole benign dataset, which contains 1795 benign samples. CICMalDroid2020-139 consists of 139 extracted features including the frequencies of system calls. CICMalDroid2020-470 consists of 470 extracted features including the frequencies of system calls, binders, and composite behaviors.

For most machine learning-based classification tasks, imbalanced datasets could cause the classification surfaces of the classifiers bias to the majority class, which leads to the misclassification of the minority class. Generally, the network threat data is treated as the minority class. Therefore, in our experiment, the ratios of “Normal” and “Abnormal” instances in all the three datasets are close to 1, which can void the imbalanced problem.

**4.2. Machine Learning Classifiers.** There are many shallow machine learning classifiers, e.g., NB, RF, and LR. Through our previous experimental results and analysis of the existing literature, we find that SVM is the most commonly used classifier.

SVM has many advantages: (1) It has good stability, which in many cases can maintain good classification performance. (2) It can deal with the noise and outlier data well by introducing relaxation variable. (3) It can effectively solve the problem of nonlinear and high-dimensional data. (4) It can keep good classification efficiency and effect for small data sets.



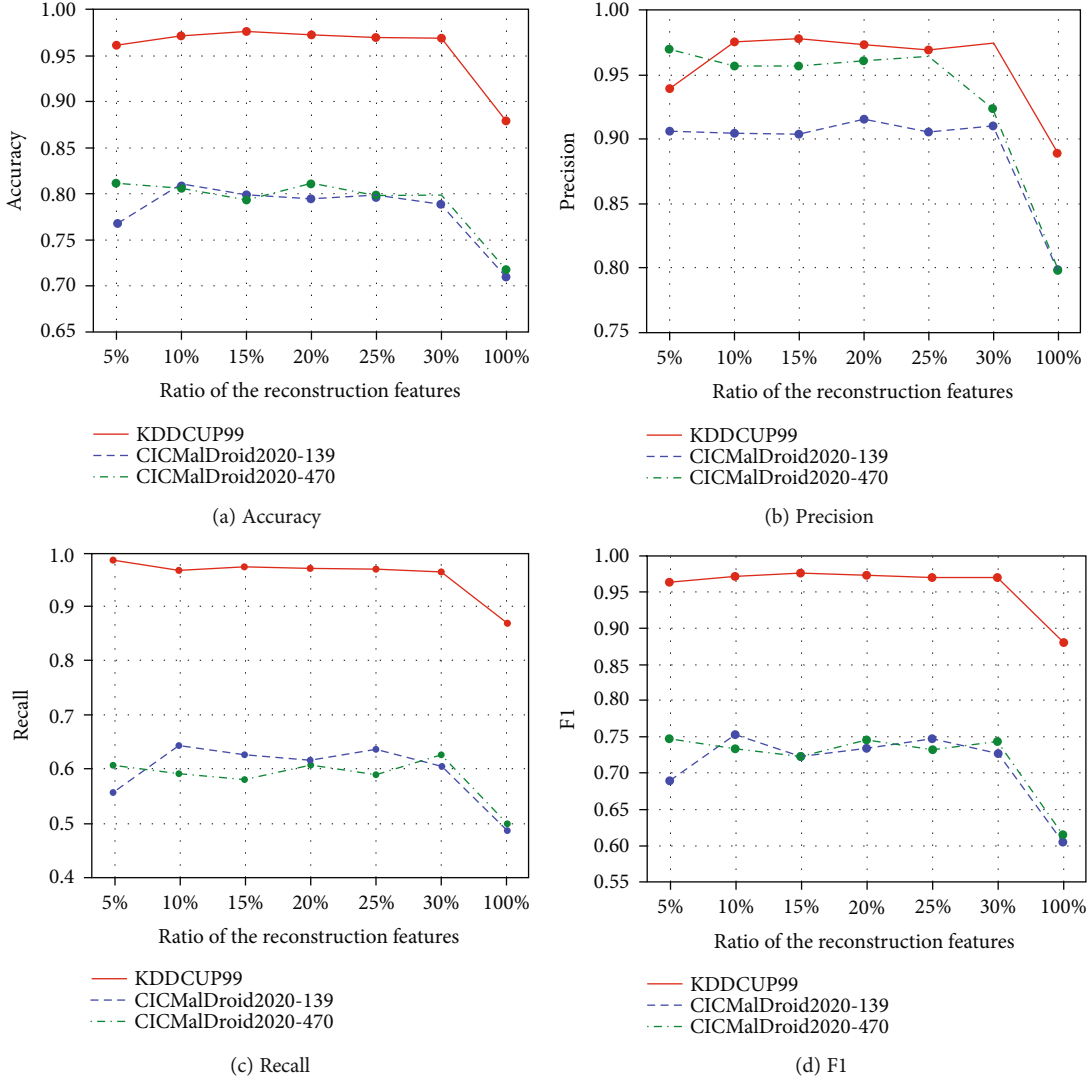


FIGURE 2: The performance of the reconstruct features at different ratios.

To sum up, combined with the characteristics of our dataset, which is high-dimensional and small, we choose SVM as the classifier in our experiment.

All experiments are performed in JetBrains PyCharm 2017 with Python 3.6 interpreter on a laptop Intel CORE i5-6200U 2.3 GHz with 8 GB RAM running the Windows 10 OS.

### 4.3. Experiment Results and Discussion

**4.3.1. Comparison of the Reconstructed Features.** In this section, the performances of the reconstructed features at different ratios are compared. According to the output size of the fully connected layer, the dimensions of the reconstructed features are different. In this section, to identify the performance of the reconstructed features, the lengths of the reconstructed features are set according to different situations. Specifically, the ratios of the reconstructed feature length to the original data length are set to 5%, 10%, 15%, 20%, 25%,

and 30%. First, the original data are input to group CNN models to generate the reconstructed features. Second, the data composed of reconstructed features are input to SVM, and then, the accuracy, precision, recall, and F1 are computed to evaluate the performance of the reconstructed features. The performances of the reconstructed features at different ratios are plotted in Figure 2. In addition, it should be noted that the number of iterations of the group CNN algorithms is 1000. The recorded results are the average of 5 experiments.

According to the curve of the performance of the reconstructed features at different ratios in Figure 2, including the accuracy, precision, recall, and F1, we can obtain some conclusions. First, the performances of the reconstructed feature data at some low ratios are better than those of the original data, whose ratio is 100%. In particular, the performances of the KDDCUP99 dataset are more obvious. Therefore, it is necessary to reduce the data dimensions by using the group CNN to reconstruct the features, which cannot reduce the

TABLE 2: The parameters of group CNN and basic 1D CNN network structures.

	Basic 1D CNN		Group CNN	
	KDD99	CICMaIDroid2020-139	CICMaIDroid2020-470	CICMaIDroid2020-139
Count of the convolution layers	3	4	5	4
Count of the pooling layers	0	3	2	3
Learning rate	0.0009	0.0009	0.0009	0.0009
Count of groups	1	1	1	2
Stride	1	1	1	1

TABLE 3: Accuracy of group CNN and basic 1D CNN.

(a) Accuracy of basic 1D CNN							
Datasets	Accuracy						
	5%	10%	15%	20%	25%	30%	100%
KDD99	0.9605	0.9566	0.9599	0.9627	<b>0.9667</b>	0.9548	0.8788
CICMalDroid2020-139	0.7760	<b>0.7854</b>	0.7721	0.7587	0.7733	0.7724	0.7094
CICMalDroid2020-470	0.6783	0.7065	0.6808	0.6320	0.6127	0.6246	<b>0.7171</b>

(b) Accuracy of group CNN							
Datasets	Accuracy						
	5%	10%	15%	20%	25%	30%	100%
KDD99	0.9612	0.9717	0.9724	<b>0.9764</b>	0.9696	0.9692	0.8788
CICMalDroid2020-139	0.7681	0.7988	<b>0.8091</b>	0.7945	0.7967	0.7891	0.7094
CICMalDroid2020-470	<b>0.8111</b>	0.8058	0.7937	0.8108	0.7985	0.7983	0.7171

data quality. Second, the higher the dimension of the original data is, the lower the ratio of the reconstruction features with better performance.

For example, KDDCUP99 is a low-dimension dataset, whose highest accuracy and F1 are at 15%. CICMalDroid2020-139 is a middle-high-dimensional dataset, whose highest accuracy and F1 are at 10%. Meanwhile, CICMalDroid2020-470 is a high-dimensional dataset, whose highest accuracy and F1 are at 5%. To sum up, we can conclude that reconstructed features are helpful to reduce the data dimensions and improve the performance.

#### 4.3.2. Comparison of the Group CNN and the Basic 1D CNN.

Both the group CNN and the basic 1D CNN can reconstruct features. In this part, we compare the performance of the reconstructed features by these two methods. First, the original data are input to group CNN and basic 1D CNN models, respectively. Different ratios from 5% to 30% of the reconstructed features are generated. Second, the data composed of reconstructed features are input to SVM, and the accuracy are computed to evaluate the performance of the reconstructed features. The parameters of their network structures are shown in Table 2. The performance of different ratios of the reconstructed features are recorded in Table 3. In addition, it should be noted that the number of iterations of the CNN algorithms is 1000. The recorded results are the average of 5 experiments.

The original data are directly input to SVM, and the accuracy is recorded in the last column of Tables 3(a) and 3(b). By contrast, the accuracy at different ratios from 5% to 30% of the reconstructed features are recorded in other columns. Comparing the results in Table 3(a), we find that in some situations the accuracy of the reconstructed features by the basic 1D CNN is higher than that of the original data. KDDCUP99 achieves the highest accuracy at 25%. CICMalDroid2020-139 achieves the highest accuracy at 10%. And CICMalDroid2020-470 achieves the highest accuracy with the original data. Comparing the results in Table 3(b), we find the accuracy of the reconstructed features

by the group CNN is higher than that of the original data. KDDCUP99 achieves the highest accuracy 0.9764 at 15%. CICMalDroid2020-139 achieves the highest accuracy 0.8091 at 10%. And CICMalDroid2020-470 achieves the highest accuracy 0.8111 at 5%. Comparing the results in Table 3(a) with that in Table 3(b), we find that the accuracy by the group CNN is generally higher than that by the basic 1D CNN. And the highest accuracy of each dataset in Table 3(b) by group CNN is higher than that in Table 3(a) by the basic 1D CNN. Furthermore, the datasets get the highest accuracy by the group CNN at the lower ratios. For example, KDDCUP99 gets the highest accuracy by the group CNN at 15%, but gets the highest accuracy by basic 1D CNN at 25%. Finally, we can conclude that the performance of the group CNN is better than that of basic 1D CNN mainly because grouped data based on the feature correlation helps to improve the inside stickiness of the data of each group.

#### 4.3.3. Training Loss of the Group CNN.

During training stage, the training loss is achieved based on the cross entropy loss function to compare the probability that the predicted labels of the reconstructed features are close to the real labels. The smaller the training loss is, the closer the predicted labels to the true labels of each data. In this section, we study the trend of the training loss of the group CNN. KDDCUP99 and CICMalDroid2020-139 are grouped to two groups, while CICMalDroid2020-470 is grouped to four groups. The grouped data are separately input to the group CNN to train the models. Then, different ratios from 5% to 30% of the reconstructed features are generated. During the training of the group CNN, the loss of each iteration is recorded and plotted in Figure 3. The number of iterations in the training stage is 1000.

From the curves in Figure 3, on the one hand, we find that some training loss curves of the grouped data are closer to each other and approaching to 0. For example, in Figure 3(a), the training loss curves of 20% reconstructed feature data of KDDCUP99, which are grouped to two groups, are closer. So are the training loss curves of 15%



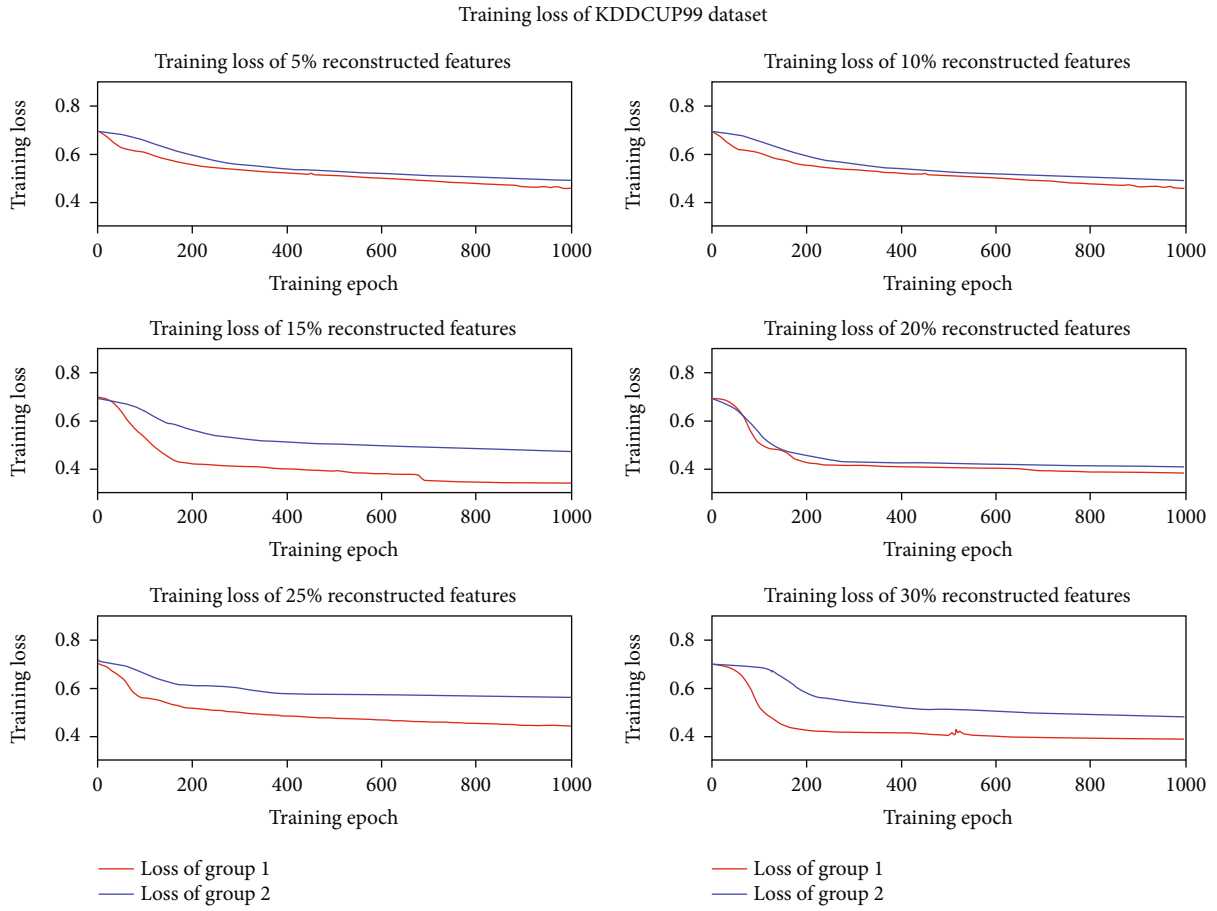
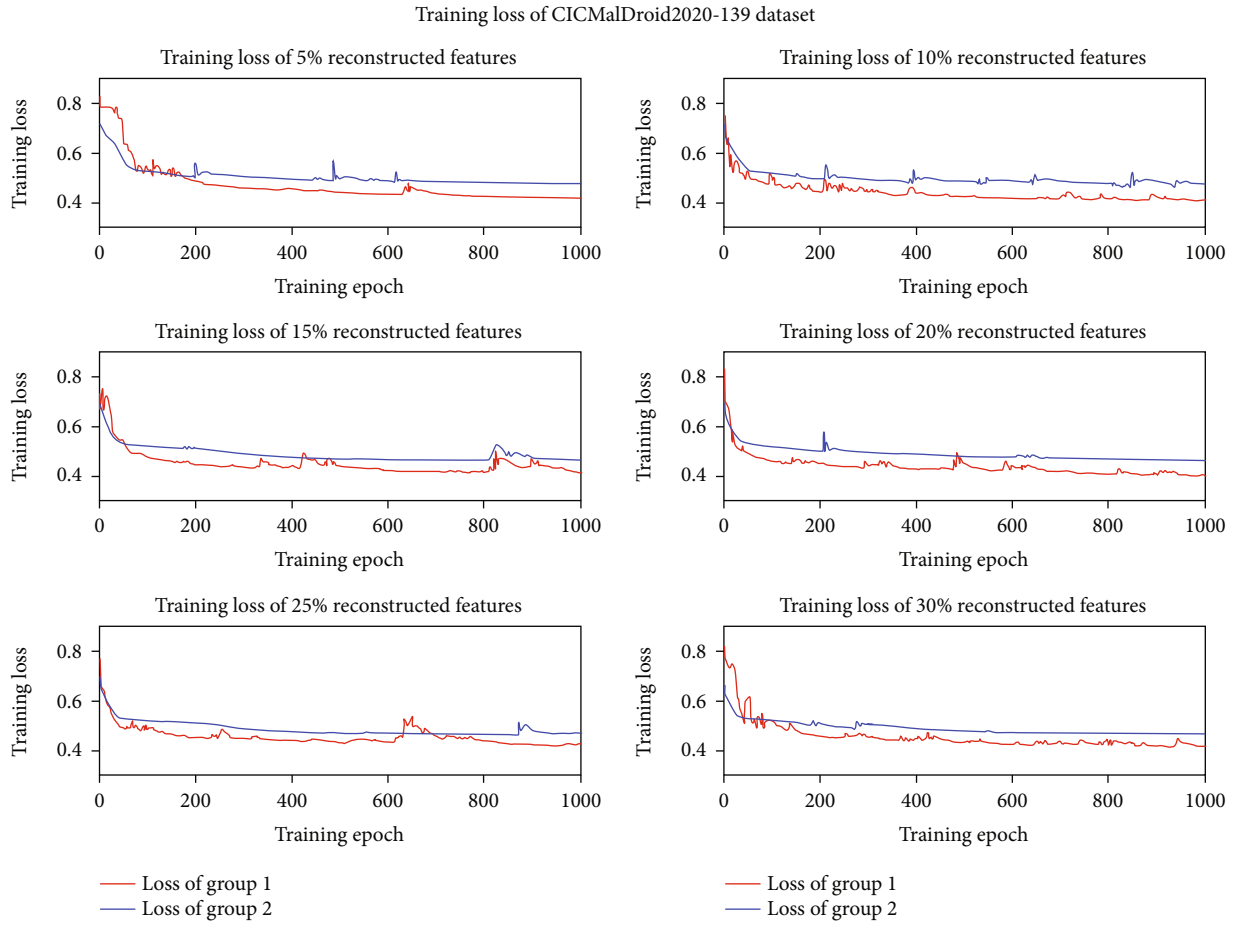


FIGURE 3: Continued.



(b) Training loss of CICMalDroid2020-139 by group CNN

FIGURE 3: Continued.

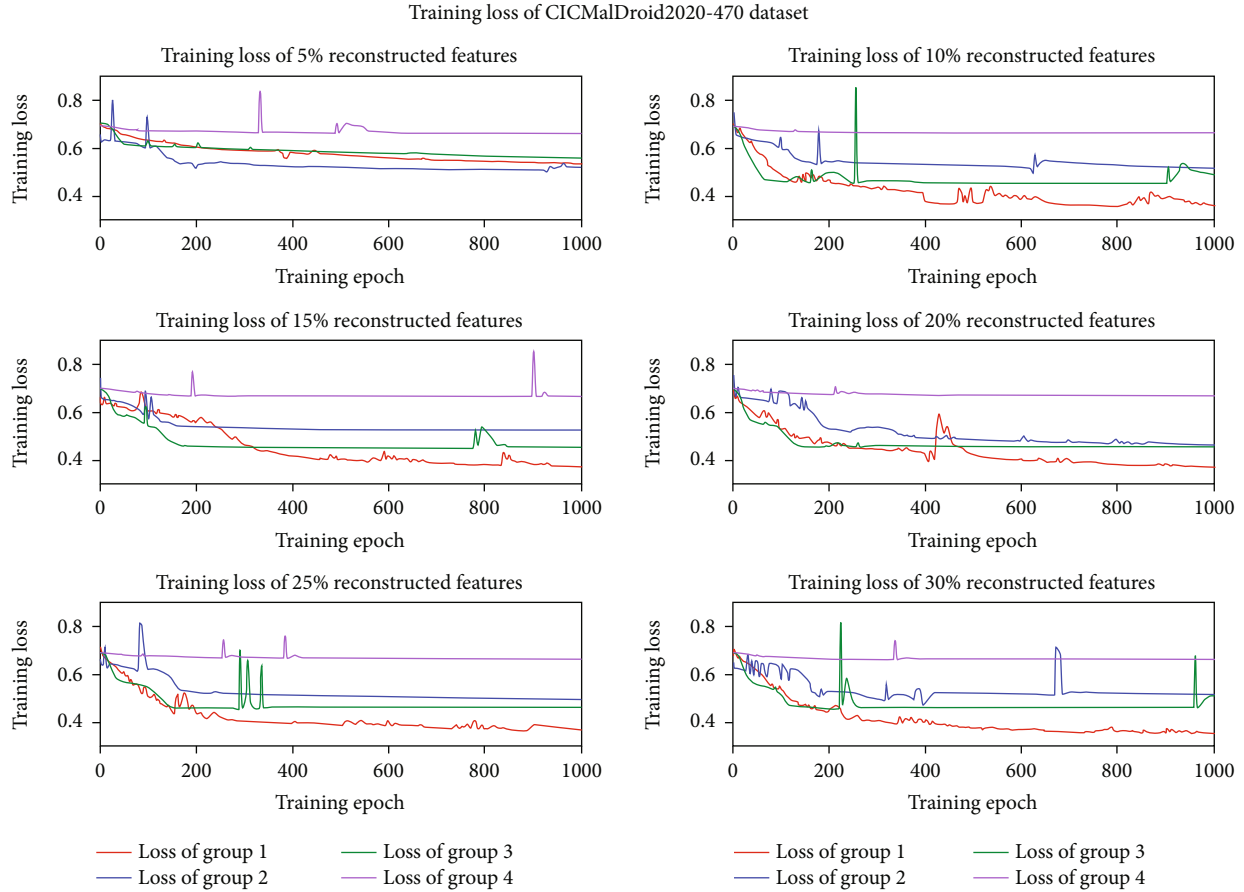


FIGURE 3: Training loss of group CNN.

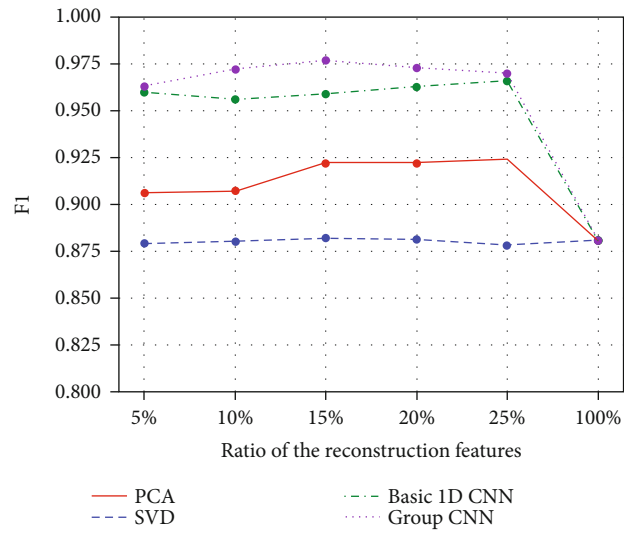
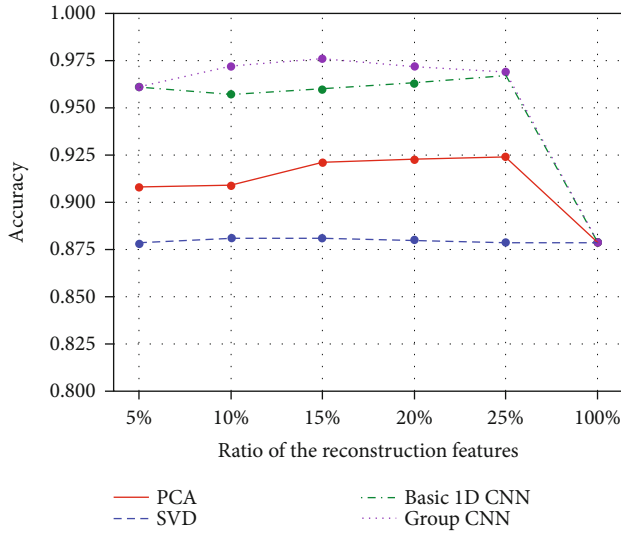
reconstructed feature data of CICMalDroid2020-139 in Figure 3(b), and the training loss curves of 5% reconstructed feature data of CICMalDroid2020-470 in Figure 3(c).

Furthermore, the ratios of the closer training loss curves in Figure 3 are the same as that of the highest accuracy in Table 3(a). On the other hand, we find that when the curves converge, the training loss curve of group 1 is under that of group 2 in Figures 3(a) and 3(b), and the loss curves are the same in Figure 3(c), where the loss curve of group 1 is at the bottom and the loss curve of group 4 is on the top. That is because the data are grouped based on the feature correlation. We first calculate the correlations between features, and rank the correlations in descending order. Then, we divide the data into several groups equally according to the descending correlation coefficients. So, the correlation coefficients of the first group are biggest, and that of the last group are smallest. Therefore, the loss of reconstructed features are smaller when the correlation coefficients are larger.

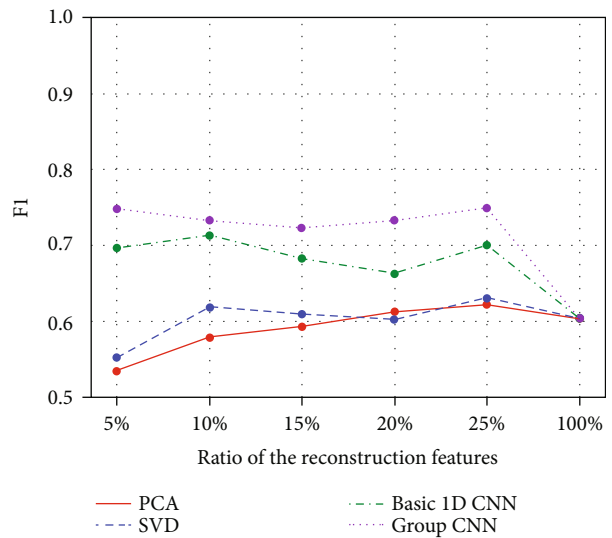
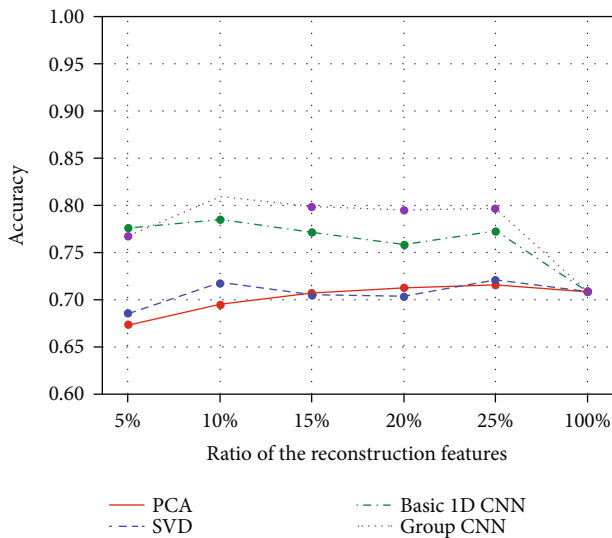
**4.3.4. Comparison of the Dimension Reduction Algorithms.** The group CNN can reconstruct features and reduce the dimensions of the features. Therefore, the group CNN can be seen as a dimension reduction algorithm. At present, there are many dimension reduction algorithms, such as PCA, FA, ICA, and SVD. In this section, we choose PCA and SVD to

compare with the basic 1D CNN and the group CNN. Like in Section 4.3.1, first, the dimensions of the original data by the dimension reduction algorithms are reduced to 5%, 10%, 15%, 20%, 25%, and 30%, separately. Then, the dimension reduction data are input to SVM. Accuracy and F1 are calculated to evaluate the performance of the low-dimensional data. The accuracy and F1 of the dimension reduction algorithms are recorded in Figure 4. In addition, it should be noted that the number of iterations of the basic 1D CNN and the group CNN algorithms are 1000. The recorded results are the average of 5 experiments.

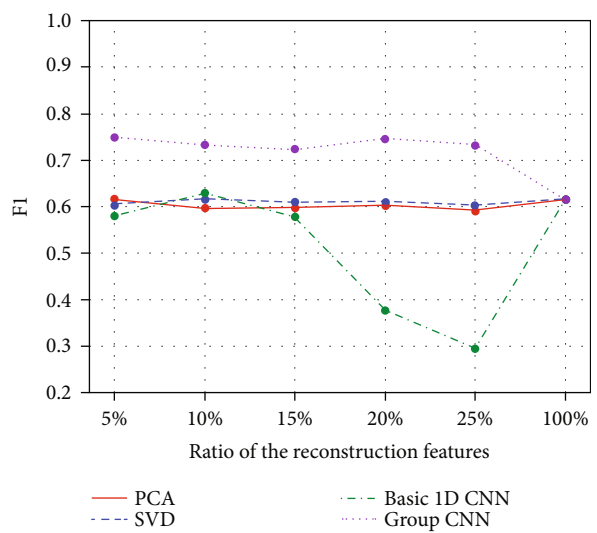
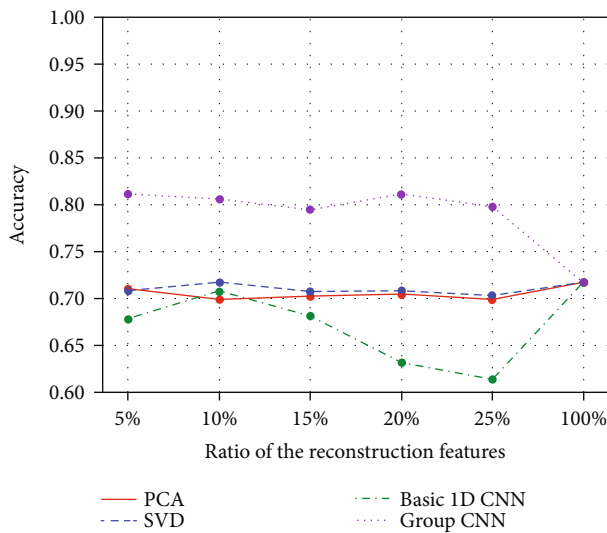
According to the accuracy and F1 of different dimension reduction algorithms in Figure 4, we can obtain some conclusions. First, for the low-dimensional dataset, such as KDDCUP99, the ratios of the highest accuracy and F1 are high. For the high-dimensional dataset, the ratios of the highest accuracy and F1 are low, such as CICMalDroid2020-470. Furthermore, the highest accuracy and F1 at the low ratios are even higher than that of the original data. Therefore, we think that it is quite necessary to reduce the data dimensions by the dimension reduction algorithms. Second, the accuracy and F1 of different ratios by the group CNN are the highest. Therefore, we can obtain that the group CNN is the best dimension reduction algorithm. At the same time, the accuracy and F1 of the basic 1D CNN are less than that of the



(a) The accuracy and F1 of KDDCUP99 by the dimension reduction algorithms



(b) The accuracy and F1 of CICMalDroid2020-139 by the dimension reduction algorithms



(c) The accuracy and F1 of CICMalDroid2020-470 by the dimension reduction algorithms

FIGURE 4: The accuracy and F1 of the dimension reduction algorithms.

TABLE 4: The structures, FLOP, parameter counts, and running time of the basic 1D CNN and the group CNN.

(a) The structures, FLOP, parameter counts, and running time of the basic 1D CNN								
Datasets	Structures of the basic 1D CNN	FLOP	Parameter counts	Running time (S)				
KDD99	Layers: 3 Layer 1: $C_{in} = 1, C_{out} = 40, M' = 40, W'_1 = 10, W'_2 = 32$ Layer 2: $C_{in} = 40, C_{out} = 40, M' = 40, W'_1 = 8, W'_2 = 25$ Layer 3: $C_{in} = 40, C_{out} = 80, M' = 80, W'_1 = 8, W'_2 = 18$	$4.63 * 10^9$	45700	602.68				
	CICMalDroid2020-139				Layers: 4 Layer 1: $C_{in} = 1, C_{out} = 30, M' = 30, W'_1 = 20, W'_2 = 128$ Layer 2: $C_{in} = 30, C_{out} = 20, M' = 20, W'_1 = 20, W'_2 = 109$ Layer 3: $C_{in} = 20, C_{out} = 40, M' = 40, W'_1 = 10, W'_2 = 100$ Layer 4: $C_{in} = 40, C_{out} = 20, M' = 20, W'_1 = 10, W'_2 = 91$	$6.69 * 10^9$	86798	852.84
					CICMalDroid2020-470			
(b) The structures, FLOP, parameter counts, and running time of the group CNN								
Datasets	Structures of the group CNN	FLOP	Parameter counts	Running time (S)				
KDD99	Groups: 2; layers: 3 Layer 1: $C_{in} = 1, C_{out} = 20, M' = 20, W'_1 = 5, W'_2 = 16$ Layer 2: $C_{in} = 20, C_{out} = 20, M' = 20, W'_1 = 4, W'_2 = 13$ Layer 3: $C_{in} = 20, C_{out} = 40, M' = 40, W'_1 = 4, W'_2 = 10$	$0.82 * 10^9$	13994	595.77				
	CICMalDroid2020-139				Groups: 2; layers: 4 Layer 1: $C_{in} = 1, C_{out} = 15, M' = 15, W'_1 = 10, W'_2 = 60$ Layer 2: $C_{in} = 15, C_{out} = 10, M' = 10, W'_1 = 10, W'_2 = 51$ Layer 3: $C_{in} = 10, C_{out} = 20, M' = 20, W'_1 = 5, W'_2 = 47$ Layer 4: $C_{in} = 20, C_{out} = 10, M' = 10, W'_1 = 5, W'_2 = 43$	$4.90 * 10^9$	61180	484.02
					CICMalDroid2020-470			

group CNN, but higher than that of PCA and SVD, which are traditional methods. Furthermore, we can conclude that the results of the deep learning methods are better than that of the traditional methods. Therefore, we suggest to apply deep learning algorithms to reduce the dimensions.

*4.3.5. Comparison of Running Time.* In theory, we have already proved that the parameter counts and FLOP of the group CNN are smaller than that of basic 1D CNN. In this section, we compare the values of FLOP, parameter counts, and running time between the basic 1D CNN and the group CNN. The basic 1D CNN and the group CNN are built with different structures to analyze the datasets. In particular, the numbers of layers and the parameters of each layer are shown in Table 4.

The basic 1D CNN and the group CNN have similar structures, when dealing with the same dataset. It should be noted that the count of convolutional kernels in each layer of the basic 1D CNN is equal to that of the group CNN, which means that the count of convolutional kernels in each layer of the basic 1D CNN is equal to the numbers of the groups multiplied by the counts of convolutional kernels in each group. When the models are operating to analyze the data, running time is recorded. At the same time, FLOP and parameters are computed. The results are shown in Table 4.

Table 4 shows the structures, FLOP, parameters, and running time of the basic 1D CNN and the group CNN. It is easy to find that the more layers of the structures have, the larger the FLOP, parameters, and running time in Table 4(a) and

Table 4(b). Furthermore, the FLOP, parameters, and running time of the group CNN in Table 4(b) are less than that of the basic 1D CNN in Table 4(a), when these two CNN models deal with the same datasets.

In particular, more FLOP, parameter counts, and running time of the group CNN on CICMalDroid2020-470 decrease, compared to that of the group CNN on KDD99 and CICMalDroid2020-139. Maybe, we can infer that the larger the group count is, the more FLOP, parameter counts, and running time reduce. It should be noted that the structures of the basic 1D CNN and the group CNN in this section are set to compare the running time, which are not used in other sections. On the contrary, in other sections, the structures of basic 1D CNN and group CNN are set to obtain the highest performance, which are totally different from that in this section.

## 5. Conclusions

In this paper, we present a 1D group CNN model to reconstruct the features and reduce the dimensionality. The main characteristic is that grouped data are based on feature correlations, which means that the data are grouped by column. CNN model grouping occurs in convolution kernel grouping. In summary, first, compared to all features, our group CNN can achieve the best performance with fewer features. Second, compared to the basic 1D CNN, the group CNN outperforms the basic 1D CNN on the features at different ratios. Third, compared to the dimension reduction algorithms, the accuracies and F1 of the group CNN are the highest. Fourth, compared to the basic 1D CNN, the FLOP, parameters, and running time of the group CNN are lower. Therefore, from the evaluations of all of the aspects, the group CNN spends less time but achieves better performance with fewer features.

## Data Availability

The datasets used to support the findings of this study can be downloaded from the public websites whose references are provided in this paper. And the datasets also are available from the corresponding author upon request.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This paper is supported by the Natural Science Foundation of Zhejiang Province (Nos. LY20F020012 and LQ19F020008), the National Natural Science Foundation of China (No. 61802094), Zhejiang Electronic Information Product Inspection and Research Institute (Key Laboratory of Information Security of Zhejiang Province), and Key Laboratory of Brain Machine Collaborative Intelligence of Zhejiang Province.

## References

[1] X. Zhou, W. Liang, Z. Luo, and Y. Pan, "Periodic-aware intelligent prediction model for information diffusion in social net-

works," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 894–904, 2021.

- [2] Z. Cai and Z. He, "Trading private range counting over big IoT data," in *The 39th IEEE International Conference on Distributed Computing Systems*, pp. 144–153, Dallas, TX, USA, 2019.
- [3] L. Qi, C. Hu, X. Zhang et al., "Privacy-aware data fusion and prediction with spatial-temporal context for smart city industrial environment," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 9, pp. 4159–4167, 2020.
- [4] X. Yan, Y. Xu, X. Xing, B. Cui, Z. Guo, and T. Guo, "Trustworthy network anomaly detection based on an adaptive learning rate and momentum in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6182–6192, 2020.
- [5] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.
- [6] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2018.
- [7] Y. Xu, C. Zhang, G. Wang, Z. Qin, and Q. Zeng, "A blockchain-enabled deduplicatable data auditing mechanism for network storage services," *IEEE Transactions on Emerging Topics in Computing*, 2020.
- [8] Y. Xu, Q. Zeng, G. Wang, C. Zhang, J. Ren, and Y. Zhang, "An efficient privacy-enhanced attribute-based access control mechanism," *Concurrency & Computation Practice & Experience*, vol. 32, no. 5, pp. 1–10, 2020.
- [9] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.
- [10] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, "Blockchain empowered arbitrable data auditing scheme for network storage as a service," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 289–300, 2020.
- [11] C. Zhang, Y. Xu, Y. Hu, J. Wu, J. Ren, and Y. Zhang, "A blockchain-based multi-cloud storage data auditing scheme to locate faults," *IEEE Transactions on Cloud Computing*, 2021.
- [12] Y. Xu, C. Zhang, Q. Zeng, G. Wang, J. Ren, and Y. Zhang, "Blockchain-enabled accountability mechanism against information leakage in vertical industry services," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1202–1213, 2021.
- [13] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: a survey," *Applied Sciences*, vol. 20, no. 9, p. 4396, 2019.
- [14] J. Cheng, J. Zheng, and X. Yu, "An ensemble framework for interpretable malicious code detection," *International Journal of Intelligent Systems*, 2020.
- [15] Y. Ye, T. Li, D. Adjeroh, and S. S. Iyengar, "A survey on malware detection using data mining techniques," *ACM Computing Surveys*, vol. 50, no. 3, pp. 1–40, 2017.
- [16] X. Yan, Y. Xu, B. Cui, S. Zhang, T. Guo, and C. Li, "Learning URL embedding for malicious website detection," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6673–6681, 2020.
- [17] S. M. Ghaffarian and H. R. Shahriari, "Software vulnerability analysis and discovery using machine-learning and data-mining techniques," *ACM Computing Surveys*, vol. 50, no. 4, pp. 1–36, 2017.



- [18] A. Khan, A. Sohail, U. Zahoor, and A. S. Qureshi, "A survey of the recent architectures of deep convolutional neural networks," *Artificial Intelligence Review*, vol. 53, no. 8, pp. 5455–5516, 2019.
- [19] X. Zhou, X. Xu, W. Liang et al., "Intelligent small object detection based on digital twinning for smart manufacturing in industrial CPS," *IEEE Transactions on Industrial Informatics*, 2021.
- [20] C. F. Tsai, Y. F. Hsu, C. Y. Lin, and W. Y. Lin, "Intrusion detection by machine learning: a review," *Expert Systems with Applications*, vol. 36, no. 10, pp. 11994–12000, 2009.
- [21] S. Maldonado, R. Weber, and F. Famili, "Feature selection for high-dimensional class-imbalanced data sets using support vector machines," *Information Sciences*, vol. 286, pp. 228–246, 2014.
- [22] R. K. Vigneswaran, R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Evaluating shallow and deep neural networks for network intrusion detection systems in cyber security," in *2018 9th International Conference on Computing, Communication and Networking Technologies*, Bengaluru, India, 2018.
- [23] S. Ansari, V. Bartos, and B. Lee, "Shallow and deep learning approaches for network intrusion alert prediction," *Procedia Computer Science*, vol. 171, pp. 644–653, 2020.
- [24] X. Zhou, X. Xu, W. Liang, Z. Zeng, and Z. Yan, "Deep learning enhanced multi-target detection for end-edge-cloud surveillance in smart IoT," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12588–12596, 2021.
- [25] Y. Liu, C. Wang, Y. Zhang, and J. Yuan, "Multiscale convolutional CNN model for network intrusion detection," *Computer Engineering and Applications*, vol. 55, no. 3, p. 90, 2019.
- [26] M. Sheikhan and Z. Jadidi, "Flow-based anomaly detection in high-speed links using modified GSA-optimized neural network," *Neural Computing and Applications*, vol. 24, no. 3-4, pp. 599–611, 2014.
- [27] X. Zhou, Y. Li, and W. Liang, "CNN-RNN based intelligent recommendation for online medical pre-diagnosis support," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 18, no. 3, pp. 912–921, 2021.
- [28] Y. Xu, X. Yan, Y. Wu, Y. Hu, W. Liang, and J. Zhang, "Hierarchical bidirectional RNN for safety-enhanced B5G heterogeneous networks," *IEEE Transactions on Network Science and Engineering*, 2021.
- [29] Z. Cai, Z. Xiong, H. Xu, P. Wang, W. Li, and Y. Pan, "Generative adversarial networks," *ACM Computing Surveys*, vol. 54, no. 6, pp. 1–38, 2021.
- [30] X. Zhou, W. Liang, S. Shimizu, J. Ma, and Q. Jin, "Siamese neural network based few-shot learning for anomaly detection in industrial cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5790–5798, 2021.
- [31] X. Yan, B. Cui, Y. Xu, P. Shi, and Z. Wang, "A method of information protection for collaborative deep learning under GAN model attack," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 18, no. 3, pp. 871–881, 2021.
- [32] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.
- [33] Q. Yang, W. Shi, J. Chen, and W. Lin, "Deep convolution neural network-based transfer learning method for civil infrastructure crack detection," *Automation in Construction*, vol. 116, no. 10, article 103199, 2020.
- [34] S. Kiranyaz, O. Avci, O. Abdeljaber, T. Ince, M. Gabbouj, and D. J. Inman, "1D convolutional neural networks and applications: a survey," *Mechanical Systems and Signal Processing*, vol. 151, p. 107398, 2021.
- [35] Q. Xiang, X. Wang, Y. Song, L. Lei, R. Li, and J. Lai, "One-dimensional convolutional neural networks for high-resolution range profile recognition via adaptively feature recalibrating and automatically channel pruning," *International Journal of Intelligent Systems*, vol. 36, no. 1, pp. 332–361, 2021.
- [36] S. Chen, J. Yu, and S. Wang, "One-dimensional convolutional auto-encoder-based feature learning for fault diagnosis of multivariate processes," *Journal of Process Control*, vol. 87, pp. 54–67, 2020.
- [37] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," *Advances in Neural Information Processing Systems*, vol. 25, pp. 1097–1105, 2012.
- [38] T. Zhang, G. J. Qi, B. Xiao, and J. Wang, "Interleaved group convolutions for deep neural networks," *ICCV*, vol. 1707, 2017.
- [39] Y. Lu, G. Lu, R. Lin, J. Li, and D. Zhang, "SRGC-nets: sparse repeated group convolutional neural networks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 99, pp. 1–14, 2019.
- [40] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.
- [41] M. Kruczkowski and E. N. Szyrkiewicz, "Support vector machine for malware analysis and classification," in *2014 IEEE/WIC/ACM International Joint Conferences on Web Intelligence and Intelligent Agent Technologies*, pp. 415–420, Warsaw, Poland, 2014.
- [42] L. Bilge, S. Sen, and D. Balzarotti, "Exposure: a passive DNS analysis service to detect and report malicious domains," *ACM Transactions on Information and System Security*, vol. 16, no. 4, pp. 1–28, 2013.
- [43] Y. Y. Aung and M. M. Min, "Hybrid intrusion detection system using K-means and classification and regression trees algorithms," in *2018 IEEE 16th International Conference on Software Engineering Research, Management and Applications*, pp. 195–199, Kunming, China, 2018.
- [44] A. Mo, K. Qader, and M. Alkasassbeh, "Comparative analysis of clustering techniques in network traffic faults classification," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 5, no. 4, pp. 6551–6563, 2017.
- [45] D. Abdelhafiz, C. Yang, R. Ammar, and S. Nabavi, "Deep convolutional neural networks for mammography: advances, challenges and applications," *BMC Bioinformatics*, vol. 20, no. 11, pp. 281–301, 2019.
- [46] Y. Xiao, C. Xing, T. Zhang, and Z. Zhao, "An intrusion detection model based on feature reduction and convolutional neural networks," *IEEE Access*, vol. 7, pp. 42210–42219, 2019.
- [47] Y. Wang, J. An, and W. Huang, "Using CNN-based representation learning method for malicious traffic identification," in *2018 IEEE/ACIS 17th International Conference on Computer and Information Science*, pp. 400–404, Singapore, Singapore, 2018.

- [48] J. Zhang, Z. Qin, H. Yin, L. Ou, and K. Zhang, "A feature-hybrid malware variants detection using CNN based opcode embedding and BPNN based API embedding," *Computers & Security*, vol. 84, pp. 376–392, 2019.
- [49] J. Zhang, Z. Qin, H. Yin, L. Ou, S. Xiao, and Y. Hu, "Malware variant detection using opcode image recognition with small training sets," in *2016 25th International Conference on Computer Communication and Networks*, Waikoloa, HI, USA, 2016.
- [50] J. Yan, Y. Qi, and Q. Rao, "Detecting malware with an ensemble method based on deep neural network," *Security and Communication Networks*, vol. 2018, 16 pages, 2018.
- [51] C. Ma, X. Du, and L. Cao, "Analysis of multi-types of flow features based on hybrid neural network for improving network anomaly detection," *IEEE Access*, vol. 7, pp. 148363–148380, 2019.
- [52] M. Azizjon, A. Jumabek, and W. Kim, "1D CNN based network intrusion detection with normalization on imbalanced data," in *2020 International Conference on Artificial Intelligence in Information and Communication*, pp. 218–224, Fukuoka, Japan, 2020.
- [53] W. Wei, Q. Ke, J. Nowak, M. Korytkowski, R. Scherer, and M. Woźniak, "Accurate and fast URL phishing detector: a convolutional neural network approach," *Computer Networks*, vol. 178, p. 107275, 2020.
- [54] H. Zhang, L. Huang, C. Q. Wu, and Z. Li, "An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset," *Computer Networks*, vol. 177, p. 107315, 2020.
- [55] S. Xie and R. Girshick, "Aggregated residual transformations for deep neural networks," in *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Honolulu, USA, 2016.
- [56] M. D. Zeiler and R. Fergus, *Visualizing and Understanding Convolutional Neural Networks*, Springer International Publishing, 2013.
- [57] Y. Zhang, T. Shen, X. Ji, Y. Zhang, R. Xiong, and Q. Dai, "Residual highway convolutional neural networks for in-loop filtering in HEVC," *IEEE Transactions on Image Processing*, vol. 27, no. 8, pp. 3827–3841, 2018.
- [58] M. E. Paoletti, J. M. Haut, X. Tao, J. Plaza, and A. Plaza, "FLOP-reduction through memory allocations within CNN for hyperspectral image classification," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 1109, no. 10, pp. 5938–5952, 2020.
- [59] X. Zhou, Y. Hu, W. Liang, J. Ma, and Q. Jin, "Variational LSTM enhanced anomaly detection for industrial big data," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3469–3477, 2021.
- [60] X. Yan, J. Zhang, H. Elahi, M. Jiang, and H. Gao, "A personalized search query generating method for safety-enhanced vehicle-to-people networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 5296–5307, 2021.
- [61] S. Hettich and S. D. Bay, *KDD Cup 1999 Data*, The UCI KDD Archive, 1999.
- [62] S. Mahdaviifar, A. Kadir, R. Fatemi, D. Alhadidi, and A. A. Ghorbani, "Dynamic android malware category classification using semi-supervised deep learning," in *2020 IEEE Int'l. Conf. on Dependable, Autonomic and Secure Computing, Int'l. Conf. on Pervasive Intelligence and Computing, Int'l. Conf. on Cloud and Big Data Computing, Int'l. Conf. on Cyber Science and Technology Congress (DASC/PiCom/CBDCOM/CyberSciTech)*, pp. 515–522, Calgary, AB, Canada, 2020.

## Research Article

# Blockchain-Based Privacy Protection Scheme for IoT-Assisted Educational Big Data Management

Xiaoshuang He <sup>1</sup>, Hechuan Guo <sup>2</sup>, and Xueyu Cheng <sup>3</sup>

<sup>1</sup>School of Education, Tianjin University, Tianjin, China

<sup>2</sup>School of Computer Science and Technology, Shandong University, Qingdao, China

<sup>3</sup>Rizhao Lanshan Experimental Middle School, Rizhao, China

Correspondence should be addressed to Hechuan Guo; ghc@mail.sdu.edu.cn

Received 16 June 2021; Accepted 21 July 2021; Published 15 August 2021

Academic Editor: Zhuojun Duan

Copyright © 2021 Xiaoshuang He et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Adoption of the Internet of Things (IoT) in education brings many benefits. However, the poor implementation of access control of educational data produced by the IoT devices has brought students' and teachers' privacy into danger. Attackers can access educational data that they are not permitted to access and even erase the records during access. To tackle this problem, we employ blockchain technology to guarantee the integrity of access control rules and trace the records of access events. In this paper, we propose a blockchain-based access control scheme for the data produced by IoT devices. The scheme consists of three components: (1) a well-implemented data collection module that is deployed in smart classrooms, which collects and uploads data about the real-time situation inside the smart classroom to the data center; (2) a MongoDB-based data center and its control module that makes access control decisions based on the verification of the permissions of visitors, where the permissions are managed by blockchain; and (3) a customized blockchain system that stores and keeps security policy updates of the role-based access control module and records access events in a trusted way. Our analysis indicates that the proposed access control scheme guarantees the correctness of the access control process and makes the access of collected educational data auditable and responsible. Our system collectively analyzes the context of the smart classroom and is capable of detecting multiple scenarios such as absence, lateness, and gunshot. We show how the scheme preserves students' and teachers' privacy by carrying out extensive experimental studies. The results indicate that the proposed data management system can give correct responses as quickly as a traditional data server does while preserving privacy.

## 1. Introduction

With the rapid development of Internet of Things (IoT), cities around the world are becoming smarter and smarter. One of the most widespread application scenarios of smart city is smart education, where educational big data is collected through multiple IoT devices deployed in smart campuses and smart classrooms and stored for a variety of data processing and analysis tasks.

Adoption of IoT in education has been widely studied. Marquez et al. [1] proposed a model to integrate objects to Virtual Academic Communities (VAC). Their results indicate that the adoption of IoT yields a more engaging learning environment for learners, and the instructors can obtain more information about the learning process, which in turn

enhances the pedagogical process. Moreira et al. [2] conducted a study to provide personalized education to learners by using the data collected through IoT, cloud computing, and learning analytical tools. It is indicated that this approach is able to provide personalized curricula that depend on the abilities of each student. Last but not least, Bagheri and Movahed [3] showed that the use of IoT in education is not limited to teaching and learning. Their study indicated that IoT in education can be used to (1) manage energy and monitor ecosystem; (2) implement secure campus and classroom access control; and (3) monitor student's health. In one word, adoption of IoT in education brings many benefits.

However, the access of the educational data produced during the work flow of these applications is not carefully controlled. Particularly, the privacy of the involved teachers

and students is in danger of being violated. There exist many instances demonstrating the severity. Here are a couple of examples. InBloom was a nonprofit educational technology company, which developed educational technology products to provide students with personalized learning services. But inBloom survived only 15 months. The main reason lies in that the information collected by the company involves too much privacy of students, and the company shared these data with other companies. Eventually, public protests and pressure from public opinion caused the company to apologize and shut down [4]. In September 2016, a high school student in Tianjin broadcasted the scenes of her classmates' learning, breaks, outdoor activities, etc., on a live broadcast platform, without the attention of her classmates. There were hundreds of people viewing the live broadcast, and some of them posted explicit information and messages, which include the personal information of the students [5].

As more and more schools are in progress of having smart campuses and smart classrooms, more and more IoT devices are used by students and teachers to interact. The involved privacy problems brought by IoT urge to be solved, which can be summarized as follows:

- (1) The uses of the sensors and the data produced by the sensors are unlimited. Access control schemes of the educational data are not well implemented. Attackers can cross the access restrictions by tampering with the access rules using methods such as SQL injection
- (2) The access of the data is not auditable. Attackers can erase the records of their visits using simple methods

To address these issues, we propose a blockchain-based access control scheme to ensure that the probability at which an adversary successfully accesses the data is a negligible probability. Our scheme consists of (1) a well implemented data collection module that is deployed in smart classrooms to collect and upload data to the data center; (2) a MongoDB-based data center and its control module that checks permissions on the blockchain and implements the results of the permissions; and (3) a role-based access control module maintained by a customized blockchain system that manages the access permissions and records access events in a trusted way.

The contributions of this paper are summarized as follows:

- (1) We propose an educational data access control scheme to support trustworthy educational data management. We use blockchain as a trusted, distributed database to store and keep the updates of the security policies involved in the role-based access control scheme, thus achieving secure and trusted data management. We illustrate that our scheme is effective to preserve privacy for IoT-assisted educational big data management. By using blockchain to record the visit events of educational data, we make the access of educational data auditable
- (2) We fully implement an educational data collection and access control system. The system includes a data

collection module deployed in a smart classroom, a MongoDB-based data center and its control module, and a role-based access control module running on top of a customized blockchain system. Our system collectively analyzes the context of the smart classroom and can detect multiple scenarios such as absence, lateness, and gunshot

- (3) We test the correctness and performance of our system. The results indicate that our system gives correct responses to users in less than one second, which is an acceptable performance for most application scenarios

The paper is organized as follows. Background and related works are presented in Section 2. Our blockchain-enabled access control scheme for educational data is proposed in Section 3. Experimental studies are reported in Section 4, and the paper is concluded in Section 5 with a discussion.

## 2. Previous Knowledge and Related Work

*2.1. Previous Knowledge.* Here, we introduce the key technologies and their related concepts used in our work.

*2.1.1. Role-Based Access Control.* We use the role-based access control (RBAC) model to represent and manage access privileges of the educational data. Role-based access control is a policy-neutral access-control mechanism defined around roles and privileges. Within an organization, users are grouped into different roles. The permissions to access certain series of data or to perform certain operations are assigned to specific roles rather than specific users. RBAC play a role as the bridge between users and permissions. A role represents a set of users and takes place of the users to be assigned permissions to, for simplification, clearance, and performance. In fact, there exist many other access control schemes such as attribute-based access control (ABAC), access control matrix (ACM), access control list (ACL), and capability-based access control (CapBAC). RBAC is proved to be equivalent to ACM with respect to the policies they can represent. Besides, RBAC is one of the most widespread, clear, and easy-to-develop access control models. The components of RBAC such as role-permission, user-role, and role-role relationships make it simple to perform user assignments, especially for user assignments on blockchain, because role-permissions, user-role, and role-role relationships are highly isomorphic with transactions on blockchain. And by maintaining RBAC with a blockchain system, we can guarantee that all access privileges are correctly stored and cannot be tampered with.

*2.1.2. Blockchain.* In our scheme, role-based access control is maintained by a blockchain system. Blockchain has served as a trustworthy environment for many different applications, ranging from secure transactions to trusted verifiable computing. Generally, blockchain can be regarded as a distributed ledger, which is kept by a series of computers called *blockchain nodes*. To make sure that every blockchain node keeps the same ledger, blockchain systems use *consensus*



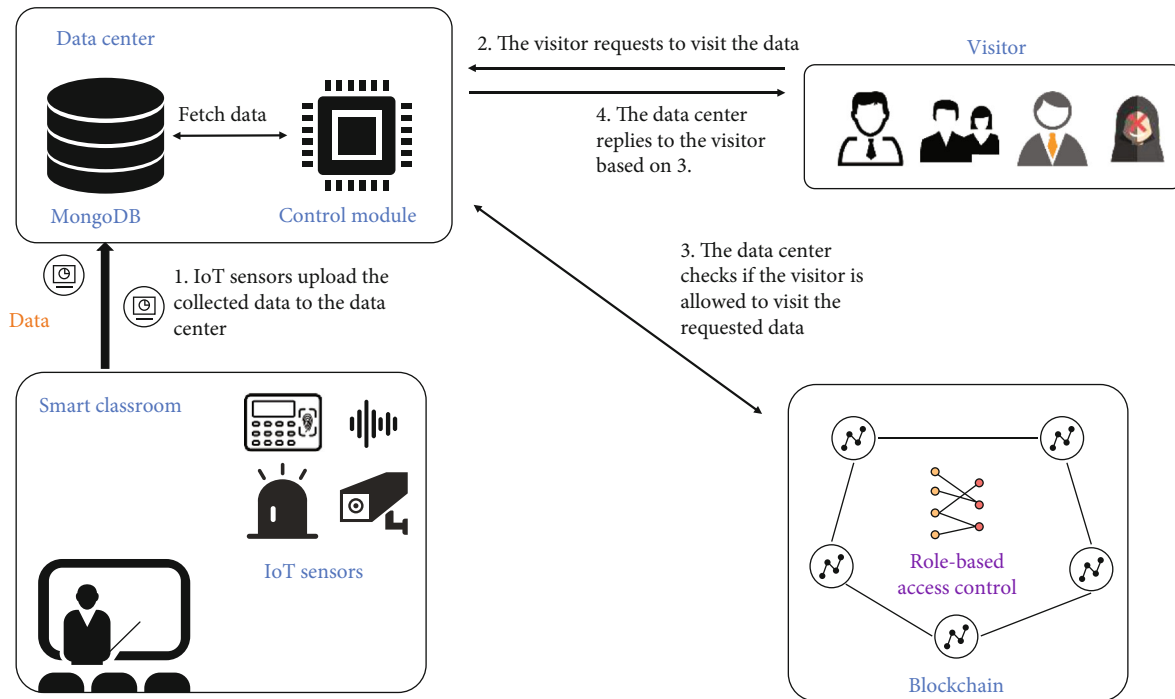


FIGURE 1: Abstract architecture of the system

algorithms. There are many kinds of consensus algorithms such as Proof-of-Work (PoW), Proof-of-Stake (PoS), and Delegated Proof-of-Stake (DPoS). Practical Byzantine Fault Tolerance (PBFT) represents the consensus algorithms from the Byzantine Fault Tolerance (BFT) consensus family. Although BFT consensus algorithms are well studied, their performance and scalability are still restricting their applications. In this paper, we choose PoW to be the consensus algorithm of our blockchain system. We make this choice for two reasons. On the one hand, PoW is the consensus algorithm for the first blockchain: bitcoin blockchain [6]. On the other hand, PoW is the most widely adopted consensus algorithm in blockchain community.

In blockchain, events recorded on the ledger are called *transactions*, and transactions are packed into blocks to be added to the end of the blockchain. In PoW, nodes compete to get the right of packing blocks. To get this right, nodes need to find a nonce, by appending the nonce to the block and calculating its hash; the outcome hash is smaller than a predefined threshold. This process is called *mining*. As the outcome of the hash process can be seen as completely random, the only way to find such a nonce is to guess and try. Then, we can expect that nodes need to try many times to find a valid nonce and add the block to the blockchain. In our experiment, the difficulty of finding a valid nonce was decreased to make the blockchain system run faster.

**2.2. Related Work.** Before cloud computing becomes prevalent, most information and data are stored locally in users' computers. As cloud computing and mobile network prevail, educational programs, applications, and data are stored in clouds, and users do not know the specific storage location of personal data. In [7], Madeth raised awareness of privacy

issues in E-learning that implicate user tracking and personal data usage for instructional purposes. In response to these privacy problems, a widely adopted method is to evaluate privacy-preserving technology of educational technology products. In fact, many schools and districts in the United States conducted privacy technology reviews on commonly used educational technology products with the help of technology review organizations [8]. The results indicate that most educational technology products cannot protect privacy. To solve the privacy problem fundamentally, a secure and trusted data management system is needed.

In fact, people have been trying to protect education privacy. Specifically, the main practices of American society to protect student privacy include three aspects: (1) publishing education privacy laws and regulations [9], (2) setting dedicated student privacy protection position at education departments [10], and (3) carrying out technical privacy reviews for educational products. At the technical level, preserving IoT data privacy in crowdsourcing with blockchain was studied by [11, 12]. Blockchain-based privacy preserving schemes on data uploading, trading, and sharing were explored by [13–15]. Blockchain systems addressing wireless challenges such as channel variation and adversarial jamming under IoT settings were thoroughly studied in [16, 17]. A cloud-enabled blockchain to support IoT applications taking advantage of the advances such as remote direct memory access and shared memory technology was presented in [18]. Trust extension from on-chain to off-chain and ground-truth data collection to blockchain were, respectively, investigated by [19, 20]. To the best of our knowledge, there is a lack of decentralized, trusted, automated access control solution to protect educational privacy, which is what this paper intends to address.



FIGURE 2: Data stored in data center.

### 3. Blockchain-Based Access Control of Educational Data

In this section, we describe the details of our blockchain-based access control scheme of educational data. As illustrated in Figure 1, our scheme consists of a smart classroom with IoT devices, a data center, and a role-based access control module running on a blockchain system.

**3.1. Smart Classroom.** IoT devices continuously monitor and collect data in smart classrooms. The collected data is uploaded to the data center for further processing and analysis. In this paper, our IoT devices include sound sensors, RFID sensors, and cameras. Sound sensors can be used to monitor whether most students are studying attentively or just chatting with each other. They can also be used as gunshot detectors, to set up alarm and notify the police when gunshot is detected. RFID sensors can be used to record attendance of teachers and students, by giving each teacher and student an RFID card. Cameras can take photos and videos of the interior of the classroom. They can be very useful, because based on Artificial Intelligence and Computer Vision technologies, photos and videos can be used to recognize human faces, analyze students' focus and emotion, and extract many other useful information.

For privacy concern, we use a sound detection module as the sound sensor. It only senses the sound intensity of the environment without collecting detailed sound information such as the timbre, frequency, phase or, any other information about the waveform. So, the content of conversations in the classroom is not recognized. The sound detection module outputs a value between 0 and 1023 representing

the current sound intensity in the environment. A larger output value means a louder environment. Particularly, as our experiment shows in Section 4, the output value ranges between 21 and 24 in a relatively quiet environment, and goes up to between 30 and 50 when a loud sound is detected.

Most schools, companies, and organizations use RFID sensors to take check-in and check-out records for their members. We do not explain how RFID sensors work here in detail, as it does not affect the design of our system. But we introduce how we use RFID sensors to collect important data. When a check-in action is detected (someone has tapped his/her RFID card or RFID tag at the RFID sensor), the user's RFID (usually a 4-byte array), the type of action (check-in or check-out), user's name, role, and the time and location of the action are collected. Besides, we calculate the SHA256 hash [21] of a record as its digest. Formally,

$$\text{Hash} = \text{SHA256}(\text{action} + \text{RFID} + \text{name} + \text{role} + \text{time} + \text{location} + \text{GPS}). \quad (1)$$

Using hash, we can setup a trusted digest to the activity, verify the integrity of data, and increase difficulty for attackers to tamper with the records.

All the collected data including sound, RFID records, and photos are uploaded and stored in the data center, for further processing and analysis.

**3.2. Data Center.** Collected educational data are stored in the data center. Teachers, parents of students, education managers, or someone else may need to access these data for different reasons, such as making educational decisions,



```

1: Initialization: Synchronize the blockchain object bc with blockchain nodes to get the newest state of the access model. Connect to
the MongoDB database and get an object db.
2: // verify the permission of an access request
3: function VERIFY(uid, hash, sig)
4:   // check if the user is offering correct signature to be identified as user uid
5:   if bc.verifySignature(uid, sig) == false then
6:     return false
7:   end if
8:   role = bc.getRole(uid)
9:   tags = bc.getTags(hash)
10:  for tag in tags do
11:    if bc.findState(role, tag) == false then
12:      return false
13:    end if
14:  end for
15:  for tag in tags do
16:    if bc.findState(role, tag) == true then
17:      return true
18:    end if
19:  end for
20:  return false
21: end function
22: function RUNSERVER
23:  while true do
24:    uid, hash, sig, addrFrom = getRequestParams()
25:    if verify(uid, hash, sig) == false then
26:      sendMessage("Authorization failed.")
27:    else
28:      sendMessage("Authorization succeed.")
29:      data = db.getData(hash)
30:      sendData(addrFrom, data)
31:    end if
32:  end while
33: end function

```

ALGORITHM 1: Data center control utilities.

TABLE 1: Access control rules in our experiment.

	Sound	Check-in & check-out	Camera
Students	✓	✗	✗
Parents	✓	✓	✗
Teachers	✓	✓	✓
Education managers	✓	✓	✓
Unauthorized people	✗	✗	✗

guarding safety of the school, and teaching enrichment. In our scheme, these educational data are stored in a MongoDB database.

MongoDB is a popular NoSQL, nonrelational database for modern app development [22]. When compared to relational databases, NoSQL databases are often more scalable and can provide superior performance. SQL databases are most often implemented in a scale-up architecture, which is based on larger computers with more CPUs and more memory to improve performance, while NoSQL databases are created in Internet and cloud computing eras that make it possible to more easily implement a scale-out architecture. In addition, the flexibility and ease of use of their data models

can speed up development in comparison to the relational model, especially in IoT and cloud computing environments.

In our design, the database stores three kinds of data: sound records, check-in and check-out records, and photo records. For a sound record, we store 5 fields: record hash, time, value, location, GPS: a check-in and check-out record contains 8 fields: record hash, action type, RFID, user's name, user's role, time, location, and GPS. And a photo record contains 5 fields: record hash, time, value, location, and GPS. Figure 2 shows one example of each kind of data.

We attach each record of data its hash as its index in both the data center and the blockchain. To protect privacy of students and teachers, access of these data should be under control. Data center should only allow authenticated access of designated data. In our access control scheme, we adopt the role-based access control model and deploy it on a customized blockchain system. When a visitor requests to access some data, the data center checks on the blockchain whether the visitor's role is allowed to access the requested data. If so, the data center grants to the visitor the access right to the data. Otherwise, the data center refuses the visitor's request. Based on this principle, we propose a control module of the data center to process visitors' access requests and verify

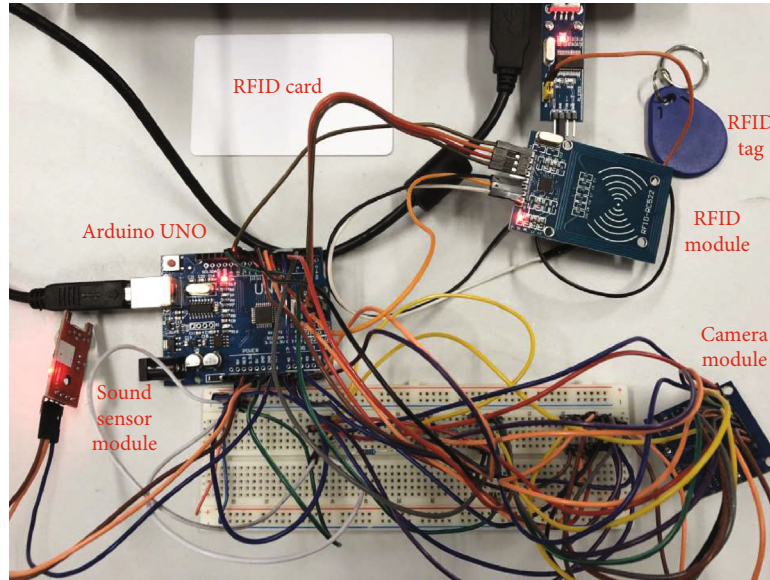


FIGURE 3: Data collection module deployment.

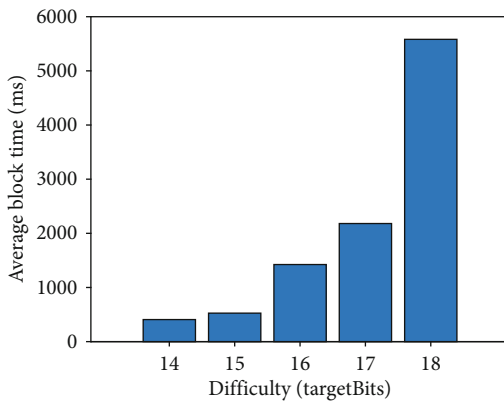


FIGURE 4: Average block time under different difficulty settings.

the permissions of visitors' access on the blockchain. Specifically, the control module is programmed to synchronize the state of RBAC module as a blockchain node and makes access control decisions based on the state of the RBAC module. Algorithm 1 shows the main frame of the control module's workflow.

In our implementation, the main thread of the control module runs the *runServer* function, which continuously waits for access requests. When receiving a request, *runServer* parses parameters of the request and verifies whether it is permitted or not, using the core part of the control module, *verify* function.

The *verify* function first checks the signature to make sure that the access request is sent by the corresponding user *uid*. Then, it extracts the tags of the data and examines the role of *uid*. Following that are two *for* loops, with the first one checking if the role of *uid* has been banned from some tag of the data and returns false if it is true and the second one checking if the role of *uid* has been authorized to access the data and returns true if it is true.

**3.3. RBAC Blockchain System.** As mentioned earlier, role-based access control (RBAC) is a policy-neutral access-control mechanism defined around roles and privileges. The components of RBAC such as role-permission, user-role, and role-role relationships make it simple to perform user assignments. A study by NIST has demonstrated that RBAC addresses many needs of commercial and government organizations. RBAC can be used to facilitate administration of security in large organizations with hundreds of users and thousands of permissions. Although RBAC is different from mandatory access control (MAC) and discretionary access control (DAC) frameworks, it can enforce these policies without any complication. Under the role-based access control model, users are grouped into several roles. Access actions of users are permitted or refused based on their roles.

For example, in our experiment described in Section 4, the roles and access control rules are designated as Table 1 shows. There are 5 roles in total: students, students' parents, teachers, education managers, and unauthorized people.

In our access control scheme, we use a blockchain system to implement the RBAC model. We authenticate user identities using SHA256 signatures and public cryptography schemes. The identities are registered on the blockchain via an authenticated trusted blockchain node. After registration, a public-private key pair is generated for each user, and the trusted node broadcasts a *user-registration* transaction on the blockchain. The transaction includes designated role for the user, and the public-private key pair can be used to verify whether the role in the transaction is designated to the user by verifying the SHA256 signature. To achieve role-based access control features, we implement 4 transaction types:

- (i) *User-registration*: as described above, we use *user-registration* transactions to register an identity for a user. The format of a user-registration transaction is  $\{user - reg, pk_{uid}, role\}$ , in which *uid* is the user's

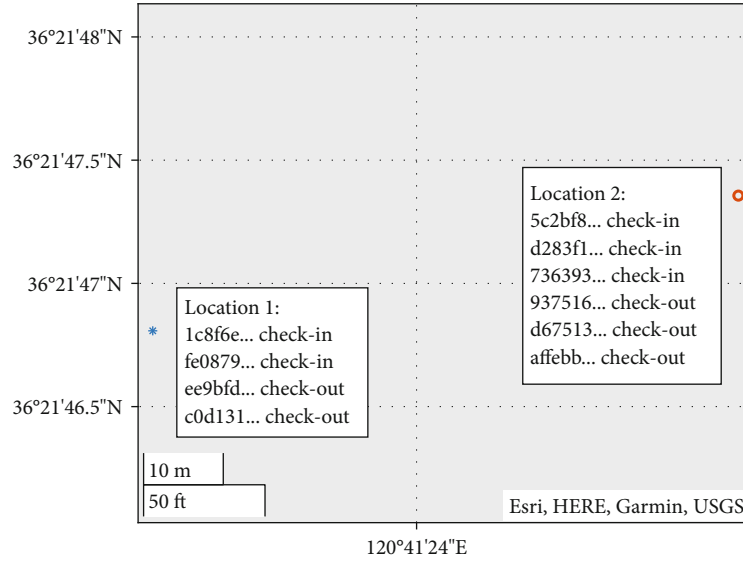


FIGURE 5: Check-in record.

TABLE 2: RFID record.

Record hash	Action	RFID	Name	Role	Time	Location	GPS
1c8f6e...	Check-in	E1 0D 2D 21	Teacher1	Teacher	08:05:17	Location 1	36.363, 120.689
fe0879...	Check-in	D1 D7 51 02	Teacher2	Teacher	08:05:26	Location 1	36.363, 120.689
5c2bf8...	Check-in	06 7F FB AD	Student1	Student	08:25:38	Location 2	36.363, 120.690
d283f1...	Check-in	82 3F B1 58	Student3	Student	08:25:43	Location 2	36.363, 120.690
736393...	Check-in	6D B6 6B 4A	Student2	Student	08:25:49	Location 2	36.363, 120.690
937516...	Check-out	6D B6 6B 4A	Student2	Student	17:01:23	Location 2	36.363, 120.690
d67513...	Check-out	06 7F FB AD	Student1	Student	17:01:48	Location 2	36.363, 120.690
affebb...	Check-out	82 3F B1 58	Student3	Student	17:01:59	Location 2	36.363, 120.690
ee9bfd...	Check-out	E1 0D 2D 21	Teacher1	Teacher	18:00:16	Location 1	36.363, 120.689
c0d131...	Check-out	D1 D7 51 02	Teacher2	Teacher	18:00:29	Location 1	36.363, 120.689

id,  $pk_{uid}$  is the public key generated for the user, and  $role$  is the designated role for the user

- (ii) *Role-registration*: like *user-registration* transactions, *role-registration* transactions are used to register a new role for the system. For a *role-registration* transaction  $\{role - reg, role\}$ ,  $role$  is the name of the role being registered
- (iii) *Rule-edit*: we use *rule-edit* transactions to create or edit role-based access control rules. For example, transaction  $\{rule - edit, role, tag, true/false\}$  creates or edits a rule to allow/forbid users of role  $role$  to access data with tag  $tag$
- (iv) *Access-result*: the blockchain system employs *access-result* transactions to respond to the data center's query about whether a user can access some data. Transaction  $\{result, uid, tag, t, true/false\}$  means the user of id  $uid$  can or cannot access the data of tag  $tag$ , where  $t$  is the timestamp of the request

action. *Access-result* transactions play the role of an immutable access log and make the request action auditable and responsible

The main benefit of running an RBAC model on a blockchain lies in that as all transactions are confirmed by all blockchain nodes, and no adversary can change any user's role at its own will.

## 4. Experiment

In this section, we report the evaluation results of our system in a practical scenario. We implemented the blockchain-based educational data access control system and used the system to perform the whole process of the educational data from collection, storage, to controlled access.

*4.1. Setup*. As shown in Figure 3, we used a data collection module to simulate the IoT devices in a smart classroom. The data collection module was implemented on an Arduino

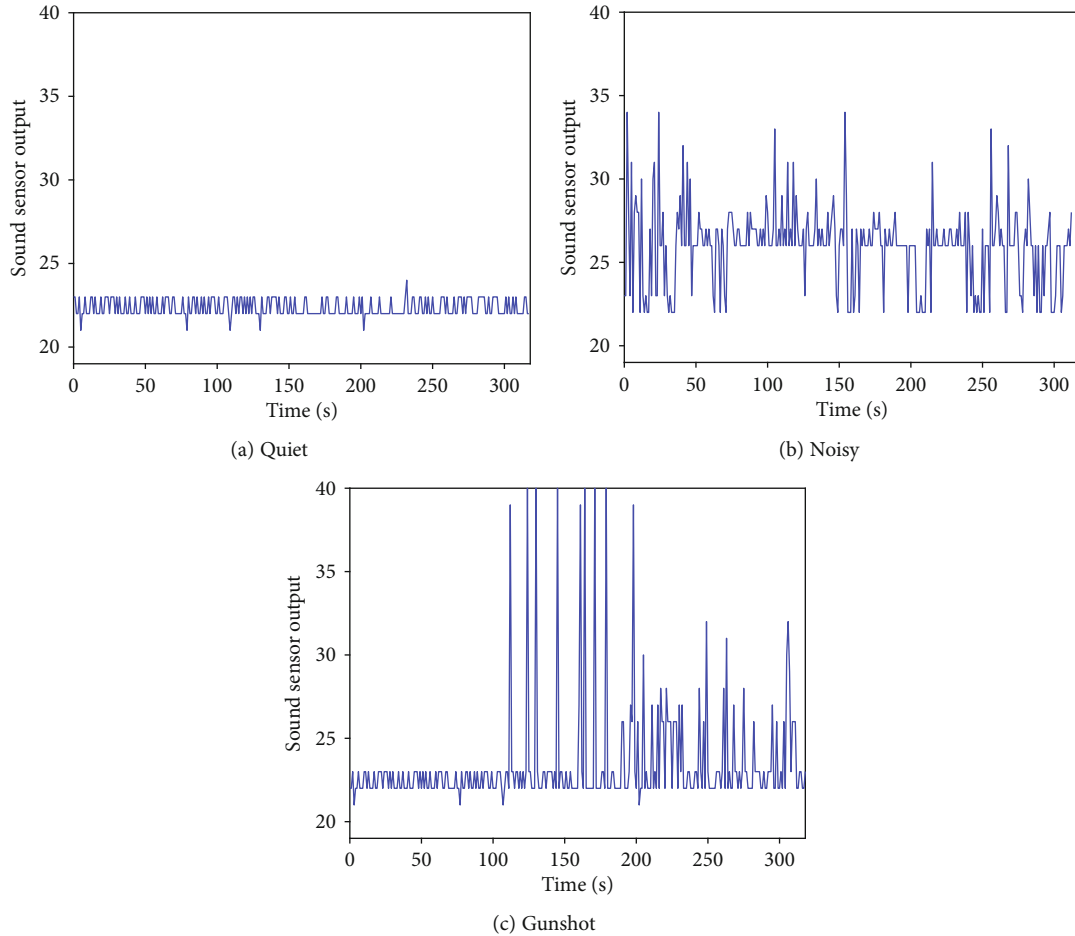


FIGURE 6: Sound monitoring.

UNO, which was connected to several sensor modules, including the following:

- (1) OV7670, a camera module
- (2) SY-M213, a sound sensor module
- (3) RFID-RC522, an RFID module

At the Arduino UNO, we develop and assemble the drivers of the camera module, sound sensor module, and RFID module in C language. The Arduino UNO board was a microcontroller board based on the ATmega328P, which supports USB connection with a computer [23]. At every second, the camera module uploaded a  $320 \times 240$ -sized grayscale image and the sound sensor module uploaded its output (it measures the sound intensity of the environment). The RFID module uploaded a record each time an action was detected.

All the collected data were uploaded to a Lenovo G580 PC running Windows 10 Professional 20H2 through serial port. We developed a Python program to display the data read from serial port. It ran on the Lenovo G580 PC and uploaded data to the data center while displaying the collected data.

For the data center, we developed a control module using Python to process visitors' access requests and verify the

authentication of visitors' access permissions on the blockchain. This module operated as both a server and a blockchain node. It read role-based access control information in on-chain transactions. If a visitor's access permission was authenticated, the control module would fetch data from the MongoDB database and send the data to the visitor by writing the data into the response body of the HTTPS connection. The control module and MongoDB ran on a 16-inch 2019 MacBook Pro with 8-Core Intel i9 @ 2.4GHz and 16GB memory that operated on macOS 11.3.

We developed our own blockchain system using Golang for the best flexibility of customization. Golang is a popular programming language in blockchain community and has become a go-to language for developing decentralized systems [24]. We used PoW consensus algorithm, which has practically the best performance and scalability. The PoW difficulty was reduced to 16 leading zero bits as we did not have as much computing power as the bitcoin network has to produce blocks in an acceptable time. That is, mining nodes needed to find a nonce that by appending the nonce to the block data, the produced SHA256 hash had 16 zero bits in the front. So, the expected try times of different nonces for mining a block were  $2^{16} = 65536$ . We ran the blockchain system on three computers, with each having 8-Core Intel i7-9700 CPU @ 3GHz and 16GB memory and running

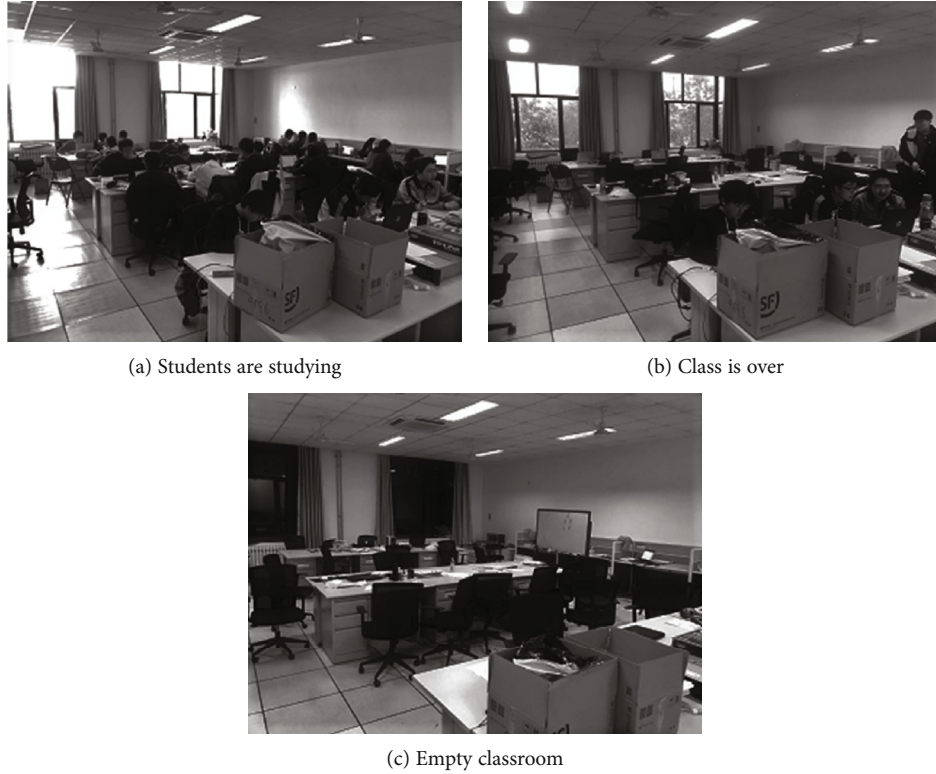


FIGURE 7: Camera recording.

Windows 10 Professional 20H2. One blockchain node ran on each of the three computers. Figure 4 shows the average time the blockchain network takes to mine a block, under different difficulty settings. In our implementation (targetBits = 16), the difficulty-reduced PoW blockchain network takes 526 ms to produce a block in average.

## 4.2. Evaluation

**4.2.1. Data Collection.** Using the RFID module, we recorded check-in and check-out actions at two different locations (shown in Figure 5). Each time a teacher or a student checks in (swipes his/her RFID card at the RFID sensor), information of his/her identity and the check-in and check-out action including time, location, and hash are collected and uploaded by the RFID module. In our experiment, location 1 is the office of the teacher, and location 2 is the classroom where the students study. Details of these actions are shown in Table 2.

In this experiment, we monitored the environment sound intensity in a classroom with the sound sensor module. As shown in Figure 6, three patterns of environment sound intensity were recorded. In the first pattern (Figure 6(a)), the classroom was relatively quiet, and the uploaded value from the sound sensor module was ranged from 21 to 24. In the second pattern (Figure 6(b)), the classroom was noisy, so the sound sensor module uploaded value higher than 25 with a high frequency. In the third pattern (Figure 6(c)), we simulated a gunshot scene with a loud speaker. From the 110 seconds to the 200 seconds, we used the speaker to play

gunshot sound at the entrance of the classroom. After the sound was played, from the 200 seconds, students in the classroom began to scream; then, the classroom became as noisy as it was in the second pattern.

We also used the camera module to take photos of the interior of the classroom. Limited by the performance of the OV7670 camera module, only one photo per second was taken. Figure 7 shows three representative scenes in the classroom: students studying in the classroom (Figure 7(a)), students leaving the classroom when the class was over while several students chose to stay for discussions (Figure 7(b)), and an empty classroom (Figure 7(c)).

These educational data were all uploaded and stored in the MongoDB database. Further analysis and data process can be done after access control.

**4.2.2. Access Control of Collected Data.** For simplicity and convenience, we ran the three nodes of the blockchain system, the data center, and the data collection module in the same local area network. This resulted in low network latency. By sending *role-registration* transactions and *user-registration* transactions, we registered 8 users of 5 roles: 3 students, 2 parents, 1 teacher, 1 education manager, and 1 unauthorized person. By sending *rule-edit* transactions, we created the following role-based access control rules:

- (i) Students can access the sound monitor data, to get noticed when gunshot is detected
- (ii) Parents can access the check-in records of their children and the sound monitor data, to see if their



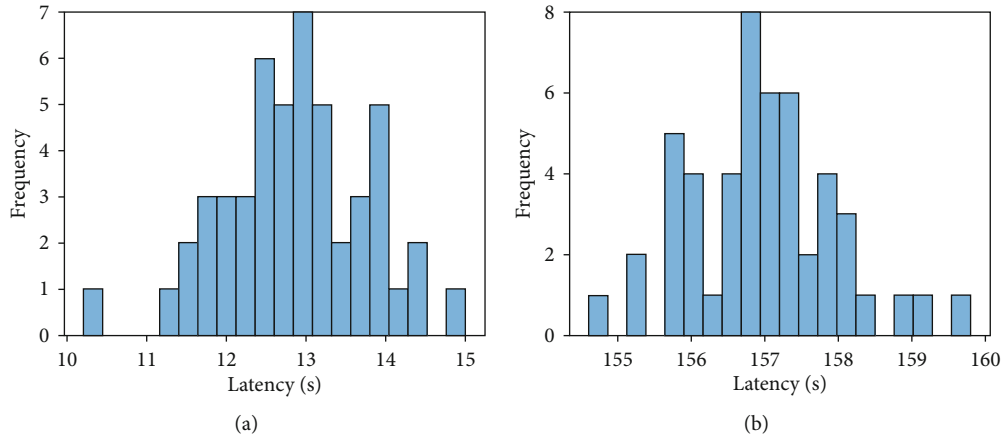


FIGURE 8: Response latency.

children have gone to school after leaving home and to be aware of students' study environment

- (iii) The teacher and the education manager can access all the educational data, for teaching evaluation and enrichment, educational decision making, school safety guarding, etc.
- (iv) The unauthorized person cannot access any data, as he or she is not authorized

Then, we tested our educational data access control system. We used different  $uid-sk_{uid}$  pairs to simulate different users and sent requests to the data center to access the data collected from the smart classroom. We sent 100 requests, 50 of them were good ones that should be accepted, while the other 50 were bad that should be refused. As a result, our access control system worked correctly. That is, for all the 50 good requests, the data center sent data to the user, and for all the 50 bad ones, the data center refused to offer data to the requester. Besides, the result of each request was logged on the blockchain in the form of an *access-result* transaction. We also analyzed the performance of our access control system. In our observation, it costs the user 13 ms in average to get a refuse message (Figure 8(a)) or 157 ms in average to get the requested data (Figure 8(b)), counting from sending a request to the data center. It can be concluded that the response time of our educational data access control system under local area network is acceptable.

## 5. Conclusions

In this paper, we proposed a scheme to preserve privacy in educational application of IoT. We achieved our privacy preservation goal by implementing a blockchain-based access control system. We implemented the full system including the components of collecting educational data, storing the data in a data center, and maintaining a role-based access control on educational data. Our scheme consists of a data collection module, a MongoDB-based data center, and the role-based access control module running on top of a blockchain system. Our educational data access control system

guarantees correct execution of the access control rules and makes the access events of educational data auditable and responsible. Our experiment results indicate that our access control system gives a correct response as quickly as a traditional data server. What is more, our access control system was designed to be relatively general-purpose. So, it can be easily extended to other application fields, by including necessary IoT devices and implementing drivers for them.

## Data Availability

The recorded data used to support the findings of this study are included within the article.

## Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

## References

- [1] J. Marquez, J. Villanueva, Z. Solarte, and A. Garcia, "Iot in education: integration of objects with virtual academic communities," in *New Advances in Information Systems and Technologies*, Á. Rocha, A. M. Correia, H. Adeli, L. P. Reis, and M. M. Teixeira, Eds., vol. 444, pp. 201–212, Springer International Publishing, 2016.
- [2] F. Moreira, M. J. Ferreira, and A. Cardoso, "Higher education disruption through IoT and big data: a conceptual approach," in *Learning and Collaboration Technologies. Novel Learning Ecosystems*, P. Zaphiris and A. Ioannou, Eds., pp. 389–405, Springer International Publishing, 2017.
- [3] M. Bagheri and S. H. Movahed, "The effect of the Internet of Things (IoT) on education business model," in *2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, pp. 435–441, Naples, Italy, 2016.
- [4] Parent Coalition for Student Privacy, *inBloom Timeline*, vol. 1, 2021, <https://studentprivacymatters.org/inbloom-timeline/>.
- [5] The Beijing News, *Senior high school girls were interviewed for live broadcast, claiming to be early adopters*, vol. 1, 2021,

- [http://epaper.bjnews.com.cn/html/2016-09/04/content\\_650845.htm?div=1](http://epaper.bjnews.com.cn/html/2016-09/04/content_650845.htm?div=1).
- [6] N. Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Decentralized Business Review*, vol. 1, p. 21260, 2008.
  - [7] M. May and S. George, "Privacy concerns in e-learning: is using tracking system a thread?," *International Journal of Information and Education Technology*, vol. 1, no. 1, 2011.
  - [8] Common Sense, "2019 State of Edtech Privacy Report," vol. 1, 2019.
  - [9] U.S. Department of Education, *Department of Education's Computer Matching Agreements*, vol. 1, 2021, <https://www2.ed.gov/about/offices/list/om/pirms/cma.html>.
  - [10] Chief Privacy Officer U.S. Department of Education.
  - [11] S. Zhu, Z. Cai, H. Hu, Y. Li, and W. Li, "zkCrowd: a hybrid blockchain-based crowdsourcing platform," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4196–4205, 2020.
  - [12] S. Zhu, W. Li, H. Li, L. Tian, G. Luo, and Z. Cai, "Coin hopping attack in blockchain-based IoT," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4614–4626, 2019.
  - [13] Z. Cai and Z. He, "Trading private range counting over big IoT data," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 144–153, Dallas, TX, USA, 2019.
  - [14] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.
  - [15] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.
  - [16] M. Xu, C. Liu, Y. Zou, F. Zhao, J. Yu, and X. Cheng, "wChain: a fast fault-tolerant blockchain protocol for multihop wireless networks," *IEEE Transactions on Wireless Communications*, p. 1, 2021.
  - [17] M. Xu, F. Zhao, Y. Zou, C. Liu, X. Cheng, and F. Dressler, "BLOWN: a blockchain protocol for single-hop wireless networks under adversarial SINR," *arXiv:2103.08361*, vol. 1, 2021.
  - [18] M. Xu, S. Liu, D. Yu, X. Cheng, S. Guo, and J. Yu, "Cloud-Chain: a cloud blockchain using shared memory consensus and RDMA," *arXiv:2106.04122*, vol. 1, 2021.
  - [19] C. Liu, H. Guo, M. Xu et al., "Extending on-chain trust to off-chain-a trustworthy vaccine shipping example," *arXiv:2106.15934*, vol. 1, 2021.
  - [20] C. Liu, M. Xu, H. Guo et al., "Tokoin: a coin-based accountable access control scheme for Internet of Things," *arXiv:2011.04919*, vol. 1, 2020.
  - [21] National Institute of Standards and Technology (NIST), *SHA-2 Standard*, vol. 1, 2021, <https://www.itl.nist.gov/fipspubs/fip180-2.htm>.
  - [22] Mongo DB, *What is NoSQL? NoSQL Databases Explained*, vol. 1, 2021, <https://www.mongodb.com/nosql-explained>.
  - [23] Arduino, "Arduino uno description," 2021, <https://store.arduino.cc/arduino-uno-rev3>.
  - [24] S. J. Naqvi, "Why I am building a blockchain in Go," *Karacchain*, vol. 1, 2018.

## Research Article

# A Framework to Test Resistency of Detection Algorithms for Stepping-Stone Intrusion on Time-Jittering Manipulation

Lixin Wang <sup>1</sup>, Jianhua Yang,<sup>1</sup> Michael Workman,<sup>1</sup> and Peng-Jun Wan<sup>2</sup>

<sup>1</sup>TSYS School of Computer Science, Columbus State University, Columbus GA, USA

<sup>2</sup>Department of Computer Science, Illinois Institute of Technology, Chicago IL, USA

Correspondence should be addressed to Lixin Wang; wang\_lixin@columbusstate.edu

Received 25 June 2021; Accepted 27 July 2021; Published 10 August 2021

Academic Editor: Zhuojun Duan

Copyright © 2021 Lixin Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Hackers on the Internet usually send attacking packets using compromised hosts, called stepping-stones, in order to avoid being detected and caught. With stepping-stone attacks, an intruder remotely logs these stepping-stones using programs like SSH or telnet, uses a chain of Internet hosts as relay machines, and then sends the attacking packets. A great number of detection approaches have been developed for stepping-stone intrusion (SSI) in the literature. Many of these existing detection methods worked effectively only when session manipulation by intruders is not present. When the session is manipulated by attackers, there are few known effective detection methods for SSI. It is important to know whether a detection algorithm for SSI is resistant on session manipulation by attackers. For session manipulation with chaff perturbation, software tools such as Scapy can be used to inject meaningless packets into a data stream. However, to the best of our knowledge, there are no existing effective tools or efficient algorithms to produce time-jittered network traffic that can be used to test whether an SSI detection method is resistant on intruders' time-jittering manipulation. In this paper, we propose a framework to test resistency of detection algorithms for SSI on time-jittering manipulation. Our proposed framework can be used to test whether an existing or new SSI detection method is resistant on session manipulation by intruders with time-jittering.

## 1. Introduction

Hackers on the Internet usually send attacking packets using compromised hosts, called stepping-stones, in order to avoid being detected and caught. With stepping-stone attacks, an intruder remotely logs these stepping-stones using programs like SSH or telnet, uses a chain of Internet hosts as relay machines, and then sends the attacking packets. To launch a stepping-stone attack, the intruder enters the attacking commands on his/her local machine which are relayed through the stepping-stone machines until the attacking packets arrive at the final target machine. It is well-known that every such TCP session between a server and a client is independent of one another even if they are relayed sessions. Such a nature of the TCP protocol makes it much more challenging to know the attacker's geographical location while accessing a remote machine via multiple relayed TCP sessions. The final target machine can only see the TCP packets from the last hub of the connection chain. Therefore, a target

machine can hardly learn any information regarding the origin of the intrusion.

To launch a stepping-stone attack, the intruder could use a remote login program (SSH, telnet, or rlogin) and create a connection chain as shown in Figure 1. In this figure, Host 0 is the intruder's machine, Host  $N$  is the final target host, and Host 1, Host 2, ..., and Host  $N - 1$  are the stepping-stone machines. With stepping-stone intrusion detection (SSID), the detection program can be installed at any of the stepping-stones. The stepping-stone host with the detection program installed is called a detecting sensor. In Figure 1, we assume that Host  $i$  is the (detecting) sensor. The purpose of SSID is to know if the detecting sensor Host  $i$  is employed as a stepping-stone machine. Two important concepts related to a detecting sensor of a connection chain are the incoming and outgoing connections. The connection from Host  $i - 1$  to Host  $i$  is called an incoming connection to Host  $i$ , and the connection from Host  $i$  to Host  $i + 1$  is called an outgoing connection from Host  $i$ . If the detecting sensor Host

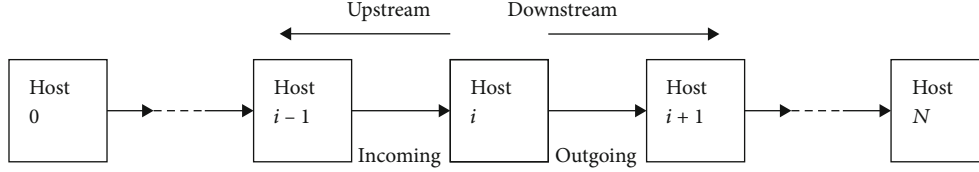


FIGURE 1: A sample connection chain.

$i$  is employed as a stepping-stone machine, then, there exists at least one matched pair between all of its incoming connections and all of its outgoing connections.

**1.1. Definitions of Send/Echo Packets.** The definitions of Send and Echo packets will be illustrated using Figure 1. Assuming that Host  $i$  is the detecting sensor. First, let us look at its incoming connection. Send packets are those TCP packets with the flag bit TCP.Flag.PSH set to TRUE that are sent from Host  $i-1$  to Host  $i$ ; Echo packets are those TCP packets with the flag bit TCP.Flag.PSH set to TRUE that are sent from Host back to Host  $i-1$ . Now, let us look at the outgoing connection. Send packets of the outgoing connection from Host  $i$  are those TCP packets with the flag bit TCP.Flag.PSH set to TRUE that are sent from Host  $i$  to Host  $i+1$ ; Echo packets are those TCP packets with the flag bit TCP.Flag.PSH set to TRUE that are sent from Host  $i+1$  back to Host  $i$ .

Which Send packet is matched with which Echo packet? Let us answer this question by using an example on the command line. If an attacker enters the command “ps” on a command line in a terminal, the command could be sent to the target machine with one or two TCP packets. For simplicity, we assume that the command “ps” is delivered to the target host with two different TCP packets, one for “p” and the other one for “s.” When the attacker types “p” on the command line, its packet is delivered to the target host. After this Send packet is echoed, an Echo packet is sent back to the attacker’s machine, and then the letter “p” is visible on the screen of the attacker’s host. The Send packet associated with the command “p” and its Echo packet are referred to as a *matched pair*, or sometimes called a *relayed pair*. Based on the TCP protocol design, an Echo packet may echo more than one Send packets. Similarly, a Send packet may be echoed by more than one Echo packets.

**1.2. The Distribution of Packets’ RTTs for a Connection Chain.** In a TCP connection, a packet RTT is the sum of four delays including queuing delay, transmission delay, processing delay, and propagation delay. For connection chain-based SSI detection, packet RTTs can be used to estimate a connection chain length. The network traffic can be represented by the RTTs calculated from the matched pairs of a Send packet and an Echo packet. In the work [1] by Yang et al., the authors proved that a connection chain length is the same as the number of clusters that are generated by employing the RTTs calculated from the connection chain.

The work [2] by Paxson and Floyd discovered that the packet RTTs calculated from a connection chain follow the Poisson distribution. This important discovery can be employed to match TCP packets as well as calculate a con-

nection chain length. Figure 2 shows that the packet RTTs obtained from a connection chain follow the Poisson distribution. In this figure, the RTTs were obtained from the TCP packets collected from a connection chain whose length is four. Based on this experiment in a connection chain with four connections, most RTT values are very close to the average  $\mu$  which is 138,500 (microsecond) of all the RTT values. Clearly, at least 95% of the RTTs are larger than 137,000 (microsecond) as well as less than 141,000 (microsecond).

If a random variable  $X$  obeys the Poisson distribution, its mean and standard deviation are represented by  $\mu$  and  $\sigma$ , respectively. It is well-known that

$$|X - \mu| \leq 2\sigma. \quad (1)$$

According to the above inequality, the majority values of the random variable  $X$  should be around its mean value  $\mu$ . The absolute value of the difference between  $X$  and  $\mu$  is at most  $2\sigma$ . Therefore, the packet RTT values calculated from captured network traffic from a TCP connection chain follow the Poisson distribution. That is, most values of the packet RTTs calculated from a connection chain of fixed length must be close to its mean value which is inside a circle centered at  $X$  of radius  $2\sigma$ .

**1.3. Session Manipulation by Intruders Using Chaff-Perturbation or Time-Jittering.** A great number of detection approaches for SSI have been developed in the literature [2–12]. However, malicious attackers never stop developing new session manipulation approaches to evade detection. The two most popular such techniques used by attackers are time-jittering and chaff perturbation. Time-jittering is a method that an attacker’s host does not transmit packets immediately. Instead, every packet will be hold for a random period of time, and then it will be released. The timestamp of each packet will be jittered. Therefore, if the network traffic is manipulated by intruders using the time-jittering technique, the timestamp of every packet is modified. As a result, all the existing approaches for time-based SSID do not work anymore.

Chaff perturbation is a session manipulation approach with which attackers can create some meaningless packets and then insert them into a normal network traffic. Due to the injection of these meaningless packets into a normal network traffic, the total number of packets is changed, so are the time gaps between the normal packets. Therefore, if the network traffic is manipulated by intruders using chaff perturbation technique, the total number of packets and the time gaps of packets are all modified. As a result, those existing approaches (SSID) that are based on the amount

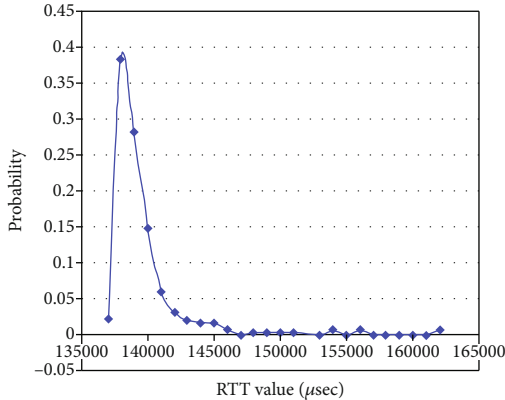


FIGURE 2: The distribution of packets' RTTs for a connection chain.

of network traffic or time gaps of packets do not work anymore. Therefore, it is very important to know whether an existing or new SSID method is resistant to intruders' session manipulation.

For chaff perturbation, software tools such as Scapy have been developed to inject meaningless packets into data streams. These software tools can be used to test whether a SSID algorithm is effective in resisting intruders' session manipulation with chaff perturbation. Scapy is a software for packet manipulation in computer networks. Its first version was implemented in Python. It can create or decode packets and then send them to the Internet. It can also capture the packets and match an Echo packet with its corresponding Send packet. Moreover, scanning, tracerouting, attacks, and network probing and discovery can all be done using Scapy.

However, to the best of our knowledge, there are no existing software tools or effective algorithms to test resistency of SSID algorithms on session manipulation with time-jittering. In this paper, we propose a framework to test resistency of detection approaches for SSI on time-jittering manipulation. Our proposed framework can be used to test whether an existing or new SSID method is resistant on session manipulation by intruders with time-jittering. The output file generated by our proposed algorithm satisfies the following properties: (1) it remains a valid list of captured TCP packets as for each Send packet with jittered timestamp, and its timestamp is still less than that of every following Echo packet; (2) only the timestamps of a given percentage of the Send packets will be jittered; (3) those Send packets whose timestamps will be jittered are randomly selected; and (4) for every Send packet whose timestamp will be jittered, the increment of its timestamp is a random and independent value.

Table 1 lists all the notations used in this paper to help readers for easy referencing.

The remaining of this paper is organized as follows. In Section 2, we give literature review on many existing and significant SSID methods. In Section 3, we present a framework to test resistency of detection algorithms for SSI on time-jittering manipulation by intruders. This paper will be summarized in Section 4, and the funding information of this research work will be provided in Acknowledgments.

## 2. Literature Review on SSID

Network security experts and researchers have proposed many SSID approaches since Stanford-Chen and Heberlein published their seminar work in SSID in 1995 [7]. In this section, we will conduct a literature review on SSID methods since 1995. There are two different types of SSID approaches: host-based SSID and network-based SSID. A host-based SSID approach is to detect stepping-stone intrusion by comparing all the outgoing connections with all the incoming connections of a single host (that is, the detecting sensor) to see if there exists a matched pair in these two connections. A network-based SSID is to estimate the length of the connection chain (the number of connections in the connection chain).

Let us begin with reviews on host-based SSID. Stanford-Chen and Heberlein [7] proposed a content-thumbprint method to find a matched pair on a single machine by comparing all the outgoing connections with all the incoming connections of the host. As law content of packets is used for the comparison, this content-thumbprint method does not work if the network traffic is encrypted. In order to overcome the problem of this content-thumbprint method, Zhang and Paxson [12] proposed a time-thumbprint method for SSID. As the timestamps of packets are usually not encrypted, this time-thumbprint method could work effectively if the network traffic is encrypted. If intruders send encrypted attacking packets to launch attacks by using SSH, for example, it makes the detection process of SSID much more challenging. Furthermore, if intruders use session manipulation techniques such as chaff perturbation and/or time-jittering to evade detection, it will make the SSID process even more challenging.

There are quite a few SSID methods have been proposed for network traffic with session manipulation by attackers using chaff perturbation and/or time-jittering to evade detection. He and Tong [9] proposed the packet counting approach aimed at addressing such challenges caused by intruders' session manipulation. The authors of [9] assumed that network traffic is encrypted, and the session is manipulated by intruders using the time-jittering and chaff perturbation techniques. Furthermore, an attacker can inject chaff packets into an attacking stream. This paper developed two detection algorithms for SSID that deal with the time-jittering and chaff perturbation manipulation. Donoho et al. [4] employed a gateway router as the detecting sensor and proposed detection algorithms for SSID. This paper considered that a stepping-stone host maybe a single machine on the Internet or a whole network associated with the gateway router.

As we mentioned earlier, Zhang and Paxson [12] proposed detection algorithms for SSID that work for encrypted network traffic. However, those approached proposed in [12] have problems when the session is manipulated by attackers using time-jittering and chaff perturbation. The detection algorithms for SSID developed in [12] depend on accurate timestamps of network packets; otherwise, these SSID approaches do not work effectively, even if packets' timestamps are slightly jittering. Yoda and Etoh [13] proposed a better approach to address this issue. This method for SSID



TABLE 1: All notations used in this paper.

$X$	A random variable
$\mu$	Mean of a random variable
$\sigma$	Standard derivation
$p$	Percentage of which timestamps of Send packets will be jittered
$N$	Total number of Send packets in the input file
$M$	Largest integer less than or equal to $pN$
$l\_packets$	A list of all the packets in the input file
$l\_Send$	A list of all Send packets in the input file
$l\_random$	An increasing list of $M$ random numbers in the range $0 \sim N - 1$

is called a deviation-based approach as the deviations between an existing intruder stream and all other concurrent data streams in the network are computed. This method tries to discover a set of data streams that could match the stream sent from the intruder. He and Tong [9] proposed a better way to resist attackers' session manipulation using chaff perturbation. The detection algorithms work effectively when the network traffic having meaningless packets chaffed into the data stream. These algorithms for SSID still work if the number of chaffed packets is proportional to the total number of packets sent from the attacker's machine. Yang et al. [14] used random walks to design a method for SSID to handle intruders' manipulation using chaff perturbation evasion. In this paper, the difference between the number of responses and the number of requests is modelled as a random walk. Yang and Zhang [15] proposed a better way of using random walks to design detection algorithms for SSID. The method used in [15] is referred to as an RTT-based random walk approach. The key idea of this paper is to decide if an outgoing connection and an incoming connection are a matched pair by applying the number of RTTs in a connection as well as the idea of random walks. The detection algorithms proposed in [15] work effectively when the network traffic is manipulated by attackers using time-jittering and/or chaff perturbation evasion.

Ding et al. [16] took a different approach that detected SSI at the target victim machine. This paper used and considered the time delay between the attacker completing typing an attacking command and the time when the next letter is entered. Later, Huang et al. [17] improved the detection algorithm for SSID proposed in [16]. The authors in [16, 17] assumed that cross-over packets must be present in a long connection chain. Huang et al. [17] discovered that a longer connection chain should produce more cross-over packets. Wang and Reeves [18] proposed a watermark-based method for SSID. This paper assumed that a unique watermark is injected into the network traffic. The matching between an incoming connection and an outgoing connection is based on the injected watermark.

Yang et al. [6] developed a computer program to inject TCP/IP packets into network traffic. The program developed in this paper could help network security researchers better understand how session manipulation works and design more innovative detection algorithms for SSID that are resis-

tant to time-jittering and/or chaff perturbation manipulations by intruders.

Because stepping-stones may be employed by legal applications for remote access, host-based SSID approaches could produce high false positive errors. To avoid the problem caused by host-based detection methods, network-based detection approaches were proposed. This type of detection method for SSID is to calculate the length of a connection chain. It is well-known that most hosts access a remote server using at most three stepping-stones. If a host uses more than three stepping-stones to access a remote server, it is most likely an intrusion. This is the rationale of all network-based detection approaches.

Next, we present the literature review on network-based detection approaches for SSI. The first known detection algorithm via the network-based approach was presented in [19] in 2002. The key idea of this paper is to compute the RTT of a Send packet and then attempt to match this Send packet with its corresponding acknowledgment (ACK) packet transmitted from the next adjacent host in the connection chain. The method proposed in [18] reduced the false positive error a little bit. However, this method for SSID produces high false negative error as the ACK packet from the next adjacent host instead of the actual Echo packet was used for the matching. The problem with the work presented in [19] was that the way to set up the connection chain was not proper.

To overcome the problem caused by the improper connection chain setup in the paper [19], a step-function detection method was developed to calculate the length of a connection chain in [20] in 2004. The step-function method developed in this paper reduced both the false positive and false negative errors in the case of local area networks (LANs). The connection chain was properly created in [20] so that the corresponding Echo packet of a Send packet can be used for the matching. In this paper, a Send packet was matched with its corresponding Echo packet, and then the packet RTTs was calculated using the step-functions. The drawback of this detection approach presented in [20] is that this method works effectively only in LANs, but it does not work well in the context of the Internet. The conservative and greedy packet matching method for SSI detection presented in [21] worked effectively in the context of the Internet, but this detection method can only match very

few TCP packets, and thus, it is not practical in SSID for computer networks connected with the Internet.

The data mining approach with clustering and partitioning proposed in [5] is a very effective connection chain-based detection approach SSI. In this work, the packet RTTs are obtained by applying the maximum-minimum distance (MMD) clustering method, and all the possible packets were checked during packet matching. The clusters' number outputted by the MMD algorithm gives the length of the connection chain. Also, the detection method based on MMD reduced largely the false negative errors as well as the false positive. A drawback of this detection algorithm for SSI is that a large number of TCP packets must be captured and analyzed. Therefore, the detection method based on MMD presented in [5] is not efficient in terms of processing time. A SSID method using the  $k$ -means clustering approach was developed in [22] in order to overcome the weakness of the MMD-based SSID algorithm proposed in [5]. This  $k$ -means-based detection algorithm is very efficient as it did not require to capture and analyze a large number of TCP packets. It is well-known that packet RTTs cluster around a number of levels [5, 20]. In general, the  $k$ -means data mining algorithm has been widely used to put data-set items into groups of related observations without none of the prior knowledge regarding their relationships. As long as most of the RTT outliers are removed from the captured RTTs in the input file, the  $k$ -means-based SSID algorithm proposed [22] works effectively in LANs.

It is worth mentioning some recent significant results that are related to network security. Using a combination of social relationship and nonsensitive attributes, Cai et al. [23] investigated how social networks are exploited and an inference attack is launched. With differential privacy, Cai et al. [24] proposed a mechanism that employed a sampling approach to generate rough counting results. In theory, these counting results are verified to satisfy privacy guarantee as well as unbiasedness. An innovative method to upload data in smart cyber-physical systems was proposed in [25]. The method proposed in this paper considered privacy preservation as well as energy conservation. A framework to mimic the behaviors of stepping-stones was proposed in [3]. The proposed framework in [3] contains tools for evasion and some other tools that can be used for evaluating detection rates of existing SSID approaches. With industrial Internet of Things, a privacy-preserved data sharing scheme was proposed in [26] where competing customers can coexist in different stages of the IoT system. Gamarra et al. [27] developed a model that describes the propagation of SSI attacks in the IoT systems using a vulnerability graph whose topology is fixed as well as switching. The model can be expanded to a more realistic scenario when the vulnerability graph changes because the attack is discovered or the intrusion detection system of the IoT is triggered. Liu et al. [28] proposed an adaptive intrusion detection approach using the fuzzy rough set theory and a new pattern learning. Using a greedy approach, the authors of [28] introduced a Gaussian mixture model clustering method aiming at obtaining the intrinsic structure of instances of computer networks.

### 3. A Framework to Test Resistency of SSID Methods on Time-Jittering Manipulation

In this section, we first propose a framework to test resistency of detection algorithms for SSI on time-jittering manipulation. Our proposed framework can be used to test whether an existing or new SSID method is resistant on session manipulation by intruders with time-jittering. Then, we present the properties of the output generated by our proposed algorithm with jittered timestamps. Finally, the significance of our proposed framework is discussed.

*3.1. An Algorithm to Test Resistency of SSID Methods on Time-Jittering.* The algorithm for testing resistency of SSID methods on time-jittering manipulation is described in Algorithm 1.

Next, we explain the above Algorithm 1 for testing resistency of SSID methods on time-jittering manipulation.

Both the input file `input.txt` and the output file `output.txt` contain two columns: one lists packet timestamp and the other column lists the packet type for each packet. The input file is obtained from a PCAP file captured in the Internet environment. The output file contains jittered timestamps in the first column and the same packet type in the second column as in the input file, and the only timestamps of a given percentage of the Send packets will be jittered.

The algorithm begins with copying the content of `input.txt` into `output.txt`. Let  $p$  denote the percentage with which of Send packets' time stamps will be jittered,  $N$  the total number of Send packets in the file `input.txt`, and  $M$  the largest integer less than or equal to  $pN$ . Clearly,  $M$  is the number of Send packets that will be jittered.

Then, we generate  $M$  random numbers in the range  $0 \sim N - 1$ , sort them in an increasing order, and store them in a list `l_random`. These random numbers are the indices of the Send packets in the list `l_Send` whose timestamps will be jittered, where `l_Send` represents the list of all the Send packets in the file `input.txt`.

After that, the for loop iterates each Send packet in the list `l_Send`. For each Send packet in `l_Send`, if its index belongs to the list `l_random`, then its timestamp will be jittered. The increment will be a random value between zero and `diff`, where `diff` represents the timestamp difference between this Send and the first following Echo packet in the list `l_packets`. Finally, update this Send's timestamp in the file `output.txt` by adding the increment to its original timestamp.

*3.2. Properties of the Output Generated by the Above Algorithm 1 with Jittered Timestamps.* Clearly, the output file `output.txt` generated by the above Algorithm 1 satisfies the following important properties:

- (1) It remains a valid list of captured TCP packets as for each Send packet with jittered timestamp, its timestamp is still less than that of every following Echo packet
- (2) Only the timestamps of a given percentage of the Send packets will be jittered

**Input:** a TXT file input.txt with two columns (including packet timestamps and the packet type) obtained from the packets captured in the Internet environment

**Output:** a TXT file output.txt with two columns (including packet timestamps and the packet type) and the timestamps of a given percentage of Send packets have been jittered

copy the file input.txt into the file output.txt

p = percentage; /\* timestamps of this percentage of Send packets will be jittered \*/

N = total number of Send packets in the file input.txt;

M = largest integer less than or equal to pN;

/\* number of Send packets that will be jittered \*/

l\_packets = a list of all the packets in the file input.txt

l\_Send = a list of all Send packets in the file input.txt

l\_random = an increasing list of M random numbers in the range 0~N-1

/\* the Send packets in the list l\_Send with these indices in l\_random will be jittered \*/

for each Send packet in the list l\_Send, do

  if its index equals a number in the list l\_random

    /\* jitter its timestamp \*/

    diff = timestamp difference between this Send and the first following Echo packet in the list l\_packets

    incr = a random number in the range 0~diff

    increase the timestamp of this Send packet by incr

    update this Send's timestamp in the file output.txt

ALGORITHM 1: An efficient algorithm for testing resistency of SSID methods on time-jittering.

- (3) Those Send packets whose timestamps will be jittered are randomly selected
- (4) For every Send packet whose timestamp will be jittered, the increment of its timestamp is a random and independent value

*3.3. Significance of the Proposed Framework.* Stepping-stones have been widely used by hackers to launch their attacks, especially after the emerging of the Internet. Network security researchers have been proposing approaches for SSID during the last two decades since Staniford-Chen and Heberlein published their seminar work [7] in 1995. However, intruders have also been developing new techniques to evade our detection. When SSI attacks are launched, intruders tend to use session manipulation techniques to evade detection. By far, the most two popular session manipulation techniques used by intruders for evasion are time-jittering and chaff perturbation. All the known SSID methods to handle intruders' time-jittering and/or chaff perturbation for detecting intruder's evasion either are not feasible to implement or do not work effectively. Some of such methods can only detect an intruder's evasion with very limited capacity. Therefore, newly proposed SSID methods should be resistant to intruders' session manipulation so that they can be used to protect practical computer networks against SSI attacks.

For chaff perturbation, software tools such as Scapy have been developed to inject meaningless packets into data streams. These software tools can be used to test whether a SSID algorithm is effective in resisting intruders' session manipulation with chaff perturbation. Currently, there are no existing software tools or effective algorithms to test resistency of SSID algorithms on session manipulation with time-jittering. Our proposed framework in this paper can be used by network security researchers to test whether their pro-

posed SSID algorithms are resistant on session manipulation by intruders with time-jittering.

## 4. Conclusion

In this paper, we developed a framework to test resistency of detection approaches for SSI on time-jittering manipulation by intruders. Network security researchers have been proposing approaches for SSID during the last two decades. However, intruders have also been developing new techniques to evade our detection. When SSI attacks are launched, intruders tend to use session manipulation techniques to evade detection. Therefore, newly proposed SSID methods should be resistant to intruders' session manipulation so that they can be used to protect practical computer networks against SSI attacks. Currently, there are no existing software tools or effective algorithms to test resistency of SSID algorithms on session manipulation with time-jittering. Our proposed framework in this paper can be used by network security researchers to test whether their proposed SSID algorithms are resistant on session manipulation by intruders with time-jittering.

As a future research direction, we will develop new effective methods for SSID that are efficient and resistant to intruders' evasion manipulation using time-jittering and/or chaff perturbation. Our proposed framework can be used to verify the resistency of the proposed SSID methods on time-jittering manipulation by intruders.

## Data Availability

All data generated or analyzed during this study are included in this published article.

## Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

## Acknowledgments

This work of Drs. Lixin Wang and Jianhua Yang is supported by the National Security Agency (NSA) NCAE-C research grant H98230-20-1-0293 with Columbus State University, Columbus GA, USA.

## References

- [1] J. Yang, S. H. S. Huang, and M. D. Wan, "A clustering- partitioning algorithm to find TCP packet round-trip time for intrusion detection," in *20th International Conference on Advanced Information Networking and Applications-Volume 1 (AINA'06)*, vol. 1, Vienna, Austria, 2006.
- [2] V. Paxson and S. Floyd, "Wide area traffic: the failure of Poisson modeling," *IEEE/ACM Transactions on Networking*, vol. 3, no. 3, pp. 226–244, 1995.
- [3] H. Clausen, M. S. Gibson, and D. Aspinall, "Evading stepping-stone detection with enough chaff," in *International Conference on Network and System Security*, pp. 431–446, Cham, 2020.
- [4] D. Donoho, A. Flesia, U. Shankar, V. Paxson, J. Coit, and S. Staniford, "Multiscale stepping-stone detection: detecting pairs of jittered interactive streams by exploiting maximum tolerable delay," in *the 5th International Symposium on Recent Advances in Intrusion Detection, Lecture Notes in Computer Science*, Berlin, Heidelberg, 2002.
- [5] J. Yang and S. S.-H. Huang, "Mining TCP/IP packets to detect stepping-stone intrusion," *Journal of Computers and Security*, vol. 26, no. 7-8, pp. 479–484, 2007.
- [6] J. Yang, L. Wang, A. Lesh, and B. Lockerbie, "Manipulating network traffic to evade stepping-stone intrusion detection," *Internet of Things*, vol. 3, pp. 34–45, 2018.
- [7] S. Staniford-Chen and L. T. Heberlein, "Holding intruders accountable on the Internet," in *Proceedings 1995 IEEE Symposium on Security and Privacy*, pp. 39–49, Oakland, CA, 1995.
- [8] T. He and L. Tong, "Detecting stepping-stone traffic in chaff: fundamental limits and robust algorithms," in *9th International Symposium on Recent Advances in Intrusion Detection (RAID 2006)*, Hamburg, Germany, April 2006.
- [9] T. He and L. Tong, "Detecting encrypted stepping-stone connections," *IEEE Transaction on Signal Processing*, vol. 55, no. 5, pp. 1612–1623, 2007.
- [10] A. Blum, D. Song, and S. Venkataraman, "Detection of interactive stepping-stones: algorithms and confidence bounds," in *Proceedings of International Symposium on Recent Advance in Intrusion Detection (RAID)*, pp. 20–35, Sophia Antipolis, France, September 2004.
- [11] L. Wang and J. Yang, "A research survey in stepping-stone intrusion detection," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, Article ID 276, 2018.
- [12] Y. Zhang and V. Paxson, "Detecting stepping-stones," in *Proc. of the 9th USENIX Security Symposium*, pp. 67–81, Denver, CO, August 2000.
- [13] K. Yoda and H. Etoh, "Finding connection chain for tracing intruders," in *Proc. 6th European Symposium on Research in Computer Security*, pp. 31–42, Toulouse, France, September 2000.
- [14] J. Yang, B. Lee, and S. S.-H. Huang, "Monitoring network traffic to detect stepping-stone intrusion," in *Proceedings of 22nd IEEE International Conference on Advanced Information Networking and Applications (AINA 2008)*, pp. 56–61, Okinawa, Japan, March 2008.
- [15] J. Yang and Y. Zhang, "RTT-based random walk approach to detect stepping-stone intrusion," in *IEEE 29th International Conference on Advanced Information Networking and Applications*, pp. 558–563, Gwangju, Korea (South), 2015.
- [16] W. Ding, M. J. Hausknecht, S.-H. S. Huang, and Z. Riggle, "Detecting stepping-stone intruders with long connection chains," in *2009 Fifth International Conference on Information Assurance and Security*, Xi'an, China, August 2009.
- [17] S. S. H. Huang, H. Zhang, and M. Phay, "Detecting stepping-stone intruders by identifying crossover packets in SSH connections," in *Proceedings of 30th IEEE International Conference on Advanced Information Networking and Applications*, pp. 1043–1050, Crans-Montana, Switzerland, March 2016.
- [18] Xinyuan Wang and D. Reeves, "Robust correlation of encrypted attack traffic through stepping stones by flow watermarking," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 3, pp. 434–449, 2011.
- [19] K. H. Yung, "Detecting long connecting chains of interactive terminal sessions," in *Proc. of International Symposium on Recent Advance in Intrusion Detection (RAID)*, pp. 1–16, Zurich, Switzerland, October 2002.
- [20] J. Yang and S.-H. S. Huang, "A real-time algorithm to detect long connection chains of interactive terminal sessions," in *Proceedings of 3rd ACM International Conference on Information Security (Infosecu'04)*, pp. 198–203, Shanghai, China, November 2004.
- [21] J. Yang and S. H. S. Huang, "Matching TCP packets and its application to the detection of long connection chains," in *Proceedings of 19th IEEE International Conference on Advanced Information Networking and Applications (AINA 2005)*, pp. 1005–1010, Taipei, Taiwan, China, March 2005.
- [22] L. Wang, J. Yang, X. Xu, and P. J. Wan, "Mining network traffic with the -means clustering algorithm for stepping-stone intrusion detection," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6632671, 9 pages, 2021.
- [23] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2016.
- [24] Z. Cai and Z. He, "Trading private range counting over big IoT data," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 144–153, Dallas, TX, USA, 2019.
- [25] Z. Cai and Z. Xu, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2018.
- [26] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.

- [27] M. Gamarra, S. Shetty, O. Gonzalez, D. M. Nicol, C. A. Kamhoua, and L. L. Njilla, "Analysis of stepping-stone attacks in internet of things using dynamic vulnerability graphs," *Modeling and Design of Secure Internet of Things*, vol. 12, pp. 273–294, 2020.
- [28] J. Liu, W. Zhang, Z. Tang et al., "Adaptive intrusion detection via GA-GOGMM-based pattern learning with fuzzy rough set-based attribute selection," *Expert Systems with Applications*, vol. 139, p. 112845, 2020.



## Research Article

# Aspect-Level Sentiment Analysis Approach via BERT and Aspect Feature Location Model

Guangyao Pang <sup>1</sup>, Keda Lu,<sup>1</sup> Xiaoying Zhu,<sup>1</sup> Jie He,<sup>1</sup> Zhiyi Mo,<sup>1</sup> Zizhen Peng <sup>2</sup>,  
and Baoxing Pu<sup>1</sup>

<sup>1</sup>School of Data Science and Software Engineering, Wuzhou University, Wuzhou 543002, China

<sup>2</sup>Department of Mechanical and Electrical Engineering, Wuzhou Vocational College, Wuzhou 543002, China

Correspondence should be addressed to Zizhen Peng; pengzizhen@qq.com

Received 27 February 2021; Revised 13 June 2021; Accepted 16 July 2021; Published 10 August 2021

Academic Editor: Zhuojun Duan

Copyright © 2021 Guangyao Pang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the rapid development of Internet social platforms, buyer shows (such as comment text) have become an important basis for consumers to understand products and purchase decisions. The early sentiment analysis methods were mainly text-level and sentence-level, which believed that a text had only one sentiment. This phenomenon will cover up the details, and it is difficult to reflect people's fine-grained and comprehensive sentiments fully, leading to people's wrong decisions. Obviously, aspect-level sentiment analysis can obtain a more comprehensive sentiment classification by mining the sentiment tendencies of different aspects in the comment text. However, the existing aspect-level sentiment analysis methods mainly focus on attention mechanism and recurrent neural network. They lack emotional sensitivity to the position of aspect words and tend to ignore long-term dependencies. In order to solve this problem, on the basis of Bidirectional Encoder Representations from Transformers (BERT), this paper proposes an effective aspect-level sentiment analysis approach (ALM-BERT) by constructing an aspect feature location model. Specifically, we use the pretrained BERT model first to mine more aspect-level auxiliary information from the comment context. Secondly, for the sake of learning the expression features of aspect words and the interactive information of aspect words' context, we construct an aspect-based sentiment feature extraction method. Finally, we construct evaluation experiments on three benchmark datasets. The experimental results show that the aspect-level sentiment analysis performance of the ALM-BERT approach proposed in this paper is significantly better than other comparison methods.

## 1. Introduction

E-commerce is a thriving industry with increasing importance to the global economy. Particularly with the rapid development of social media, more and more users begin to express their sentiments on various online platforms. These comments reflect the sentiments of users and consumers and provide sellers and governments with a lot of valuable feedback on the quality of goods or services [1–3]. For example, before purchasing a product, the users can browse a large number of comments about the product on the e-commerce platform to determine whether the product is worth buying. Similarly, governments and companies can collect a large number of public comments directly from the Internet and analyze users' opinions and satisfaction from them, so as to meet their needs. Therefore, as a basic and key work of natu-

ral language processing (NLP), sentiment analysis has attracted widespread attention from the theoretical and practical circles [4]. However, the classic sentiment analysis task can only determine the users' sentiment polarities (e.g., positive, negative, and neutral) of the product or event from the entire sentences and cannot determine the sentiment polarity of a particular aspect of the sentence, let alone identify the multiple sentiments existing in a single sentence. In contrast, aspect-based sentiment analysis is a more fine-grained classification task, which can identify the sentiment polarities of multiple aspects in a sentence. Specifically, this scene is shown in Figure 1, where a sentence as a whole has an overall sentiment, and there are also multiple aspect-level sentiments. We can observe from the comment text: in the “It didn't come with any software installed outside of windows media, but for the price, I was very pleased with the condition

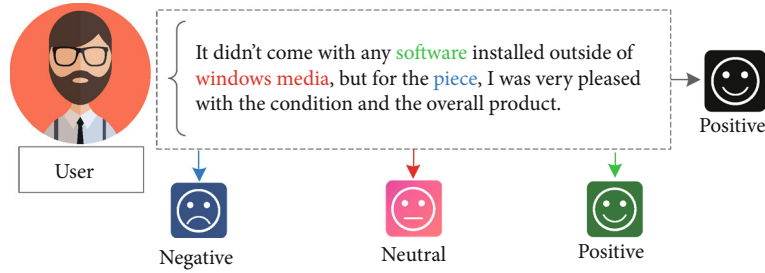


FIGURE 1: An example of consumer review with three aspect terms. Black represents sentence level sentiment analysis, while red, green, and blue represent the sentiment of corresponding aspect word, respectively.

and the overall product,” the emotional polarity of “software” is negative, “Windows Media” is neutral, and “price” and “very satisfied” are positive. Among them, these different sentiment words are called aspect words.

In recent years, researchers have proposed various methods to complete aspect-level sentiment analysis. Among them, the supervised machine learning algorithm has the best effect [5–7]. However, such statistical-based methods rely on carefully designed manual features on large-scale datasets, resulting in a lot of waste of manpower and time [8, 9]. The neural network model can automatically learn the low-dimensional representation of reviews without relying on artificial feature engineering. This feature allows neural networks to be used for aspect-level sentiment analysis tasks and has attracted the attention of researchers [10, 11].

Unfortunately, the existing methods mainly use recurrent neural network (RNN) [12] or convolutional neural network (CNN) [6] to mine the semantic information of aspect word and its context, which is easy to ignore the fact that they are insensitive to the location of key components [10, 13]. Researchers have proved that the emotional polarity of the aspect word is highly correlated with the word order of the aspect word information [4], which means that the emotional polarity of aspect words is more easily affected by the context of aspect words with similar distance [14]. Besides, the neural network is difficult to capture long-term dependencies between aspect words and context, which causes a loss of valuable information. Even if the attention mechanism [15] can be positioned in the right context to alleviate this problem, but the problem still remains and limits their performance.

For the sake of solving the aforementioned problems, on the basis of Bidirectional Encoder Representations from Transformers (BERT) [16], this paper establishes an aspect-level sentiment analysis approach based on BERT and aspect feature location model (i.e., ALM-BERT). The core idea of the ALM-BERT approach is to recognize the emotion of different aspect words in the text, consider the contextual interaction information of aspect words, and reduce the interference of irrelevant words, thus forming an effective aspect-based sentiment analysis framework. The main contributions of this paper are as follows:

- (i) Based on the pretrained general model BERT, we have constructed a multiangle text vectorization mechanism that can obtain high-quality contextual

information representation and aspect information representation. In addition, we also construct an aspect-based sentiment feature extraction method. This method utilizes an encoder based on the multi-head attention mechanism to learn the expression features of the aspect words and the interactive information of the aspect word context, which can effectively distinguish different sentences and different contributions of different aspect words

- (ii) We construct an aspect feature location model to capture the aspect information when modeling sentences and integrate the complete information of the aspect words into the interaction semantics. This model can effectively reduce the influence of noise words that have nothing to do with aspect words and improve the integrity of aspect word information
- (iii) We conduct aspect-level sentiment analysis evaluation experiments on three benchmark datasets. The experimental results show that the accuracy and macro-F1 score of our proposed model (i.e., ALM-BERT) on the Restaurant dataset are 13.66% and 29.76% higher than those of the baseline MGAN models, respectively. At the same time, the accuracy of the ALM-BERT model on comment texts of different lengths is also better than other comparison methods. This shows that the ALM-BERT approach can better mine the users’ aspect-level sentiments

We organize the remainder of this paper as follows: in Section 2, we introduce some related works on aspect-based sentiment analysis task briefly, the problem formulation is described in Section 3, we present the proposed model and its training process in detail in Section 4, experimental evaluation and result analysis are given in Section 5, and we conclude the paper and briefly discuss the future work in Section 6.

## 2. Related Works

The core goal of aspect-based sentiment analysis is to recognize the sentiment polarity of different aspect words in a given text, which means that it can mine more fine-grained sentiments, so it has become a research hotspot in the current sentiment analysis field. Currently, aspect-based sentiment analysis methods are mainly divided into two categories:

classic aspect-based sentiment analysis methods and neural network-based sentiment analysis methods.

**2.1. Classical Aspect-Based Sentiment Analysis Methods.** In the field of aspect-based sentiment analysis, early research mainly focused on traditional machine learning methods, including rule-based methods [17] and statistical-based methods [18]. These studies generally relied on laborious manual annotation and feature engineering and then employed traditional machine learning to establish a sentiment classifier [19]. For example, Qiu et al. [20] analyzed the relationship between aspect words and sentiment polarity according to the grammatical features. Analogously, Liu et al. [21] proposed a word alignment model to identify aspect words and sentiment polarity based on grammatical information. Subrahmanian and Reforgiato [22] proposed a comprehensive framework that fully considered the information of adjectives, verbs, and adverbs. Jing et al. [23] presented a topic modeling method and utilized grammatical features to help separate aspect words and sentiment words. Wu et al. [24] introduced the concept of phrase dependency parsing and took phrase fragments as an important part of identified polarity of sentiment. Zhao et al. [19] proposed a novel method, which decided the sentiment polarity of aspect words according to the grammatical features of the words related to aspect words. Kiritchenko et al. [25] adopted a support vector machine algorithm based on n-gram features, parse features, and lexical features.

Although these methods have achieved certain results, they rely too much on manual annotation and feature engineering, which means that there are performance bottlenecks that are difficult to break through.

**2.2. Neural Network-Based Sentiment Analysis Methods.** Different from the traditional methods mentioned above, the neural network can automatically learn continuous and low-dimensional representation features from the text without relying on manual feature engineering. In other words, the neural network can effectively solve the problems of excessive dependence on manual annotation and feature engineering in the above-mentioned traditional methods. Therefore, more and more researchers have constructed a series of aspect-based sentiment analysis methods based on neural networks. Tang et al. [26] constructed a Target-Dependent Long Short-Term Memory (TD-LSTM) model based on two LSTM networks, which concatenates the left context representation and right context representation of the aspect as the final context representation for predicting the sentiment. Moreover, neural network models based on attention mechanism, which was proposed in machine translation task, have been successfully applied in aspect-based sentiment analysis. Wang et al. [27] designed an LSTM model based on the attention mechanism, which can focus on the important parts related to aspect words in a sentence. Chen et al. [28] utilized a bidirectional LSTM and multiple attention mechanism to pick up important features to predict the final sentiment. Ma et al. [29] employed an interactive attention mechanism to obtain the context representation and aspect word representation. Ou et al.

[4] established a neural network with an attention-over-attention model based on LSTM. The neural network models aspect words and context at the same time, which can mine important auxiliary information in aspect words and context.

Recently, the pretraining model BERT, which can not rely on labeled data, has attracted the attention of academia and industry. Specifically, the BERT model can train a general model with preliminary natural language features only by using a large amount of unlabeled text [16]. Of course, the BERT model needs to be further fine-tuned using labeled data to complete the training of the predictor. For instance, Song et al. [30] regarded the BERT model as the embedding layer to obtain the vector representation of context and have achieved good results. Qui et al. [31] proposed a novel auxiliary sentence construction method and transformed aspect-based sentiment classification task into a sentence-pair classification task. Gao et al. [32] constructed a BERT-based encoder to determine the sentiment polarity of aspect words.

The above-mentioned research has made some progress, but there are still many problems. For example, the standard BERT model only provides local context information [33], ignoring the differences in the emotional polarity and importance of words in different aspects. In addition, most of these existing studies do not explicitly model the complete information of the aspect words in a sentence. However, other researchers have indicated that the irrelevant information to aspect words would severely degrade the performance of the model [18]. Therefore, it remains a challenging task to identifying the sentiment polarity of different aspects.

### 3. Problem Formulation

Aspect-based sentiment analysis refers to the process of outputting the sentiment polarity of each aspect word in a sentence with a sentence and some predefined aspect words as input data. We will utilize some real comment examples to illustrate aspect-level sentiment analysis tasks.

Obviously, as shown in Table 1, each example sentence contains two aspect terms, and each aspect term has four different sentiment polarities (i.e., positive, neutral, negative, and conflict). The aspect-based sentiment analysis can be defined as follows:

*Definition 1.* Formally, we give a comment sentence  $S = \{w_1, w_2, \dots, w_n\}$ , where  $n$  is the total number of words in  $S$ .  $A = \{a_1, \dots, a_i, \dots, a_m\}$  with length  $m$  represents an aspect vocabulary of length  $m$ , where  $a_i$  denotes the  $i$ th aspect word in aspect vocabulary  $A$ , and  $A$  is a subsequence of sentence  $S$ .  $P = \{p_1, \dots, p_j, \dots, p_C\}$  denotes the candidate sentiment polarities, where  $C$  denotes the number of categories of sentiment polarity and the  $p_j$  is the  $j$ th sentiment polarity.

*Problem 2.* The goal of the aspect-based sentiment analysis model is to predict the most likely sentiment polarity of

TABLE 1: Some examples of aspect-based sentiment analysis.

Comments	Aspect	Sentiment polarities			
		Positive	Negative	Neutral	Conflict
All the money went into the interior decoration, none of it went to the chefs.	Interior decoration	✓			
	Chefs		✓		
Great Indian food and the service is incredible.	Indian food	✓			
	Service	✓			
The lobster sandwich is \$24, and although it was good, it was not nearly enough to warrant that price.	Lobster sandwich				✓
	Price		✓		

specific aspect word in a sentence, which can be formulated as follows:

$$\begin{aligned}
 \text{input : } & \begin{cases} S = \{w_1, w_2, \dots, w_n\}, \\ A = \{a_1, \dots, a_i, \dots, a_m\}, \end{cases} \\
 \text{output : } & p_k = \phi_{\max}(a_i, p_j | S), \\
 \text{constraints : } & A \in S, m \in [1, N],
 \end{aligned} \tag{1}$$

where  $\phi$  represents a function that quantifies the degree of matching between the aspect word  $a_i$  and the sentiment polarity  $p_j$  in the sentence  $S$ . Finally, the model outputs the sentiment polarity with the highest matching degree to be the classification result. The notation and their description in this model are summarized in Table 2.

#### 4. Our Proposed Model

In word-level sentiment analysis and sentence-level sentiment analysis, the details of sentiment analysis will be covered up, and it also cannot accurately reflect people's fine-grained emotional expressions. In order to conduct a more complete sentiment analysis and discover the sentiment information expressed by different angles (i.e., aspects) of text reviews, this paper proposes an aspect-location model based on BERT for aspect-based sentiment analysis (i.e., ALM-BERT), which can mine different aspects of sentiment in comment details, to avoid incorrect results in real-world applications such as recommendation systems and question answering systems. The overall framework of the ALM-BERT approach is shown in Figure 2, which mainly includes four parts: multiangle text vectorization mechanism, important feature extraction model, fusion layer, and sentiment predictor.

Firstly, we employ the pretrained model BERT to generate a high-quality word vector of sequence, which provides effective support for subsequent steps (such as Section 4.1). Then, we build a new feature extractor (i.e., important feature extraction model) of multihead attention mechanism and position feedforward network to extract important context and target information (such as Section 4.2.1) and build an aspect feature location model, which can select information related to aspect words from context feature representation (such as Section 4.2.2). Finally, on the basis of fusing the

TABLE 2: The used symbols and their description.

Symbols	Description
$S$	The comment sentence
$A$	The aspect vocabulary
$C$	The number of categories of sentiment polarity
$al$	The length of aspect words
$p_j$	The $j$ th alternative sentiment polarity
$E_c$	The context representation
$E_a$	The aspect representation
$c_{cc}$	The long-term dependent information of the context
$t_{ca}$	The context-aware information to aspect word
$h_{af}$	The important features of aspect word
$h_{cm}$	The final interaction hidden state of a context interaction
$h_{am}$	The final interaction hidden state of context and aspect words
$f_s(\cdot)$	The attention score function
$f_e(\cdot)$	The energy function

context and relevant important information related to the target, we use a sentiment predictor at the aspect level to predict the probability of different emotion polarities (such as Section 4.3).

**4.1. Multiangle Text Vectorization Mechanism.** The word embedding maps each word to a high-dimensional vector space, which mainly assists machines in understanding natural language. Its mainstream methods include Word2vec and Glove. Both of these methods belong to context-based word embedding models and have achieved good performance in aspect-level sentiment analysis tasks. However, previous research has already demonstrated that these two word embedding models cannot capture the enough information in the text [34], which leads to poor classification accuracy and reduces the performance of the aspect-based sentiment analysis model. Therefore, a high-quality word embedding model has an important influence on improving the accuracy of classification results [35].

The key of aspect-level sentiment analysis is to understand natural language processing effectively. This idea usually highly relies on large-scale high-quality annotation text. Fortunately, BERT is a language pretraining model that can



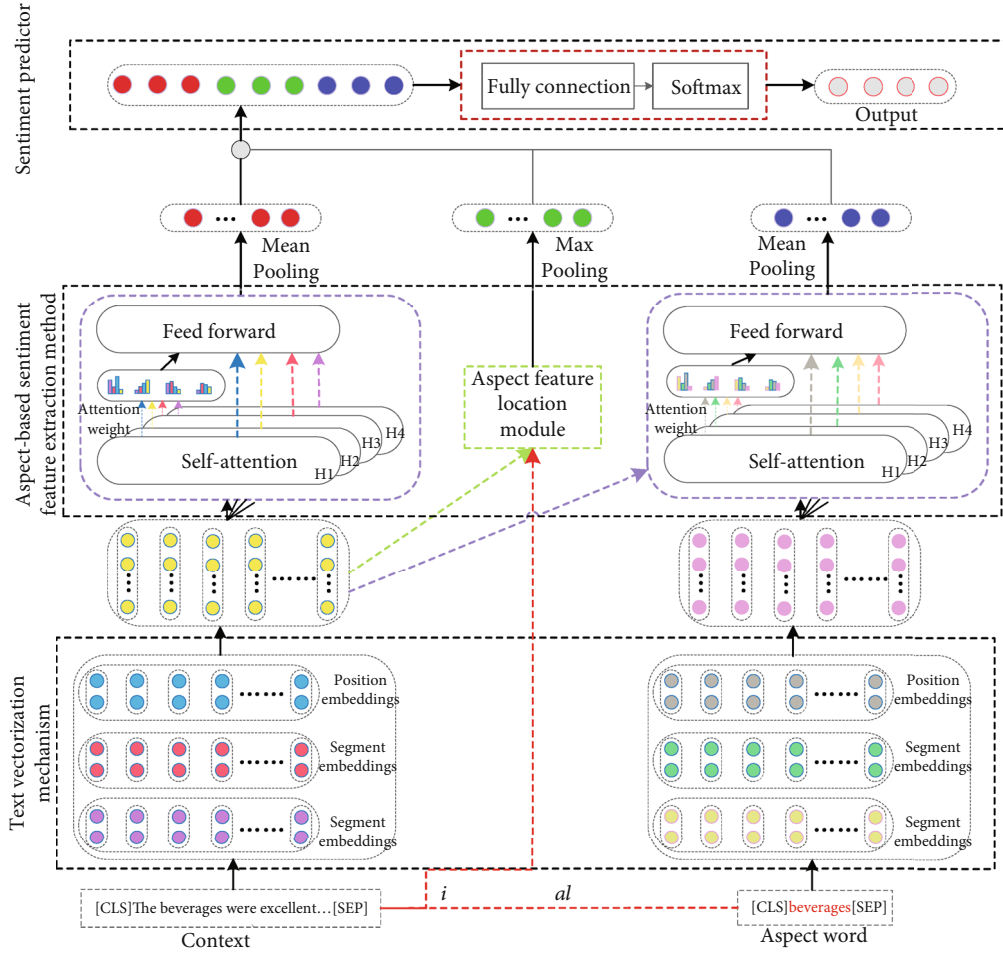


FIGURE 2: The overall framework of ALM-BERT.

effectively use unlabeled text. The model utilizes a method of randomly covering some words, utilizes a multilayer two-way converter encoder to extract a general natural language recognition model from a large amount of unlabeled text, and further uses a small amount of labeled data for fine-tuning to generate high-quality text feature vectors. Inspired by this idea, the ALM-BERT approach mentioned in this paper adds special word breaker tags [CLS] and [SEP] at the beginning and end of a given word sequence, respectively, and finally divides a given sequence into different segments. That is, the word embedding vector input in this way includes generating vectors such as token embeddings, segmentation embedding, and position embedding for different segments. In the ALM-BERT approach, we convert the comment text and aspect word into the form of “[CLS] + comment text + [SEP]” and “[CLS] + target + [SEP]”, respectively. Finally, we obtain the context representation  $E_c$  and aspect representation  $E_a$ :

$$\begin{aligned} E_c &= \{we_{[CLS]}, we_1, we_2, \dots, we_{[SEP]}\}, \\ E_a &= \{ae_{[CLS]}, ae_1, ae_2, \dots, ae_{[SEP]}\}, \end{aligned} \quad (2)$$

where  $we_{[CLS]}$ ,  $ae_{[CLS]}$  denotes the vector of classification mark [CLS], and the  $we_{[SEP]}$  and  $ae_{[SEP]}$  expressions the vector of separator [SEP].

**4.2. Aspect-Based Sentiment Feature Extraction Method.** In order to extract the implicit features of the aspect words and their context and to consider the auxiliary information contained in the aspect words, we design an aspect-based sentiment feature extraction method inspired by a transformer encoder [36]. The basic idea of this method is to integrate the information of aspect words and context and to model the interaction between context and target words. Furthermore, we hold the opinion that the accuracy of sentiment classification can be improved by capturing the feature information of aspect words in context.

**4.2.1. Important Feature Extraction Model.** A transformer encoder is a novel feature extractor based on multihead attention mechanism and position-wise feed-forward networks, which can learn different important information in different feature representation subspaces. Not only that, the transformer encoder can also directly capture the long-term dependencies in the sequence, and it is easier to parallelize than recurrent neural network and convolutional neural



**Require:** the context representation  $e_c$ ; the position  $i$  of aspect words in a sentence; the length  $al$  of aspect words; the batch size  $bs$ ;

- 1: **repeat**
- 2:     **for** each  $e_c \in bs$  **do**
- 3:         Select lines  $(i + 1$  and  $i + 1 + al)$  of  $e_c$  to obtain aspect feature  $af$ ;
- 4:         Calculate the most important features  $AF$  according to Eq. (8);
- 5:         Apply the dropout operation to all the important features to get the  $h_{af}$ ;
- 6:     **end for**;
- 7: **until** Accuracy and macro-F1 tend to be stable.

ALGORITHM 1: Aspect feature location algorithm.

networks, which greatly reduces the training time. Based on the same principle, we design the important feature extraction model as shown below.

Specifically, we first construct a multihead attention mechanism composed of multiple self-attention mechanisms. This mechanism employs different heads to capture the implicit information of the text from different aspects and can achieve high-performance parallel computing independently of RNN and CNN. Among them, the different aspects include query sequence ( $Q$ ), key-value pairs ( $K$  and  $V$ ). The attention score  $f_s(\cdot)$  in the self-attention mechanism is calculated as follows:

$$f_s(Q, K, V) = \sigma(f_e(Q, K))V, \quad (3)$$

where  $\sigma(\cdot)$  stands for the normalized exponential function, and  $f_e(\cdot)$  is the energy function to learn the correlation features between  $K$  and  $Q$ , which can be calculated by using the following formula:

$$f_e(Q, K) = \frac{QK^T}{\sqrt{d_k}}, \quad (4)$$

where  $\sqrt{d_k}$  denotes the scale factor, and the  $d_k$  is the dimension of the query and key vectors.

The attention score of multihead attention mechanism  $f_{mh}(\cdot)$  is obtained by concatenating attention score of self-attention mechanism:

$$f_{mh}(Q, K, V) = \left[ a^1; a^2; \dots; a^i; \dots; a^{n-\text{head}} \right] W_d, \quad (5)$$

$$a^i = f_s^i(Q, K, V),$$

where  $a^i$  represents the  $i$ th attention score,  $[\cdot]$  denotes concatenates of the vector, and  $W_d$  is the weight matrix.

Secondly, we input the context representation and aspect representation into the multihead attention mechanism to capture the long-term dependencies of the context and decide which context is crucial for determining the sentiment of the aspect word, which is shown in the following:

$$\begin{aligned} c_{cc} &= f_{mh}(E_c, E_c), \\ t_{ca} &= f_{mh}(E_c, E_a), \end{aligned} \quad (6)$$

where  $c_{cc}$  and  $t_{ca}$  denote the long-term dependent information of the context and the context-aware information to aspect word, respectively.

Then, we utilize the transform encoder to take  $c_{cc}$  and  $t_{ca}$  as the input of the position-wise feed-forward network and dig out the hidden states  $h_c$  and  $h_a$ . Formally, the position-wise feed-forward networks PFN,  $h_c$ , and  $h_a$  are defined as follows:

$$\begin{aligned} h_c &= \text{PFN}(c_{cc}), \\ h_a &= \text{PFN}(t_{ca}), \end{aligned} \quad (7)$$

$$\text{PFN}(h) = \zeta(hW_1 + b_1)W_2 + b_2,$$

where  $\zeta(\cdot)$  expressions the rectified linear unit,  $b_1$  and  $b_2$  represent biases, and  $W_1$  and  $W_2$  denote learnable weights.

Finally, after the mean pooling operation of  $h_c$  and  $h_a$ , we get the final hidden states  $h_{cm}$  and  $h_{am}$ .

**4.2.2. Aspect Feature Location Model.** The above-mentioned important feature extraction model captures the long-term dependence of the context and also generates the interactive semantic information between the aspect word and the context. On this basis, in order to further highlight the importance of different aspect words, we build an aspect feature positioning model based on the maximum pooling function (which is shown in Algorithm 1). This model divides the extracted aspect words and their context hiding features into multiple regions (i.e., line 3) and selects the maximum value in each region to represent the region (i.e., lines 4-5). In this way, the model can also locate core features and reduce the influence of noise words that are not related to aspect words, thereby improving the integrity of aspect word information. In other words, capturing aspect features and the different importance of aspect features can further improve the accuracy of aspect-level emotion classification.

Specifically, combining the characteristics of the position and length of the aspect word, the feature location algorithm extracts the most important relevant information of the aspect word  $af$  from the context representation  $e_c$ . Moreover, We applied max-pooling to  $af$  to get the most important features AF.

$$\text{AF} = \text{Maxpooling}(af, \text{dim} = 0). \quad (8)$$

Afterwards, we perform a dropout operation on AF and obtain the important features  $h_{af}$  of the aspect word in the context representation.

**4.3. Sentiment Predictor.** One of the cores of ALM-BERT is to utilize multiple self-attention mechanisms to obtain multi-angle text hidden expression features, and after processing by aspect feature positioning models, we have obtained a wealth of aspect-level auxiliary features and contextual interaction of aspect word information. In order to effectively utilize these complete and rich features, this paper uses fully connection layer to fuse and preprocess the features in advance and uses the softmax function to map the features to the [0,1] interval, so as to achieve effective mapping from features to sentiment classification. Specifically, we concatenate the  $h_{cm}$ ,  $h_{am}$ , and  $h_{af}$  first to obtain the comprehensive representation  $r$ , which is shown as follows:

$$r = [h_{cm}; h_{am}; h_{af}]. \quad (9)$$

Subsequently, we use a linear function to preprocess the data of  $r$ , as shown in the following:

$$x = W_u r + b_u, \quad (10)$$

where  $W_u$  represents the weight matrix, and  $b_u$  denotes the bias.

At last, we utilize a softmax function to compute the probability Pr that the sentiment polarity of the aspect word  $a$  in a sentence is  $p$ , as shown in the following:

$$\Pr(a=p) = \frac{\exp(x_p)}{\sum_{i=1}^C \exp(x_i)}, \quad (11)$$

where  $C$  denotes the number of categories of sentiment polarity.

On the whole, the ALM-BERT approach, which is proposed in this paper, is an end-to-end computing process. Moreover, in order to optimize the parameters of the ALM-BERT approach, so as to minimize the loss between the predicted sentiment polarity  $y$  and the correct sentiment polarity  $\hat{y}$ , we adopt cross-entropy with L2 regularization as the loss function to train our model, which is defined as

$$\text{loss} = - \sum_{j=1}^D \sum_{i=1}^C y_i^j \log \hat{y}_i^j + \lambda \|\theta\|^2, \quad (12)$$

where  $D$  means all training data, and  $j$  and  $i$  denote the index of a training data sample and a sentiment class, respectively.  $\lambda$  represents the factor for L2 regularization, and  $\theta$  denotes the parameter set of the model.

## 5. Experimental Evaluation

For the sake of evaluating the rationality and effectiveness of the ALM-BERT approach, this section describes the details of experiment settings and designs comparative experiments. Moreover, we also analyze the experimental results.

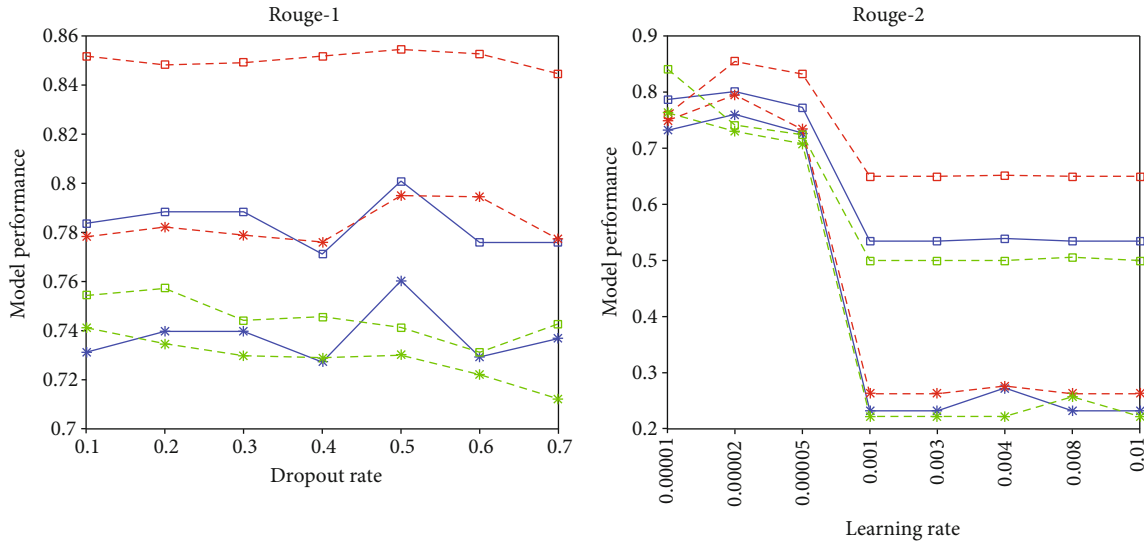
TABLE 3: The statistical information of datasets.

Dataset	Overall	Positive	Neutral	Negative	Conflict
Laptop-train	2373	994	870	464	45
Laptop-test	654	341	128	169	16
Restaurant-train	3699	2164	807	637	91
Restaurant-test	1134	728	196	196	14
Twitter-train	6248	1561	3127	1560	—
Twitter-test	692	173	346	173	—

**5.1. Datasets.** For our experiments, we conduct experiments on three public English review datasets. The statistical information of these datasets is illustrated in Table 3. Among them, in the Restaurant and Laptop datasets provided by SemEval 2014 [37], each sentence contains some aspect words and the corresponding emotional polarity (polarity is marked as positive, negative, neutral, and conflict); in the twitter dataset collected by Tan et al. [38], users' comments are marked with emotional polarity, and the emotional polarity is positive, negative, and neutral, respectively. These three datasets are currently popular review datasets, which have been widely used in aspect-based sentiment analysis tasks.

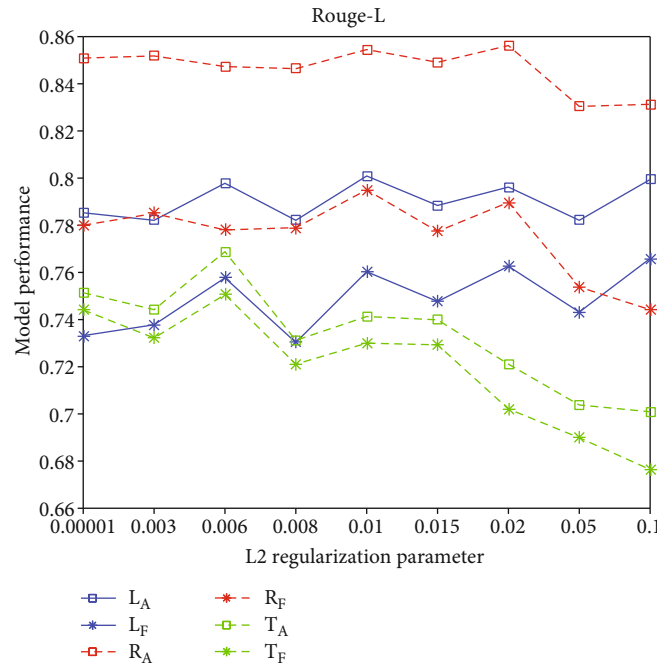
**5.2. Baselines and Evaluation Metrics.** In order to verify the effectiveness of our model, we compare the ALM-BERT approach with many popular aspect-based sentiment analysis models, as listed in the following:

- (i) *TD-LSTM* [26] is a classic model, which improves the accuracy of classification by integrating the correlation information between aspect words and context into the LSTM-based classification model
- (ii) *ATAE-LSTM* [27] is a classification model that attaches the embedded representation of aspect words to the embedded representation of sentence as input and then applies the attention mechanism to calculate the weight
- (iii) *MemNet* [39] is a data-driven model that utilizes multiple attention-based computational layers to capture the importance of each context word
- (iv) *IAN* [29] proposes interactive attention networks to model aspect words and context separately and generate the representations for targets and contexts
- (v) *RAM* [28] constructs a framework based on multi-attention mechanism, as to capture the long-distance features in the text and enhance the representation ability of the model
- (vi) *TNet* [40] utilizes bidirectional LSTM to generate the hidden representation of context and aspect words and then utilizes a CNN layer to extract important features from the hidden representation instead of the attention mechanism



(a) [ROUGE-1]

(b) [ROUGE-2]



(c) [ROUGE-L]

FIGURE 3: The scores of ROUGE on parameter optimization.

- (vii) *Cabasc* [41] proposes two kinds of attention enhancement mechanisms to focus on aspect words and context, respectively, and comprehensively considers the relevance between context and aspect words
- (viii) *AOA* [4] constructs an attention-over-attention model to associate sentiment words with aspect words. Moreover, the attention-over-attention model automatically generates mutual attentions from aspect-to-text and text-to-aspect
- (ix) *MGAN* [42] proposes a multigrained attention model to capture the interactive information

between aspect words and context from coarse to fine

- (x) *AEN-BERT* [30] is a model based on attention mechanism and BERT and shows good performance in aspect-based sentiment analysis tasks
- (xi) *BERT-base* is an aspect-based sentiment analysis model based on pretrained BERT, which has a full connection layer and a softmax layer for classification

For the sake of measuring the performance of the model fairly, we extend the AOA, IAN, and MemNet models by replacing the embedding layer of these models with BERT,

TABLE 4: Some examples of aspect-based sentiment analysis.

Word embedding	Models	Laptop		Restaurant		Twitter	
		Accuracy	Macro-F1	Accuracy	Macro-F1	Accuracy	Macro-F1
Embedding	LSTM	0.6144	0.4401	0.7304	0.533	0.6474	0.6058
	ATAE-LSTM	0.6019	0.4909	0.7375	0.5725	0.6864	0.6501
	Cabasc	0.6301	0.5297	0.7241	0.5245	0.6171	0.5657
	IAN	0.6191	0.4671	0.7268	0.4897	0.6618	0.6251
	MGAN	0.5878	0.4264	0.7179	0.4974	0.6373	0.5856
	MemNet	0.7915	0.7576	0.8241	0.7313	0.6936	0.6772
	RAM	0.5956	0.4308	0.7152	0.4656	0.6358	0.5998
	TNet	0.7022	0.6404	0.7688	0.6269	0.6994	0.6827
BERT	IAN-BERT	0.7696	0.7179	0.808	0.722	0.7269	0.7048
	AOA-BERT	0.7774	0.7407	0.7341	0.7173	0.7341	0.7173
	MemNet-BERT	0.7915	0.7576	0.8241	0.7313	0.6936	0.6772
	AEN-BERT	0.7947	0.7544	0.8125	0.7069	0.7168	0.7052
	BERT-base	0.768	0.7288	0.8375	0.7613	0.7442	0.7271
	LCF-bert	0.7837	0.7441	0.8509	0.7894	0.7254	0.7113
	ALM-BERT	0.8009	0.7603	0.8545	0.795	0.7413	0.73

to obtain AOA-BERT, IAN-BERT, and MemNet-BERT models. The structure of the rest models is consistent with those described in the corresponding paper.

In addition, in order to objectively evaluate the performance of the ALM-BERT model, similar to existing aspect-level sentiment analysis tasks, we use macro-F1 score (F1) and accuracy (Acc) as evaluation indicators.

Accuracy (Acc) is defined as

$$\text{Acc} = \frac{\text{SC}}{N}, \quad (13)$$

where SC denotes the number of samples correctly classified, and  $N$  represents the total number of samples. Generally, the higher the accuracy, the better the performance of the model.

In addition, macro-F1 is used to truly reflect the performance of the model, which is the weighted average of precision and recall. The macro-F1 is calculated according to the following formula:

$$\begin{aligned} \Pr e_{C_i} &= \frac{T_{C_i}}{T_{C_i} + \text{FP}_{C_i}}, \\ R_{C_i} &= \frac{T_{C_i}}{T_{C_i} + \text{FN}_{C_i}}, \\ \text{macro-F1} &= \frac{1}{C} \left( \sum_{i=1}^C \left\{ \frac{(2 * \Pr e_{C_i} * R_{C_i})}{(\Pr e_{C_i} + R_{C_i})} \right\} \right), \end{aligned} \quad (14)$$

where  $T$  represents the number of samples correctly classified as sentiment polarity  $i$ , FP denotes the number of samples incorrectly classified as sentiment polarity  $i$ , FN represents the number of samples whose sentiment polarity  $i$  is misclassified as other sentiment polarities,  $C$  denotes the number of categories of sentiment polarity,  $\Pr e_{C_i}$  indicates

the precision of sentiment polarity  $i$ , and  $R_{C_i}$  denotes the recall of sentiment polarity  $i$ . In our experiment, for a more comprehensive evaluation of the performance of our model, we divided the categories of sentiment polarity into  $3C = \{\text{positive, neutral, negative}\}$  and  $4C = \{\text{positive, neutral, negative, conflict}\}$ .

**5.3. Parameter Optimization.** The training process of the ALM-BERT model mainly introduces BERT to generate vector representations of context and aspect words. Therefore, we use BERT's standard parameter  $BERT_{BASE}$  to complete the model training, that is, the number of conversion models, the number of hidden neurons, and the number of self-attention heads are 12, 768, and 12, respectively. Furthermore, we have optimized the training process of the model as follows.

The dropout [43] refers to the probability of discarding some neurons during the training process of neural network, which is used to enhance the generalization ability of the model. We initialize the value of dropout to 0.3 and then search for the optimal value at intervals of 0.1. As shown in Figure 3(c), the experimental results demonstrate that when the dropout is 0.5, the ALM-BERT has the best accuracy and F1 value on the three datasets.

The learning rate determines whether and when the objective function converges to the local minimum. In our experiments, we use the Adam optimization algorithm to update the parameters of the model and explore the best learning rate parameters in the range of  $[10^{-5}, 0.1]$ . As shown in Figure 3(c), when the learning rate is  $2 * 10^{-5}$ , ALM-BERT has the best performance.

The L2 regularization parameter is a hyperparameter, which can prevent the model from overfitting. According to the results of Figure 3(c), the ALM-BERT performs best when the value of L2 regularization parameter is set to 0.01. Meanwhile, we initialize model weights by Glorot

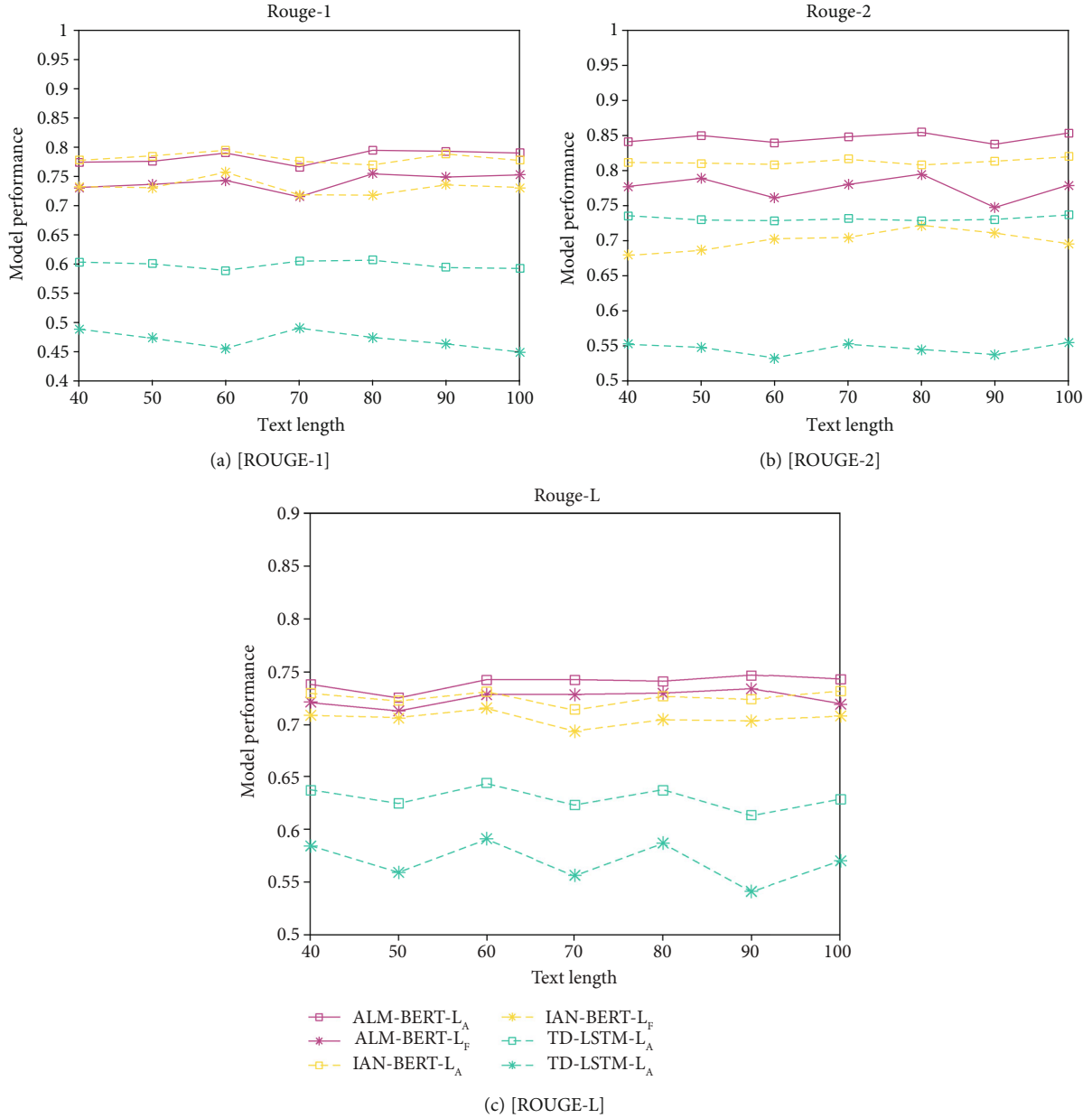


FIGURE 4: The scores of ROUGE on different lengths of the source text.

initialization [44] and set the batch size to 16 and train a total of 10 epochs.

**5.4. Evaluation Experiment of All Comparison Methods.** As shown in Table 4, the results of sentiment classification when sentiment polarity  $C = 3$ . We can easily observe from the experimental results that the accuracy and macro-F1 of  $BE RT_{BASE}$  are significantly higher than those of Glove and Word2vec based models. Particularly for Restaurant dataset, the accuracy and macro-F1 of ALM-BERT are 12.77% and 30.97% higher than those of the classical IAN model, respectively. This shows that in the field of NLP, the introduction of BERT to build a pretrained word embedding model can indeed better express the semantic and grammatical features

of the text. Meanwhile, we find that the ALM-BERT approach presented in this paper achieves the best classification performance on the three datasets.

Specifically, compared with the performance of the AEN-based model on Restaurant dataset, the ALM-BERT can improve the accuracy and macro-F1 by 4.2% and 8.81%. In addition, it is not difficult to find that the classification accuracy and macro-F1 of the ALM-BERT on the Laptop dataset are 3.29%, 3.15% higher than those of the BERT-base model. This proves that our aspect feature location model plays a positive role in aspect-based sentiment analysis.

**5.5. Evaluation Experiment for Mining Long-Term Dependencies.** For the sake of verifying the performance of



different methods to capture long-term dependencies, we construct a series of verification experiments in texts of different lengths.

As shown in Figures 4(a)–4(c), the ALM-BERT approach obtains higher accuracy and macro-F1 than TD-LSTM on the whole, which means that our transform encoder can simulate the implicit relationship between contexts better than LSTM-based encoder. In addition, compared with AEN, as shown in Figure 1, the prediction accuracy and macro-F1 of the ALM-BERT model in different length sentences are improved by 3.1% and 6.56%, respectively. This shows that ALM-BERT makes better use of aspect information than AEN and reduces the interference of aspect independent information.

To sum up, these experiments reveal that the ALM-BERT can get higher accuracy and macro-F1, which further verifies that the BERT and aspect information is feasible and effective in the task of aspect-based sentiment analysis.

## 6. Conclusion

In this paper, we establish a transformer encoder based on BERT to capture the long-term dependencies of the context and generate the interactive semantic information between aspect words and context. Then, we propose an aspect feature location model to extract more aspect features from context information. Experiments on several datasets demonstrate that our proposed approach (i.e., ALM-BERT) is superior to other methods. In addition, with the increase of text length, our proposed approach continues to maintain excellent performance. In other words, the ALM-BERT approach is better able to handle long text data and better excavate the users' aspect-level sentiment.

In our proposed approach, we mainly focus on utilizing natural language texts to identify users' sentiment. However, people's way of expression on social platforms has become more abundant. Therefore, we are interested in combining with image processing technology to analyze multimodal data in the future.

## Data Availability

For our experiments, we conduct experiments on three public English review datasets. Among them, the Restaurant and Laptop datasets are provided by SemEval 2014; each sentence in those datasets contains some aspect words and corresponding sentiment polarity, which are labeled with positive, negative, neutral, and conflict. The last datasets consist of user comments collected from twitter; the sentiment polarity is labeled with positive, negative, and neutral. These three datasets are currently popular review datasets, which have been widely used in aspect-based sentiment analysis tasks.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This work was supported by the Scientific Research Basic Ability Promotion Foundation of Guangxi Universities' Young and Middle-aged Teachers (Grant Nos. 2020KY17018, 2021KY1492, and 2019KY0686), the National Natural Science Foundation of China (Grant No. 61961036), the Guangxi Innovation-Driven Development Special Fund Project (Guike AA18118036), the Industry-University-Research Project of Wuzhou High-tech Zone and Wuzhou University (Grant No. 2020G003), and the Guangxi Natural Science Foundation (No. 2020GXNSFAA238013).

## References

- [1] M. E. Mowlaei, M. Saniee Abadeh, and H. Keshavarz, "Aspect-based sentiment analysis using adaptive aspect-based lexicons," *Expert Systems with Applications*, vol. 148, article 113234, 2020.
- [2] Z. Cai and Z. He, "Trading private range counting over big IoT data," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 144–153, Dallas, TX, USA, 2019.
- [3] Y. Lin, X. Wang, F. Hao et al., "Dynamic control of fraud information spreading in mobile social networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 6, pp. 3725–3738, 2021.
- [4] O. Yanglan, B. Huang, and K. M. Carley, "Aspect level sentiment classification with attention-over-attention neural networks," in *Social, Cultural, and Behavioral Modeling. SBP-BRiMS 2018*, R. Thomson, C. Dancy, A. Hyder, and H. Bisgin, Eds., vol. 10899 of Lecture Notes in Computer Science, pp. 197–206, Springer, Cham, 2018.
- [5] S. Cortes, U. B. Dasha, J. F. Bogdanova, J. Wagner, P. Arora, and L. Tounsi, "Dcu: aspect-based polarity classification for semeval task 4," in *Proceedings of the 8th International Workshop on Semantic Evaluation (SemEval 2014)*, pp. 223–229, Dublin, Ireland, 2014.
- [6] H. Xu, P. W. W. L. Z. Cai, Z. Xiong, and Y. Pan, *Generative adversarial networks: a survey towards private and secure applications*, ACM Computing Surveys (CSUR), 2021.
- [7] Z. Cai and Z. Xu, "A private and efficient mechanism for data uploading in smart cyberphysical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2018.
- [8] A. Nazir, Y. Rao, L. Wu, and L. Sun, "Issues and challenges of aspect-based sentiment analysis: a comprehensive survey," *IEEE Transactions on Affective Computing*, 2020.
- [9] Y. Lin, Z. Cai, X. Wang, F. Hao, L. Wang, and A. M. V. V. Sai, "Multi-round incentive mechanism for cold start-enabled mobile crowdsensing," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 993–1007, 2021.
- [10] N. Liu and B. Shen, "Aspect-based sentiment analysis with gated alternate neural network," *Knowledge-Based Systems*, vol. 188, article 105010, 2020.
- [11] Y. Liang, Z. Cai, J. Yu, Q. Han, and Y. Li, "Deep learning based inference of private information using embedded sensors in smart devices," *IEEE Network*, vol. 32, no. 4, pp. 8–14, 2018.
- [12] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

- [13] Z. Xiong, Z. Cai, D. Takabi, and W. Li, "Privacy threat and defense for federated learning with non-i.i.d. data in aiot," *IEEE Transactions on Industrial Informatics*, p. 1, 2021.
- [14] P. Zhao, L. Hou, and O. Wu, "Modeling sentiment dependencies with graph convolutional networks for aspect-level sentiment classification," *Knowledge-Based Systems*, vol. 193, article 105443, 2020.
- [15] Y. B. J. F. D. Bahdanau, K. H. Cho, and L. Tounsi, "Neural machine translation by jointly learning to align and translate," in *Proceedings of the 3rd international conference on learning representations*, pp. 1–15, San Diego, USA, 2015.
- [16] M.-W. Chang, L. K. Devlin, and J. K. Toutanova, "Bert: pre-training of deep bidirectional transformers for language understanding," in *Proceedings of the Conference of the North American Chapter of the Association for Computational Linguistics*, pp. 1–16, Minneapolis, USA, 2018.
- [17] B. L. X. Ding and S. Y. Philip, "A holistic lexicon-based approach to opinion mining," in *Proceedings of the International Conference on Web Search and Web Data Mining - WSDM '08*, pp. 231–240, New York, NY, USA, 2008.
- [18] L. Jiang, M. Yu, M. Zhou, X. Liu, and T. Zhao, "Target-dependent twitter sentiment classification," in *Proceedings of the 49th annual meeting of the Association for Computational Linguistics: human language technologies*, pp. 151–160, Portland, Oregon, USA, 2011.
- [19] X. Zhao, J. Jiang, H. Yan, and X. Li, "Jointly modeling aspects and opinions with a MaxEnt-LDA hybrid," in *Proceedings of the 2010 Conference on empirical methods in natural language processing*, pp. 56–65, Cambridge, MA, 2010.
- [20] G. Qiu, B. Liu, J. Bu, and C. Chen, "Opinion word expansion and target extraction through double propagation," *Computational Linguistics*, vol. 37, no. 1, pp. 9–27, 2011.
- [21] Y. Liu, K. Liu, H. L. Xu, and J. Zhao, "Opinion target extraction using partially-supervised word alignment model," in *Proceedings of the international joint conferences on artificial intelligence*, pp. 2134–2140, Beijing, China, 2013.
- [22] V. S. Subrahmanian and D. Reforgiato, "Ava: adjective-verb-adverb combinations for sentiment analysis," *IEEE Intelligent Systems*, vol. 23, no. 4, pp. 43–50, 2008.
- [23] Jing, Y. Hongfei, X. Zhao, Jiang, and X. Li, "Jointly modeling aspects and opinions with a maxent-lda hybrid," in *Proceedings of the Conference on Empirical Methods in Natural Language Processing*, pp. 56–65, MIT, Massachusetts, USA, 2010.
- [24] Y. Wu, Q. Zhang, X. Huang, and L. Wu, "Phrase dependency parsing for opinion mining," in *Proceedings of the 2009 Conference on Empirical Methods in Natural Language Processing Volume 3 - EMNLP '09*, pp. 1533–1541, Singapore, 2009.
- [25] C. C. S. Kiritchenko, X. Zhu, and S. M. Mohammad, "Nrc-Canada-2014: detecting aspects and sentiment in customer reviews," in *Proceedings of the 8th international workshop on semantic evaluation (SemEval 2014)*, pp. 437–442, Dublin, Ireland, 2014.
- [26] X. F. D. Tang, B. Qin, and T. Liu, "Effective lstms for target-dependent sentiment classification," in *Proceedings of the 26th International Conference on Computational Linguistics*, pp. 3298–3307, Osaka, Japan, 2016.
- [27] Y. Wang, M. Huang, L. Zhao, and X. Zhu, "Attention-based lstm for aspect-level sentiment classification," in *Proceedings of the 2016 Conference on empirical methods in natural language processing*, pp. 606–615, Austin, Texas, 2016.
- [28] P. Chen, Z. Sun, L. Bing, and W. Yang, "Recurrent attention network on memory for aspect sentiment analysis," in *Proceedings of the 2017 Conference on empirical methods in natural language processing*, pp. 452–461, Copenhagen, Denmark, 2017.
- [29] D. Ma, S. Li, X. Zhang, and H. Wang, "Interactive attention networks for aspect-level sentiment classification," in *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI)*, pp. 4068–4074, Melbourne, Australia, 2017.
- [30] Y. Song, J. Wang, T. Jiang, Z. Liu, and Y. Rao, "Targeted sentiment classification with attentional encoder network," in *Artificial Neural Networks and Machine Learning - ICANN 2019: Text and Time Series. ICANN 2019*, I. Tetko, V. Kůrková, P. Karpov, and F. Theis, Eds., vol. 11730 of Lecture Notes in Computer Science, pp. 93–103, Springer, Cham, 2019.
- [31] X. Q. C. Sun and L. Huang, "Utilizing bert for aspect-based sentiment analysis via constructing auxiliary sentence," in *Proceedings of the Conference of the North American Chapter of the Association for Computational Linguistics*, pp. 1–6, Minneapolis, USA, 2019.
- [32] Z. Gao, A. Feng, X. Song, and X. Wu, "Targetdependent sentiment classification with bert," *IEEE Access*, vol. 7, pp. 154290–154299, 2020.
- [33] Z. Lu, D. Pan, and J.-Y. Nie, "VGCNBERT: augmenting BERT with graph embedding for text classification," in *Advances in Information Retrieval. ECIR 2020*, J. Jose, Ed., vol. 12035 of Lecture Notes in Computer Science, pp. 369–382, Springer, Cham, 2020.
- [34] L.-C. Yu, J. Wang, K. R. Lai, and X. Zhang, "Refining word embeddings using intensity scores for sentiment analysis," *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, vol. 26, no. 3, pp. 671–681, 2018.
- [35] S. Rida-E-Fatima, A. Javed, A. Banjar et al., "A multi-layer dual attention deep learning model with refined word embeddings for aspect-based sentiment analysis," *IEEE Access*, vol. 7, pp. 114795–114807, 2019.
- [36] A. Vaswani, N. Shazeer, N. Parmar et al., "Attention is all you need," in *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017*, pp. 5998–6008, Long Beach, CA, USA, 2017.
- [37] M. Pontiki, D. Galanis, J. Pavlopoulos, H. Papageorgiou, I. Androutsopoulos, and S. Manandhar, "Semeval-2014 task 4: aspect based sentiment analysis," in *Proceedings of the 8th International Workshop on Semantic Evaluation (SemEval 2014)*, pp. 27–35, Dublin, Ireland, 2015.
- [38] C. Tan, D. Tang, M. Zhou, L. Dong, F. Wei, and X. Ke, "Adaptive recursive neural network for target-dependent twitter sentiment classification," in *Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics*, pp. 49–54, Baltimore, Maryland, USA, 2014.
- [39] B. Qin, D. Tang, and T. Liu, "Aspect level sentiment classification with deep memory network," in *Proceedings of the 2016 conference on empirical methods in natural language processing*, pp. 214–224, Austin, Texas, USA, 2016.
- [40] W. Lam, X. Li, L. Bing, and B. Shi, "Transformation networks for target-oriented sentiment classification," in *Proceedings of the 56th annual meeting of the Association for Computational Linguistics*, pp. 946–956, Melbourne, Australia, 2018.
- [41] Q. Liu, H. Zhang, Y. Zeng, Z. Huang, and Z. Wu, "Content attention model for aspect based sentiment analysis," in

*Proceedings of the 2018 World wide web conference*, pp. 1023–1032, Lyon France, 2018.

- [42] F. Fan, Y. Feng, and D. Zhao, “Multi-grained attention network for aspect-level sentimentclassification,” in *Proceedings of the 2018 Conference on empirical methods in natural language processing*, pp. 3433–3442, Brussels, Belgium, 2018.
- [43] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, “Dropout: a simple way to prevent neural networks from overfitting,” *Journal of Machine Learning Research*, vol. 15, no. 1, pp. 1929–1958, 2014.
- [44] Y. Bengio and X. Glorot, “Understanding the difficulty of training deep feedforward neural networks,” in *Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics*, pp. 1–8, Chia Laguna Resort, Sardinia, Italy, 2010.

## Research Article

# Temporal Index Scheme of Hyperledger Fabric System in IoT

**Yongqiang Lu** <sup>1</sup>, **Zhaobin Liu** <sup>1</sup>, **Shaoqi Wang**,<sup>1</sup> **Zhiyang Li**,<sup>1</sup> **Weijiang Liu**,<sup>1</sup>  
and **Xuhui Chen**<sup>2</sup>

<sup>1</sup>*School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China*

<sup>2</sup>*The Key Laboratory of Internet of Things Application Technology, Xiamen University of Technology, Xiamen 361024, China*

Correspondence should be addressed to Zhaobin Liu; zhbliu@dlnu.edu.cn

Received 12 March 2021; Revised 12 May 2021; Accepted 28 June 2021; Published 12 July 2021

Academic Editor: Zhuojun Duan

Copyright © 2021 Yongqiang Lu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

As a large number of mobile terminals are connected to the IoT, the security problem of IoT is a challenge to the IoT technology. Blockchain technology has the characteristics of decentralization, data encryption, smart contract, and so on, especially suitable in the complex heterogeneous network. However, sequential access based on block files in the blockchain hinders efficient query processing. The problem is due to current blockchain solutions do not support temporal data processing. In this paper, we propose two index building methods (TISD and TIF) to address this issue in Hyperledger Fabric System. TISD (temporal index based on state databases) segments the historical data by time interval in the time dimension and indexes events at the same time interval. TIF (temporal index based on files) builds the index of files by the block transaction data, which is arranged in chronological order and is stored at a certain time interval. In the experimental part, we compare the query time on two datasets and analyse the query performance. Experiments demonstrated that our two methods are relatively stable in overall time performance on different datasets in the Hyperledger Fabric System.

## 1. Introduction

The Internet of Things is made up of devices that generate, process, and exchange large amounts of security-critical data, so IoT devices are often the target of various cyberattacks [1, 2]. Due to cost constraints and harsh application scenarios, most IoT devices have general functions and limited computing and storage capabilities [3]. These devices must use most of their resources for computing and executing core applications, so they cannot consume too many resources in terms of security and privacy [4]. In terms of protecting user privacy, the existing IoT system has obvious defects, which will hinder the IoT application service program from providing normal services. Therefore, the IoT needs a lightweight, scalable, and distributed security privacy-protection mechanism. Blockchain technology supports distributed, secure, and confidential security mechanisms, which are suitable for providing security protection for the IoT.

Blockchain is an accounting technique that is maintained jointly by multiple parties and uses cryptography to ensure the security of transmission and access [5]. It can achieve consistent data storage and difficultly to tamper with and prevent denial. It is also known as a typically distributed ledger technology [6, 7]. The blockchain uses transaction signatures, consensus algorithms, and cross-chain technology to ensure the consistency of the distributed ledgers of both parties to the transaction and realize the automatic disclosure of information [8].

In 2015, Linux Foundation led an open-source blockchain project—Hyperledger-developed Fabric [9, 10], Sawtooth, Burrow, and Iroha multiple blockchain projects. One of the most concerned is Fabric, different from the currency and etheric fang public blockchain projects, such as Hyperledger Fabric as chain alliance specially designed for enterprise applications, introduced the members of the identity authentication [11].

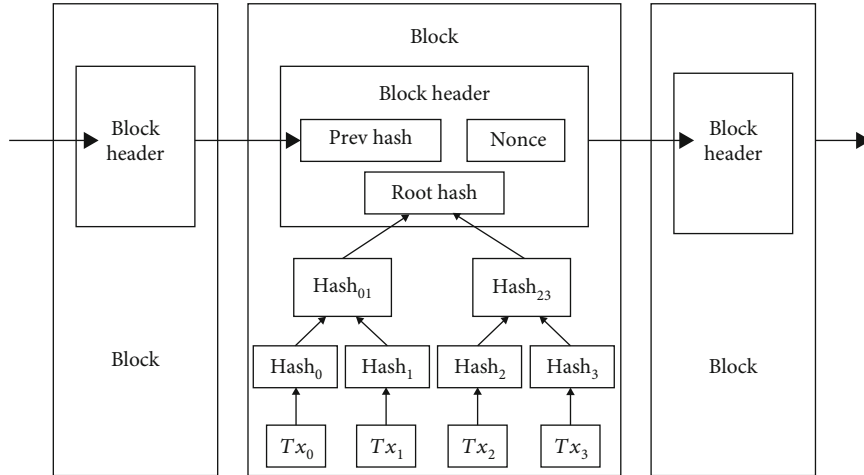


FIGURE 1: Bitcoin blockchain structure.

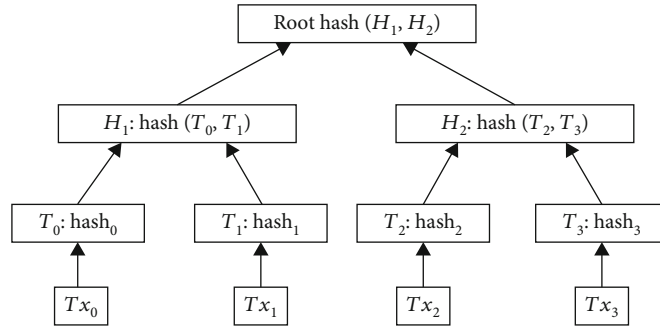


FIGURE 2: Merkle Tree structure.

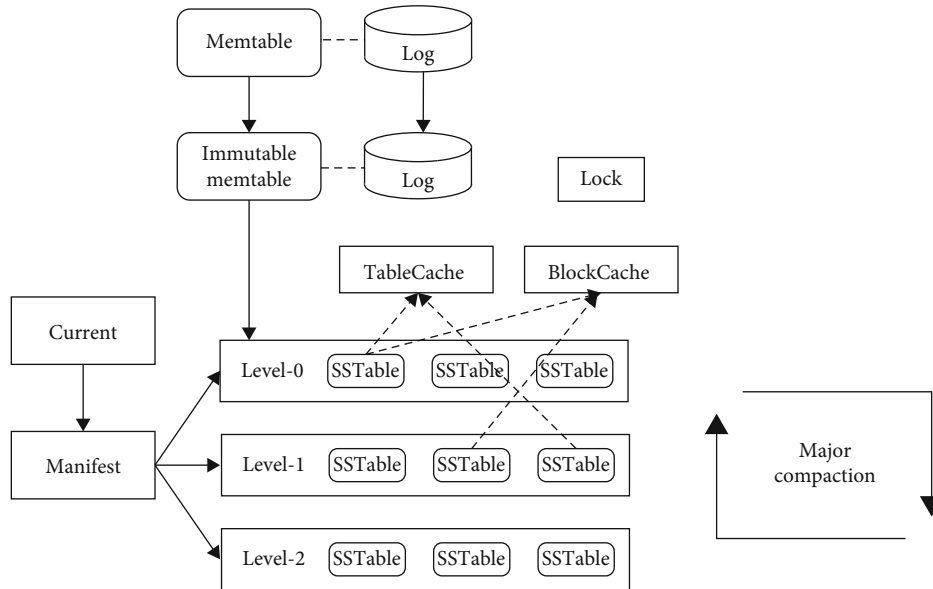


FIGURE 3: LevelDB framework.

The popularity and engagement of Fabric mainly come from its open-source and rapid iteration. At present, the frame has also undergone a relatively big change in the latest 2.0 version [12]. The main technology is as follows: pluggable

consensus mechanism, more flexible intelligent contract, and participant identity-management mechanism [13].

First, Fabric uses a pluggable consensus mechanism [14]. More projects have different requirements on transaction



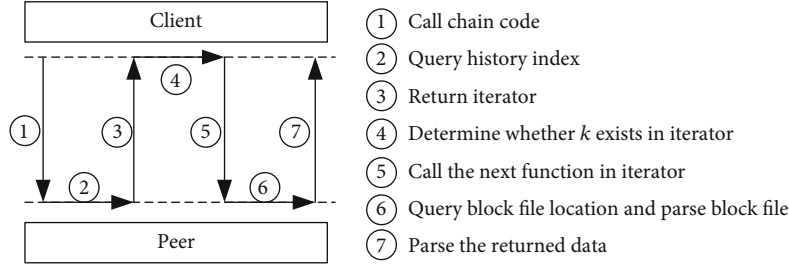


FIGURE 4: GHFK calling process.

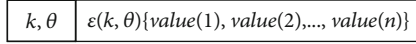
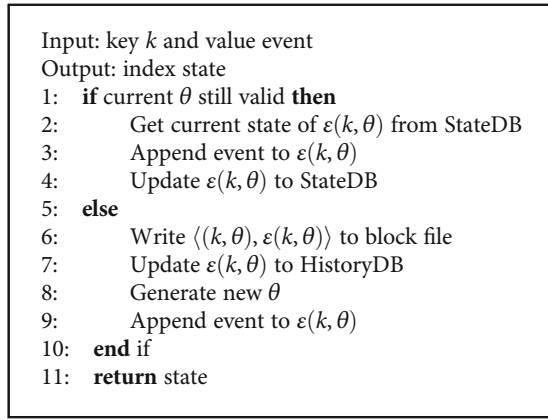


FIGURE 5: TISD structure.

ALGORITHM 1. TISD generate ( $k, event$ ).

effectiveness, timeliness, and throughput in different scenarios, so the requirements on consensus are different. In Fabric, different consensus algorithms (such as Solo, Kafka, Raft, and PBFT) are provided to adapt to different network and trading environments and meet corresponding performance requirements.

Then, Fabric also expands and improves on the smart contract, eliminating the need for a specific programming language and virtual machine like Ethereum [15, 16]. Fabric can support intelligent contracts written in C, Java, JavaScript, Go, and other languages and complete deployment to reduce the difficulty of learning [17].

Finally, according to the number and roles of the parties involved in different usage scenarios, Fabric defines the rights of users and ensures the security of private data, issues certificates, and controls the rights of users. It makes the deployment of intelligent contracts more secure and flexible.

With the rapid development of blockchain technology, it has a natural advantage in such industries as certificate storage and source tracing. At the same time, it also faces great challenges in the process of system construction and practical application. In the Hyperledger Fabric System, querying historical data can only be done through the GetHistoryForKey interface [18, 19]. In the execution process, the chain code ID needs to get the block location and transaction number from history-DB, then parse out the corresponding value from dif-

ferent block files. This has a great impact on the temporal query in this state. With the continuous growth of transaction time, the corresponding data volume, and block file quantity increase, the speed of temporal query is bound to decline rapidly [20].

If the IoT system uses the traditional temporal indexes of the Hyperledger Fabric System, the speed of the temporal query will reduce in IoT [21, 22]. So we propose two index building methods (TISD and TIF). The TISD method is building the temporal indexes based on state databases. The TIF method is building the temporal indexes based on files. These two methods can solve slow query problems, and service deployment processes complicated problems in the Hyperledger Fabric System. These two methods reduce the query time and improve the efficiency of the query. Meanwhile, these two methods also solve the temporal index problem of the Hyperledger Fabric System in IoT. We compared the query times on two datasets and verified our method.

## 2. Related Works

In this section, we will introduce the work related to the use of blockchain technology in IoT.

**2.1. Blockchain.** The blockchain was used as the underlying technology for Bitcoin in the early stage and applied to virtual machines and intelligent contracts in Ethereum [23]. Now, the blockchain as the most widespread technology has been imported into the Hyperledger Fabric System. Each stage represents the different stages of blockchain technology development, but each has the most basic chain structure, organized by block files in order, and each block is linked in chronological order by hash value [24]. In Figure 1, block files include the header section and the block body part. The block header contains the hash value of the last block header, Merkle Tree information, etc. Blocks recorded data related to trading, and each block file links from a chain structure in chronological order by hash value [25]. The blockchain, as a distributed ledger, needs to ensure to reach a consensus between the input and output values of the transaction in the distributed environment. It also maintains the consistency of the data of all parties in the process of bookkeeping [26]. To solve this problem, Bitcoin proposed the concept of consensus algorithm; the algorithm is used to ensure the consistency of the data of each node, so as to achieve the stable development of the network in the presence of malicious nodes to participate in transactions. The current consensus

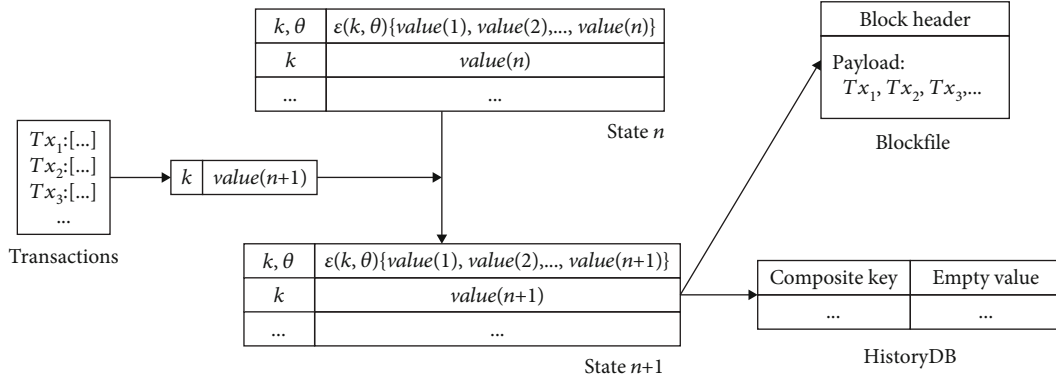


FIGURE 6: TISD construction process.

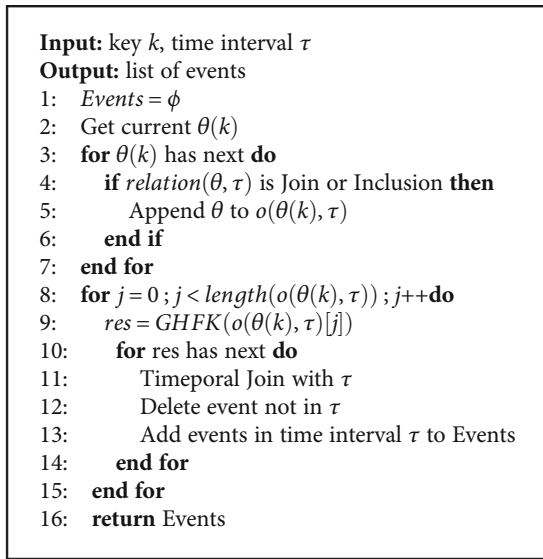
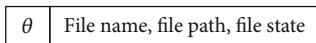
ALGORITHM 2. TISD query  $(k, \tau)$ .

FIGURE 7: TIF construction process.

algorithms are mainly divided into three types: Proof of Work (PoW [27]), Proof of Stake (PoS [27]), and traditional distributed consensus algorithm.

On the block data structure, each blockchain platform uses the Merkle Tree to process transaction data [19]. Merkle Tree is normally a full binary tree; as shown in Figure 2, the bottom of each leaf node represents a transaction data on the blockchain.  $T_0$  is the hash value of  $Tx_0$ 's transaction data.  $T_1$  is the hash value of  $Tx_1$ ,  $H_1$  is the hash value of  $T_0$  and  $T_1$ , and  $T_2$  is the hash value of  $Tx_2$ 's transaction data.  $T_3$  is the hash value of  $Tx_3$ , and  $H_2$  is the hash value of  $T_2$  and  $T_3$ . After the hash computation of every layer, it can produce a hash and store in the block header.

**2.2. Hyperledger Fabric Framework.** The Hyperledger project was established in 2015, led by the Linux Foundation, and attracted projects including IBM, Intel, and other companies contributed several blockchain platforms like Fabric [28].

Fabric is an open-source enterprise blockchain platform, which provides a highly modular and configurable architecture. It can be widely applied to multiple industries [29]. At present, Fabric has been applied in many fields such as banking, financial institutions, and insurance.

Fabric needs to be more flexible in the context of enterprise usage. So far, the following options are provided in different versions of Fabric: Solo, Kafka [30], SBFT [31], and Raft.

Solo mode is the single-node communication mode. In this environment, there is only one sort of service node, and messages sent from Peer point are sorted by this node. The availability and scalability are limited, so it is not suitable for production environment and is generally used for development and test environment.

Kafka mode is the processing of sorting information provided by Kafka service. Kafka is an open-source project of Apache that mainly provides distributed message processing and distribution services. Each Kafka cluster is composed of multiple nodes and supports fault tolerance.

SBFT is a simple Byzantine algorithm. Compared with Kafka, it can tolerate fault nodes and a certain number of malicious nodes.

In Fabric, there are four kinds of nodes participating in the network: Peer node, Orderer node, Certificate Authority node, and Client node [32].

The Peer node is divided into four nodes: accounting node, endorsement node, master node, and anchor node. Each Peer node is a billing node in the channel, responsible for receiving and verifying data blocks sent from the sorting service while maintaining a copy of the ledger.

The Orderer node is received transactions containing endorsement signatures, packages them into blocks, and broadcasts them to Peer nodes. It can ensure the logical order of transactions and ensure that all nodes on the chain receive the same message.

Certificate Authority node is to issue identity information to other nodes in the network, which is the certificate authority in Fabric.

Client node is an entity directly operated by users. It participates in the communication of the blockchain network by connecting to a Peer node or an Orderer node.

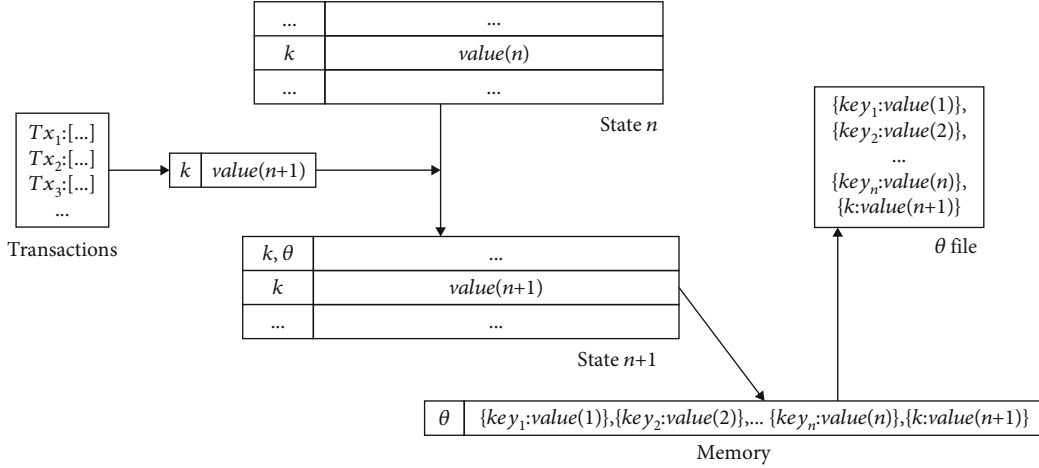
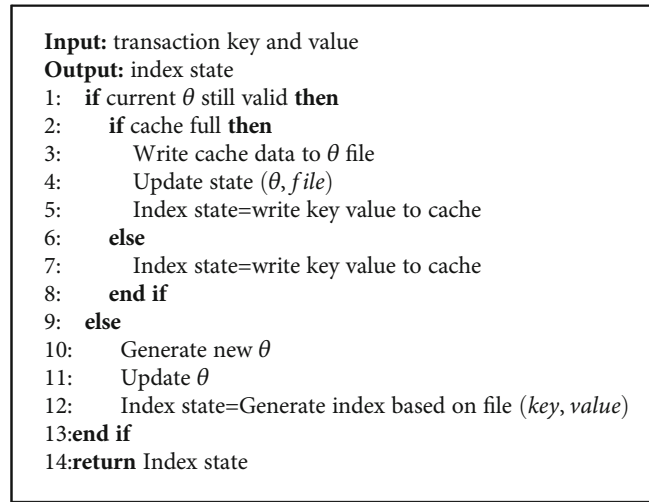


FIGURE 8: TIF construction process.

ALGORITHM 3. TIF generate ( $key, value$ ).

Fabric's data is stored in block file and database, respectively. Block file mainly stores transaction information, including hash value and block packaging time. For the database, from the perspective of database type, it can be divided into Couch DB [33] and LevelDB [34], which can be specified through the configuration file, and LevelDB is selected by default. From the perspective of database usage, there is a ledger index for storing account ID, a block index for storing block, a state database for the current latest state of transactions on the storage chain, and a history database for storing valid parts of the transaction information [35].

**2.3. Level DB.** LevelDB is a key-value storage engine developed by Google. LevelDB, like most KV systems, also has a simple operation interface and basic operations that include writing record, reading record, and deleting record [36]. LevelDB is widely used in various projects. The general architecture of LevelDB is shown in Figure 3.

Memtable is a storage mode in memory, with the data structure of skip table as the default mode [37]. When per-

forming a data write, it writes to Memtable first, and immutable Memtable changes to read-only Memtable when its data size reaches the threshold; and then, compression threads in the background change immutable Memtable to an SSTable file for storage on disk.

SSTable is a data persistence file, which is an orderly arrangement of keys within the file [38]. The first part of the file is the data, followed by the metadata for the index.

MANIFEST file contains the key range and the hierarchy. The version of MANIFEST file is changed when the database is reopened. If the database is opened, a new file will be generated each time.

CURRENT file is the file name of MANIFEST files [39]. CURRENT file can be used to locate the MANIFEST file to restore the database in the event of a failure, such as a power outage.

LOCK file is used to control multiprocess access to the database [37]. When a process opens the database, an exclusive file lock will be added to the file. If the process finishes, the lock will be automatically released.

```

Input: key  $k$ , time interval  $\tau$ 
Output: list of events
1: Events= $\phi$ 
2: Get  $\theta$  from StateDB
3: for  $\theta$  has next do
4:   if  $relation(\theta, \tau)$  is Join of Inclusion then
5:     Append  $\theta$  to  $o(\theta, \tau)$ 
6:   end if
7: end for
8: for  $j = 0 ; j < length(o(\theta, \tau)) ; j++$  do
9:    $s = GetState(\theta)$ 
10:  if  $s! = nil$  then
11:    Read file to memory
12:    Parse file
13:    Events=temporal
14:  else
15:    Read memory
16:    Events=temporal join
17:  end if
18: end for
19: for  $i = 0 ; i < length(Events) ; i++$  do
20:  if Events  $[i]$  not belong to  $k$  then
21:    Remove Events  $[i]$  from Events
22:  end if
23: end for
24: return Events

```

ALGORITHM 4. TIF query ( $k, \tau$ ).

**2.4. IoT System.** The IoT system connects the Internet and information-sensing equipment to achieve intelligent control and management of all objects. It can be divided into three layers: Perception Layer [40], Network Layer, and Application Layer. Perceptual Layer is responsible for object collection and data processing. Network Layer is responsible for transmitting the collected data. Application Layer provides IoT-based applications [41].

The IoT system usually includes embedded devices with resource constraints. As an important part of IoT, sensors will face some technical challenges in practical applications [42]. First, due to the limitations of low cost, low power consumption, and small size of sensors, these limit sensors' computing, storage, and communication capabilities, thereby affecting the expansion capabilities of the network [43]. Second, most sensors are deployed in unattended areas, so sensor security issues are particularly prominent. Third, since the monitoring and recording capabilities of sensors are often opaque, when sensors share data information, they will cause data information leakage. The IoT system is being integrated with various technologies to solve various problems, such as Liang W who proposed a fast defogging image recognition algorithm based on bilateral hybrid filtering to solve IoT image issues in foggy weather [44].

Blockchain has significant cryptographic security and immutability [8]. With its characteristics of decentralization, consensus mechanism, and nontamper ability, IoT can use the advantages of blockchain to solve its security and scalability issues [45]. The decentralization of blockchain enables IoT devices to directly obtain information without a central server, which reduces the problem of high operating costs

for central institutions. But the IoT system uses the traditional temporal indexes that cannot meet IoT's needs. We propose two index building methods to solve this issue.

### 3. Efficient Temporal Index

Fabric distinguishes between the historical state and the current state of the data [46]. The data of transactions are stored in LevelDB in the form of key-value pairs. For each key in the transaction, there are multiple states corresponding to it. The latest state is called the current state, and other states are called historical state [47].

The state database stores the current state of the key, while the history database stores only the index location of the historical data on the block file, which is stored on disk [48]. The historical data is inserted in chronological order and distributed in different block files, so the efficiency of processing the historical data is relatively low.

In Fabric, there is no interface for temporal queries in the system. When we need to analyse the historical data, we call the GHFK function to get an iterator. Through the data obtained by iterator that is connected with the corresponding time interval in memory, we realize the temporal query. GHFK function can return all the history data for the committed valid  $k$ . The calling process is shown in Figure 4.

For example, there is many trading information in the time interval  $[0, T_1]$ . If we want to query the transaction information in the time interval  $[0, T_2]$  ( $T_2 < T_1$ ), we need to call GHFK function to access large amounts of data, deserialize the block file, and connect the data to the time interval. If we want to query the transaction information in the time interval  $[T_2 < T_1]$ , we should connect the data to the time interval  $[0, T_1]$ . In other words, the data is useless in the time interval  $[0, T_2]$ . It is a waste to read and deserialize the data in the time interval  $[0, T_2]$ .

As time goes on, the block file that needs to be deserialized is increasing by transaction volume and data volume [49]. It will inevitably lead to the decline of query efficiency with the change of query interval.

In this part, we propose two methods which are temporal indexes based on state database and file in Fabric to solve this problem. It can improve the efficiency of temporal query in Hyperledger Fabric.

**3.1. Temporal Index Based on State Databases.** The reason for the low efficiency of Fabric temporal query is greatly related to the number of reads and writes to the database and the number of accesses to the file; especially, when the query volume is relatively large, the efficiency will significantly decrease. In our method, we divide the transaction into corresponding intervals according to such criteria as time intervals and add indexes to the intervals to speed up the temporal query. In this section, we will introduce how to create a temporal index (TISD: temporal index based on state databases).

In the process of constructing a temporal index, let  $t_1$  be the starting time of the temporal index and  $t_2$  be the starting time of the next build process. For each entity  $k$  in the transaction, we divide  $[t_1, t_2]$  into many time frames  $\theta(k) = \{\theta_1,$

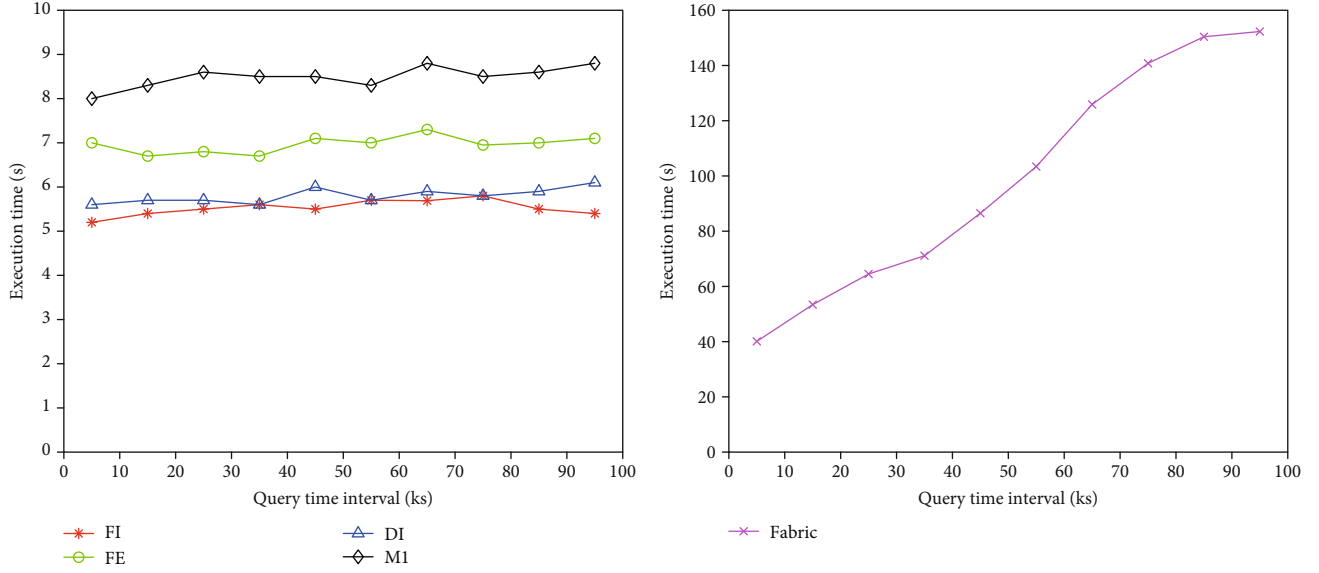


FIGURE 9: Dataset UD, network structure T1, and TISD query time.

$\theta_2, \dots, \theta_m\}$ , and every time frame  $\theta_i$  is adjacent. We build temporal index for every  $k$  in every time frame  $\theta_i$ .

In Figure 5, for entity  $k$ , let  $\varepsilon(k, \theta)$  represent a set of events that relate to  $k$  and occur in time frame  $\theta$ . Let the key-value  $\langle k, \theta \rangle$  insert the state database, where  $\langle k, \theta \rangle$  represents the composite value and  $\varepsilon(k, \theta)$  represents the value. It is useful to speed up the temporal index.

When the data is submitted to the state database, we build an index of the time state of the data. The construction process of the index is as shown in Algorithm 1. First, you need to determine the current time interval  $\theta_n$  to verify and the current time interval is valid. If  $\theta_n$  is valid, we use *GetState*( $\langle k, \theta_n \rangle$ ) to obtain  $\varepsilon(k, \theta_n)$  and update the current status.

As shown in Figure 6, the status of  $\langle k, \theta_n \rangle$  is updated from  $n$  to  $n+1$ ; it also means the current event  $value_{n+1}$  is added to  $\varepsilon(k, \theta_n)$ . At the same time, the value of  $k$  is updated from  $value_n$  to  $value_{n+1}$ . If  $\theta_n$  satisfies the separation condition, it will generate a new time interval  $\theta_{n+1}$ . If  $\theta_n$  is invalid, the status of  $\langle k, \theta_n \rangle$  will update to  $\langle k, \theta_n \rangle$  and generate a new event  $\langle k, \theta_{n+1} \rangle, \varepsilon(k, \theta_{n+1})$ .

**Algorithm 1:** TISD generate ( $k, event$ ). Input: key  $k$  and value event

Output: index state

- 1: **if** current  $\theta$  still valid **then**
- 2:     Get current state of  $\varepsilon(k, \theta)$  from StateDB
- 3:     Append event to  $\varepsilon(k, \theta)$
- 4:     Update  $\varepsilon(k, \theta)$  to StateDB
- 5: **else**
- 6:     Write  $\langle (k, \theta), \varepsilon(k, \theta) \rangle$  to block file
- 7:     Update  $\varepsilon(k, \theta)$  to HistoryDB

- 8:     Generate new  $\theta$
- 9:     Append event to  $\varepsilon(k, \theta)$
- 10: **end if**
- 11: **return** state

During index building, we need to divide the time into some time intervals  $\theta$ , the time intervals are continuous, and all data events are included. We use three times interval segmentation methods: FI (fixed time interval), FE (fixed event number), and DI (dynamic interval).

FI: In the total length of time, it builds a temporal index in the fixed time interval. Each entity may match a different number of events in each time interval by different trading situations. Therefore, the efficiency may be erratic.

FE: In this model, time intervals  $\theta$  are determined only by a fixed event number. The length of temporal index may have a big gap in each entity by different trading situations. For frequently updated entity values, the index is also frequently updated. There may be multiple time intervals in a short period of time, and the database may be accessed multiple times during the query.

DI: The time interval is determined by calculating the time and measuring the number of events. A time interval or several events are fixed, and the time interval must be determined in one of two ways. One is that the number of events must equal or exceed the specified number of events when the time interval is equal to a fixed value. Another is that the interval must be at least fixed when the number of events is equal to a fixed value, so it is able to avoid that events occur too much or too little in a time interval.

**3.2. TISD Query Process Analysis.** To illustrate the query process, we define four relations: temporal joined relation, temporal connected relation, temporal included relation, and



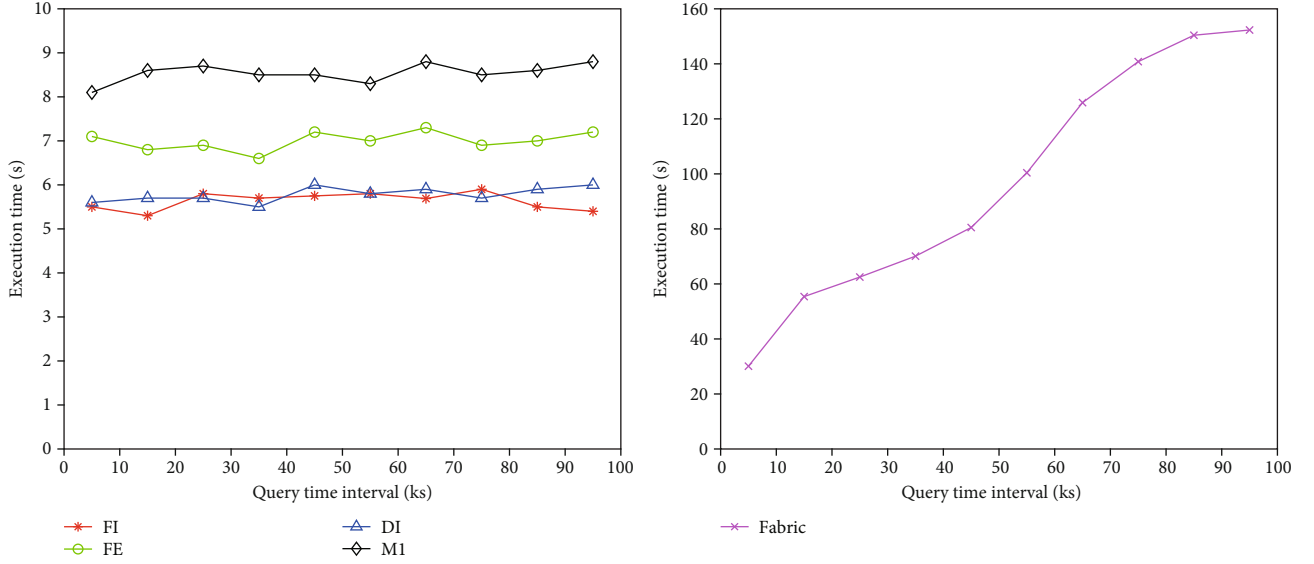


FIGURE 10: Dataset UD, network structure T2, and TISD query time.

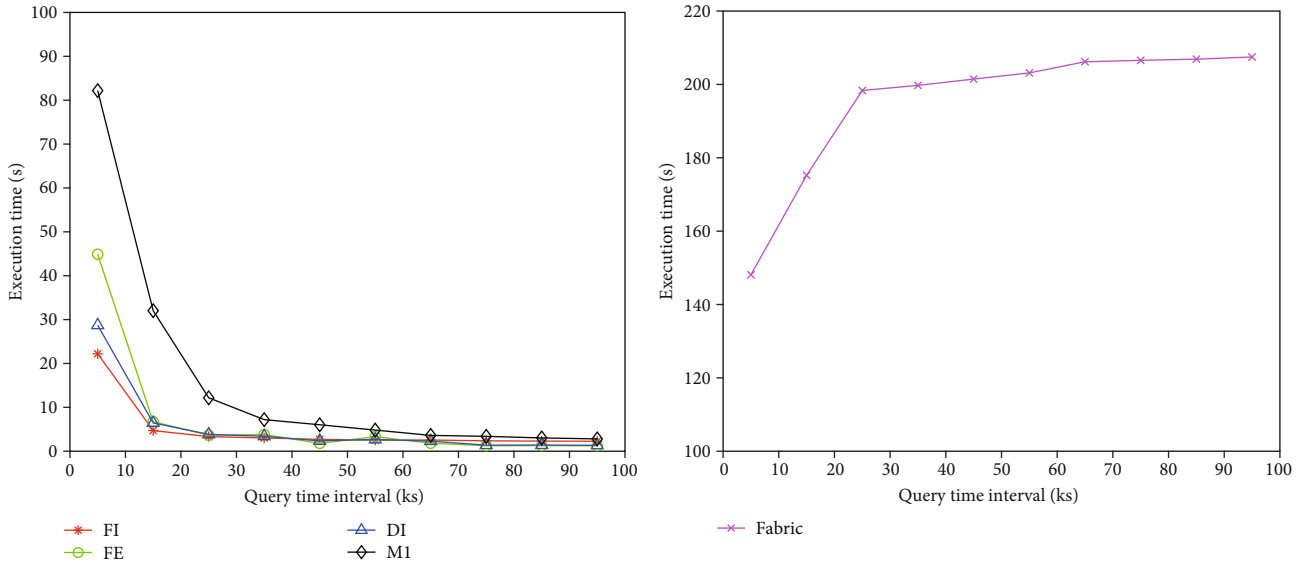


FIGURE 11: Dataset ZD, network structure T1, and TISD query time.

no temporal relation [50]. Let

$$\text{relation}(\theta_i, \theta_j) = \begin{cases} \text{Join} & \theta_i \cap \theta_j \neq \phi \\ \text{Connection} & \exists \theta_m \Rightarrow \theta_i \cap \theta_m \neq \phi, \theta_m \cap \theta_j \neq \phi \\ \text{Inclusion} & \theta_i \subseteq \theta_j \\ \text{None} & \text{otherwise,} \end{cases} \quad (1)$$

where *Join* represents temporal joined relation, *Inclusion* represents temporal included relation, *Connection* represents temporal connected relation, and *None* represents no relation between two intervals.

The query process is shown in Algorithm 2,  $\varepsilon(k, \tau)$  is all events about  $k$  in the time interval  $\tau$ . The algorithm queries

$k$  and time interval  $\theta(k)$  by the iterator returned of *GetStateByRange* and obtains  $o(\theta(k), \tau)$ , where  $o(\theta(k), \tau)$  represents an interval that has temporal joined relation or temporal included relation between  $\theta(k)$  and the target query interval. There is a temporal connected relation between the first  $\theta$  and the last  $\theta$  in  $o(\theta(k), \tau)$ .

**Algorithm 2:** TISD query  $(k, \tau)$ . **Input:** key  $k$ , time interval  $\tau$

**Output:** list of events

- 1:  $Events = \phi$
- 2: Get current  $\theta(k)$
- 3: **for**  $\theta(k)$  has next **do**
- 4:     **if**  $\text{relation}(\theta, \tau)$  is Join or Inclusion **then**

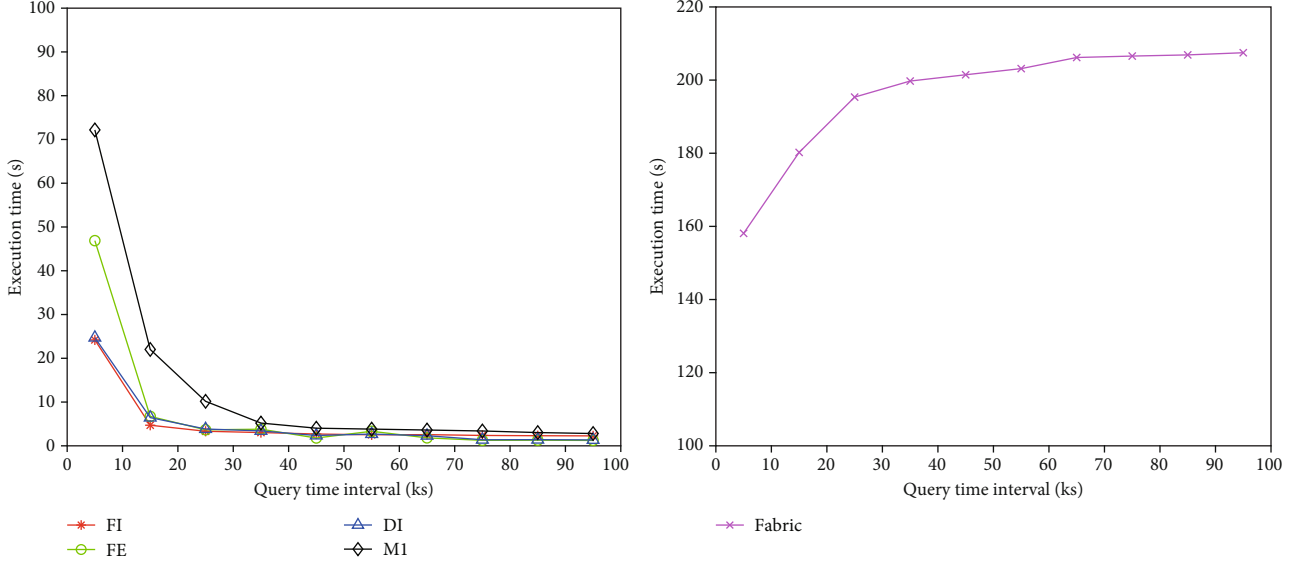


FIGURE 12: Dataset ZD, network structure T2, and TISD query time.

TABLE 1: TISD data insertion time comparison (seconds).

Dataset	TISD			Fabric
	FI	FE	DI	
UD	239.19	231.72	232.31	227.26
ZD	259.12	262.79	255.63	228.59

TABLE 2: TISD data insertion space comparison (megabytes).

Dataset	TISD			Fabric
	FI	FE	DI	
UD	191.97	191.96	191.80	103.5
ZD	191.81	191.97	191.78	103.5

```

5:   Append  $\theta$  to  $o(\theta(k), \tau)$ 
6:   end if
7: end for
8: for  $j = 0 ; j < \text{length}(o(\theta(k), \tau)) ; j + +$  do
9:    $res = GHFK(o(\theta(k), \tau)[j])$ 
10:  for  $res$  has next do
11:    Temporal Join with  $\tau$ 
12:    Delete event not in  $\tau$ 
13:    Add events in time interval  $\tau$  to Events
14:  end for
15: end for
16: return Events

```

For each  $\theta$  in  $o(\theta(k), \tau)$ ,  $GHFK(\langle k, \theta \rangle)$  is performed. The block file is parsed through the returned iterator. For

the interval with temporal included relation, the data parsed by the iterator is appended to the result sets. For the interval with temporal joined relation, the data returned by the iterator is traversed to remove the data not in the interval  $\tau$ .

In the temporal query process, the efficiency of the query is mainly measured by the query time, which depends on the rate of events, the size of the index interval, and the size of the query interval. Therefore, how to choose the appropriate index interval becomes a key problem.

For the temporal query performed by Fabric,  $T_{qk\tau}$  is used to represent the query time of the historical state of the keyword  $k$  in the time interval  $\tau(t_s, t_e)$ , which can be expressed as

$$T_{qk\tau} = \text{num}(E(k, \tau)) \times T_{it}, \quad (2)$$

where  $E(k)$  represents events about the keyword  $k$  and  $\text{num}()$  represents the number of events in the query time.

In the normal process of data insertion, we use  $V_k$  to represent the insertion rate of events related to the keyword  $k$ , which can be expressed as

$$V_k = \frac{\text{num}(E(k, T))}{T}, \quad (3)$$

where  $T$  represents the total length of time the event inserted.

Since the first transaction in the system needs to be iterated in the Fabric query process,  $T$  can be expressed as a period of time, starting from the initial transaction point  $t_0$  and ending at a larger time point in the target query interval  $\tau$ . So

$$T_{qk\tau} = V_k \times T \times T_{it} = V_k \times (\max(t_s, t_e) - t_0) \times T_{it}. \quad (4)$$

For the FI method, the index construction is determined by a fixed time length. For the total time length  $T$  and the

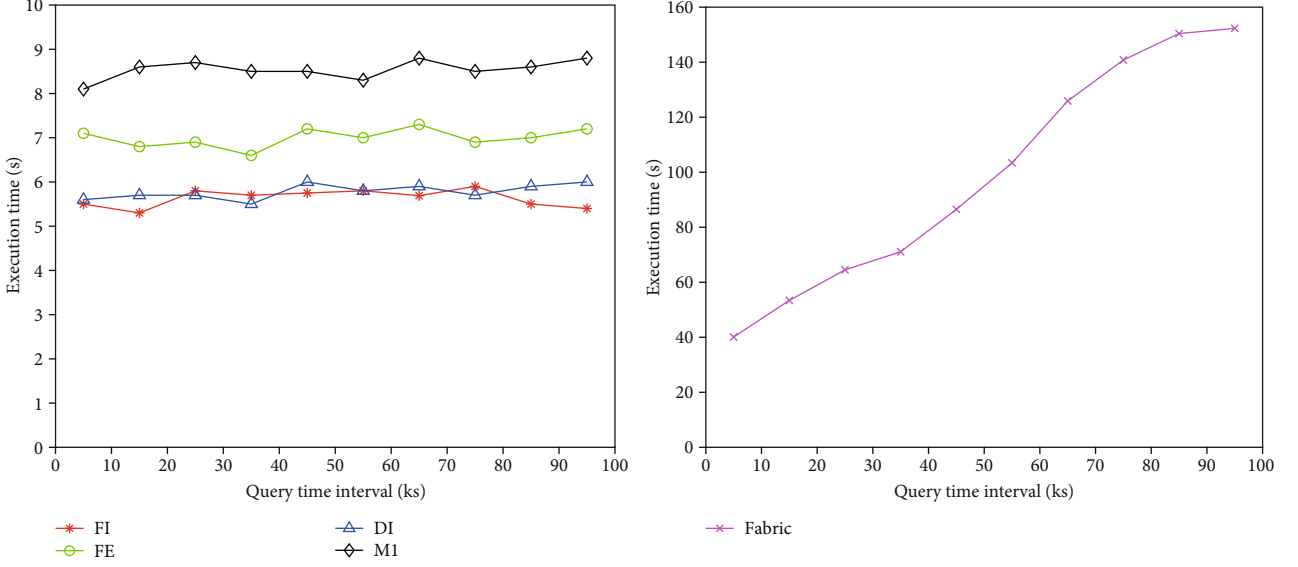


FIGURE 13: Dataset UD, network structure T1, and TIF query time.

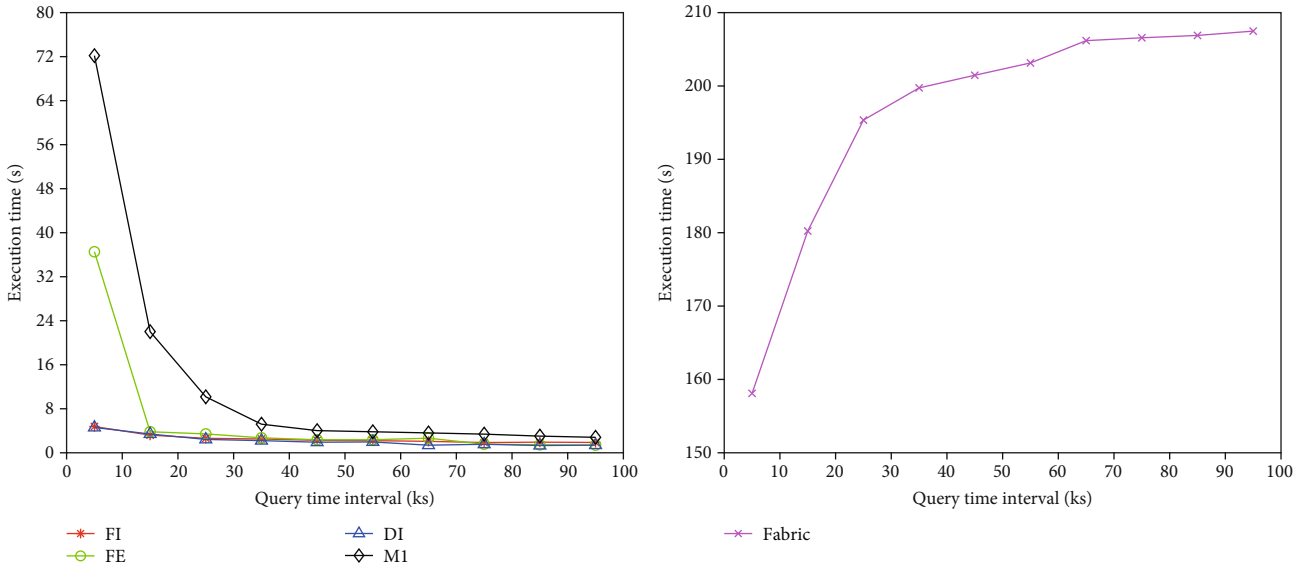


FIGURE 14: Dataset ZD, network structure T1, and TIF query time.

given fixed time length  $T_f$ , let

$$\text{num}(\theta, T) = \frac{T}{T_f}, \quad (5)$$

where  $\theta$  represents the time interval divided,  $\text{num}()$  represents the number of partitions for all time intervals.

The query time of the historical state  $T_{qk\tau}$  can be defined as

$$T_{qk\tau} = o(\theta(k), \tau) \times T_{it}. \quad (6)$$

The target query interval must be less than or equal to the

total length of time, so

$$T_{qk\tau} \leq \frac{T}{T_f} \times T_{it}. \quad (7)$$

With the increase of  $T_f$ , the query time will be reduced correspondingly. In the limit, it only needs one iteration to realize the query, but this situation is not realistic in the practical application.

For the FE method, the division of time intervals is controlled by a fixed number of events. Let

$$\text{num}(\theta, T) = \frac{\text{num}(E(k, T))}{C}, \quad (8)$$

TABLE 3: Dataset UD, network structure T2, and TIF query time (s).

Query range	TIF				
	FI	FE	DI	M1	Fabric
0-10 K	5.21	7.01	5.68	8.02	42.09
10-20 K	5.43	6.72	5.71	8.29	53.42
20-30 K	5.52	6.83	5.72	8.55	64.55
30-40 K	5.58	6.75	5.69	8.48	71.12
40-50 K	5.57	7.12	6.01	8.53	86.53
50-60 K	5.71	7.03	5.84	8.32	103.44
60-70 K	5.69	7.33	5.91	8.67	125.98
70-80 K	5.82	6.95	5.77	8.54	140.86
80-90 K	5.53	7.11	5.92	8.61	150.39
90-100 K	5.44	7.08	6.08	8.78	152.33

TABLE 4: Dataset ZD, network structure T2, and TIF query time (s).

Query range	TIF				
	FI	FE	DI	M1	Fabric
0-10 K	4.77	36.54	4.6	72.18	158.12
10-20 K	3.21	3.82	3.41	22.03	180.23
20-30 K	2.63	3.43	2.43	10.17	195.35
30-40 K	2.51	2.72	2.21	5.21	199.74
40-50 K	2.26	2.37	1.92	4.03	201.46
50-60 K	2.20	2.37	1.97	3.82	203.14
60-70 K	2.08	2.65	1.38	3.61	206.18
70-80 K	1.86	1.57	1.55	3.39	206.57
80-90 K	1.93	1.45	1.32	3.03	206.89
90-100 K	1.88	1.39	1.39	2.81	207.48

where  $C$  is the fixed number of events set. So

$$T_{qk\tau} \leq \frac{V_k}{C} \times T \times T_{it}. \quad (9)$$

When the FE method is used to divide the time interval, within the normal range, the temporal query time is negatively correlated with the number of fixed events and positively correlated with the event occurrence rate.

For the DI method, the division of time interval is determined by the number of fixed events and the length of fixed time. Let

$$num(\theta, T) \leq \min \left( \frac{T}{T_f}, \frac{num(E(k, T))}{C} \right), \quad (10)$$

where  $num(\theta, T)$  represents the number of intervals generated in total time  $T$ . In the query,  $T_{qk\tau}$  represents the query time of the historical state of the keyword  $k$  in the time interval  $\tau$ , and the target time interval  $\tau$  of the query is not more

than the total time length  $T$ , so

$$T_{qk\tau} \leq num(\theta, T) \times T_{it} \leq \min \left( \frac{T}{T_f}, \frac{V_k \times T}{C} \right) \times T_{it}. \quad (11)$$

Therefore, in the DI method, the temporal query time of the keyword  $k$  is negatively correlated with the fixed time interval  $T_f$  and the fixed number of events  $C$ . It is positively correlated with the event occurrence rate  $V_k$ .

During the query, the GHFK function is used in Fabric. When the traditional method is used to query the keyword  $k$ , the GHFK will generate a lot of access to the ledger index, as well as the access, deserialization, and parsing of files. But using temporal index only needs to deserialize  $o(\theta(k), \tau)$  times files, that is to say, using reasonable time intervals to build temporal index can greatly reduce the number of file access.

**3.3. Temporal Index Based on Files.** When TISD (temporal index based on state databases) builds indexes, it will increase the number of database accesses and the size of block files. It may have an impact on normal transactions on the blockchain as the data volume is extremely large or the disk space is high. Considering the impact of index construction on database read-write and block file growth, we propose TIF (temporal index based on files) that builds indexes without affecting the normal blockchain storage.

In order to reduce the impact on the blockchain storage space, we will explain by two aspects. One is for state database: TIF only saves the latest state of the interval and the corresponding index file information. Another is for block files: TIF will not write temporal index data to the block file.

The TIF structure is shown in Figure 7. For time interval  $\theta$ , index files related to  $\theta$  are marked such as file name, file path, and file state, and index data is not added to block files in the form of transactions.

The index construction process is as shown in Figure 8 and Algorithm 3. After the verified transaction data is generated, it writes the corresponding data to the status database, updates the database to the latest state, and checks the current existing time interval  $\theta$ . If  $\theta$  is invalid, it will regenerate  $\theta$ , update the latest information to the database, and regenerate the index.

If  $\theta$  is valid, it will check enough space allocated in memory. If memory space is enough, it will append the events generated to memory in the agreed format and classify the events by the corresponding time interval. It also updates the latest information.

**Algorithm 3:** TIF generate (*key, value*). **Input:** transaction key and value

**Output:** index state

- 1: **if** current  $\theta$  still valid **then**
- 2:     **if** cache full **then**
- 3:         Write cache data to  $\theta$  file
- 4:         Update state ( $\theta, file$ )

```

5:     Index state=write key value to cache
6:  else
7:     Index state=write key value to cache
8:  end if
9:  else
10:   Generate new  $\theta$ 
11:   Update  $\theta$ 
12:   Index state=Generate index based on file ( $key, v$ 
     $alue$ )
13:end if
14:return Index state

```

**3.4. TIF Query Process Analysis.** The TIF query process algorithm is shown in Algorithm 4, where  $\varepsilon(k, \tau)$  represents all events about  $k$  in the time interval  $\tau$ . The iterator returned by `GetStateByRange` queries the interval partition and divides  $\theta$ . Let  $o(\theta, \tau)$  represent a time interval that is joined and included between the target time interval and  $\theta$  by relation function. For each  $\theta$  of  $o(\theta, \tau)$ , it will get the file name, file path, file state, and other information by `GetState( $\theta$ )`. Then, the file state identifies whether the data has been written into memory. If the data is in memory, it will join and calculate the temporal directly, filter the keyword, and return the query results. If the data is not in memory, it will take the data into the memory, parse the data, make temporal connection to the parsed data, filter the results of the temporal connection, and select the keyword  $k$  as the returned value.

**Algorithm 4:** TIF query ( $k, \tau$ ). **Input:** key  $k$ , time interval  $\tau$

**Output:** list of events

```

1:  Events= $\phi$ 
2:  Get  $\theta$  from StateDB
3:  for $\theta$  has next do
4:    if $relation(\theta, \tau)$  is Join of Inclusion then
5:      Append  $\theta$  to  $o(\theta, \tau)$ 
6:    end if
7:  end for
8:  for $j = 0 ; j < length(o(\theta, \tau)) ; j + +$ do
9:     $s = GetState(\theta)$ 
10:   if $s! = nil$ then
11:     Read file to memory
12:     Parse file
13:     Events=temporal
14:   else

```

```

15:     Read memory
16:     Events=temporal join
17:   end if
18: end for
19: for $i = 0 ; j < length(Events) ; i + +$ do
20:   if Events [ $i$ ] not belong to  $k$ then
21:     Remove Events [ $i$ ] from Events
22:   end if
23: end for
24: return Events

```

In terms of temporal query time, the use of temporal index can reduce the consumption of time to some extent, improve query efficiency, and speed up the query, but in the process of building and maintaining temporal index, there will be some extra costs, and the main costs are time consumption and storage space consumption.

In the storage space consumption, using TIF to build an index requires only one key-value pair associated with the time interval. The value is maintained in the database. When the time interval is updated or the memory capacity reaches the threshold, the value is updated. So TIF can reduce read-write times and space usage on database.

In the time consumption, the generation of indexes is carried out at the same time as the transaction. First, the data is written into memory, the data in memory is classified, the index is established, and then the file is written. Writing to the file can be done asynchronously, so the time consumption of this process is mainly memory reading and writing. Due to the memory bandwidth, the time consumption has little impact on the business logic.

TISD takes advantage of the fast reading and writing of the database, determines the time interval in various ways, and builds the index for the data in chronological order. It reduces the reading and deserialization of the block file and speeds up the query of the historical data. With the minimizing influence of the system efficiency, TIF stores transaction information by using memory as cache and file as a subject. It avoids the state database and historical database many times to read and write and takes up the space of the database.

## 4. Experiments and Results

In this section, we will introduce the experimental data and experimental results.

**4.1. Experimental Data.** Since there is no dataset specific to blockchain query in Fabric, we generate two datasets based on usage scenarios: UD (uniform distribution data) and ZD (Zipf distribution data).

UD: There are 520 entities, including 400 cargoes, 100 containers, and 20 truck entities. The events of the transaction include the loading and unloading of cargo, the loading,



and unloading of containers and require each entity to produce 2,000 transactions in a total of 100,000 seconds. All events are even inserted into the blockchain in chronological order.

ZD: The number of entities, number of events, and total length of time are the same as UD. But events are inserted into the blockchain in a chronological Zipf distribution.

The Fabric platform is deployed using the following two network architectures:

T1: There are 1 Peer node and 1 Orderer sorting node, and the sorting service adopts solo.

T2: There are 4 Peer nodes and 1 Orderer sorting node, and the sorting service adopts solo.

## 4.2. Experimental Results

**4.2.1. TISD Query.** First, we evaluate the query time using TISD on datasets UD and ZD and network structures T1 and T2. Then, the time and space costs during index building are also evaluated.

Figure 9 is TISD query time on dataset UD and network structure T1. Due to the GHFK function, the query time increases with the temporal query interval, while the M1 model and TISD trend basically remain stable with the temporal query interval. Due to the reason of interval division, FI, FE, and DI differ to some extent. However, compared with the original method in M1 and Fabric, they have better performance, which verifies the high efficiency of TISD structure.

Figure 10 is TISD query time on dataset UD and network structure T2. The temporal query trend is similar to that in Figure 9. That is to say, the network structure has little effect on the temporal query.

Figure 11 is TISD query time on dataset ZD and network structure T1. Due to the GHFK function and dataset ZD, the query time increases with the temporal query interval. Figure 12 is TISD query time on dataset ZD and network structure T2. The temporal query trend is similar to that in Figure 11.

When using indexes, there is also a certain amount of time and space overhead in the index building process. In Table 1, the construction of index consumes many times in the process of data writing, but it consumes a small proportion of the total time on network structure T1. The extra time by index building has increased by up to about 2.2% on dataset UD. The extra time by index building has increased by up to about 14.9% in dataset ZD.

In Table 2, it shows the comparison of the disk space occupied on network structure T2. Due to the construction of the index, the size of the block file will increase significantly. Since the size of the transaction data will not be different due to different data distribution and time interval division, the data distribution and time interval division basically have no impact on the size of the generated block file.

**4.2.2. TIF Query.** In this part, we evaluate the query time using TIF on datasets UD and ZD and network structure T1.

Figure 13 is TIF query time on dataset UD and network structure T1. The query time of Fabric is the most time-consuming, while the other methods take less time to execute and perform more steadily. FI and DI have similar time interval divisions, so the performance of query time is nearly consistent. The temporal query using TIF is superior to Fabric and M1.

Figure 14 is TIF query time on dataset ZD and network structure T1. The query time of Fabric is the most time-consuming. Due to the uneven distribution of data, the execution time of FI, FE, and DI is relatively high in the initial stage. But in general, the query time of FI, FE, and DI is better than that of Fabric and M1.

Tables 3 and 4 show the performance of TIF in query time using FI, FE, and DI time segmentation methods on network structure T2.

Table 3 is TIF query time on dataset UD and network structure T2.

Table 4 is TIF query time on dataset ZD and network structure T2.

All experimental results show that, for different business scenarios, different index building methods and time interval partitioning methods have different performance in temporal query efficiency. In terms of overall performance, TIF has certain advantages compared with other methods under DI.

## 5. Conclusion

This paper proposes two temporal indexes (TISD and TIF) on the Hyperledger Fabric blockchain platform. The experimental results show that the two temporal indexes and three time interval partitioning methods proposed in this paper can improve the efficiency of temporal query in Fabric to a certain extent on different distributed data while ensuring certain time and space overhead. It can also solve the problem of a low access speed of using temporal indexes of the Hyperledger Fabric System in IoT. Our research can use blockchain technology in IoT system more seamlessly.

## Data Availability

The UD (uniform distribution data) and ZD (Zipf distribution data) data used to support the findings of this study are available from the corresponding author upon request.

## Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

## Acknowledgments

This work is supported by the National Nature Science Foundation of China under grant 61370198 and grant 61300187, the Xiamen Science and Technology Foundation of China under grant 3502Z20183047, and in part by the Liaoning Provincial Natural Science Foundation of China under grant 2019-MS-028.

## References

- [1] S. Sciancalepore, G. Piro, G. Boggia, and G. Bianchi, "Public key authentication and key agreement in IoT devices with minimal airtime consumption," *IEEE Embedded System Letter*, vol. 9, no. 1, pp. 1–4, 2017.
- [2] J. Han and J. Kim, "A lightweight authentication mechanism between IoT devices," in *Information and Communication Technology Convergence (ICTC)*, pp. 1153–1155, Piscataway, NJ, 2017.
- [3] W. Liang, S. Xie, D. Zhang, X. Li, and K. C. Li, "A mutual security authentication method for RFID-PUF circuit based on deep learning," *ACM Transactions on Internet Technology*, vol. 1, 2020.
- [4] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering (TNSE)*, vol. 7, no. 2, pp. 766–775, 2020.
- [5] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, "Blockchain empowered arbitrable data auditing scheme for network storage as a service," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 289–300, 2020.
- [6] E. Portmann, "Rezenion: blockchain: blueprint for a new economy," *HMD*, vol. 55, no. 6, pp. 1362–1364, 2018.
- [7] V. Buterin, *Ethereum: a Next-Generation Smart Contract and Decentralized Application Platform*, 2014.
- [8] W. Liang, L. Xiao, K. Zhang, M. Tang, D. He, and K. C. Li, "Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems," *IEEE Internet of Things Journal*, 2021.
- [9] E. Androulaki, A. Barger, V. Bortnikov et al., "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *The Thirteenth EuroSys Conference*, pp. 1–15, New York, NY, USA, 2018.
- [10] Y. Xu, C. Zhang, G. Wang, Z. Qin, and Q. Zeng, "A blockchain-enabled deduplicatable data auditing mechanism for network storage services," *IEEE Transactions on Emerging Topics in Computing*, 2020.
- [11] A. Pinna, S. Ibba, G. Baralla, R. Tonelli, and M. Marchesi, "A massive analysis of Ethereum smart contracts empirical study and code metrics," *IEEE Access*, vol. 7, pp. 78194–78213, 2019.
- [12] C. S. Jensen, J. Clifford, S. K. Gadia, A. Segev, and R. T. Snodgrass, "A glossary of temporal database concepts," *ACM Sigmod Record*, vol. 21, no. 3, pp. 35–43, 1992.
- [13] Y. Xu, C. Zhang, Q. Zeng, G. Wang, J. Ren, and Y. Zhang, "Blockchain-enabled accountability mechanism against information leakage in vertical industry services," *IEEE Transactions on Network Science and Engineering*, 2020.
- [14] G. Wu and U. Dayal, "A uniform model for temporal object-oriented databases," in *1992 Eighth International Conference on Data Engineering*, pp. 584–593, AZ, USA, 1992.
- [15] I. Eyal, "Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities," *Computer*, vol. 50, no. 9, pp. 38–49, 2017.
- [16] P. Danzi, A. E. Kalor, C. Stefanovic, and P. Popovski, "Analysis of the communication traffic for blockchain synchronization of IoT devices," in *2018 IEEE International Conference on Communications*, pp. 1–7, Kansas City, MO, USA, 2018.
- [17] X. Zhou, W. Liang, I. Kevin, K. Wang, R. Huang, and Q. Jin, "Academic influence aware and multidimensional network analysis for research collaboration navigation based on scholarly big data," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 1, pp. 246–257, 2021.
- [18] M. Mokbel, T. Ghanem, and W. Aref, "Spatio-temporal access methods," *IEEE Data Engineering Bull.*, vol. 26, no. 2, pp. 40–49, 2003.
- [19] L. Liu and T. Özsu, *Encyclopedia of Database Systems*, Springer, Second edition, 2018.
- [20] N. Alzahrani and N. Bulusu, "Block-supply chain: a new anti-counterfeiting supply chain using NFC and blockchain," in *the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, pp. 30–35, ACM, 2018.
- [21] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.
- [22] Z. Cai and Z. He, "Trading private range counting over big IoT data," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, Dallas, TX, USA, 2019.
- [23] X. Zhou, Y. Hu, W. Liang, J. Ma, and Q. Jin, "Variational LSTM enhanced anomaly detection for industrial big data," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3469–3477, 2021.
- [24] S. Chien, V. Tsotras, and C. Zaniolo, "Version management of XML documents, The Third International Workshop on the Web and Databases," in *International Workshop on the World Wide Web and Databases*, pp. 184–200, Springer, Berlin, Heidelberg.
- [25] Y. Xu, Q. Zeng, G. Wang, C. Zhang, J. Ren, and Y. Zhang, "An efficient privacy-enhanced attribute-based access control mechanism," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 5, pp. 1–10, 2020.
- [26] W. Liang, D. Zhang, and X. Lei, "Circuit copyright blockchain: blockchain-based homomorphic encryption for IP circuit protection," *IEEE Transactions on Emerging Topics in Computing*, 2020.
- [27] W. Y. Thin, N. Dong, G. Bai, and J. S. Dong, "Formal analysis of a proof-of-stake blockchain," in *The 23rd International Conference on Engineering of Complex Computer Systems*, pp. 197–200, Melbourne, VIC, Australia, 2018.
- [28] D. Yaga, P. Mell, N. Roby, and K. Scarfone, *Blockchain technology overview*, National Institute of Standards and Technology, 2019.
- [29] Z. Zheng, S. Xie, H. N. Dai et al., "An overview on smart contracts: challenges, advances and platforms," *Future Generation Computer Systems*, vol. 105, pp. 475–491, 2020.
- [30] P. Noac'h and A. Costan, "A performance evaluation of apache kafka in support of big data streaming applications," in *The 2017 IEEE International Conference on Big Data*, pp. 4803–4806, Boston, MA, USA, 2017.
- [31] G. G. Gueta, I. Abraham, S. Grossman et al., "SBFT: a scalable and decentralized trust infrastructure," in *The 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, pp. 568–580, Portland, OR, USA, 2019.
- [32] K. Tulkinbekov and M. Pirahandeh, "ClevelDB: coalesced LevelDB for Small Data," in *Eleventh International Conference on Ubiquitous and Future Networks*, pp. 567–569, Zagreb, Croatia, 2019.
- [33] C. Dyreson, "Using couchdb to compute temporal aggregates," in *The 18th IEEE International Conference on High Performance Computing and Communications; 14th IEEE International Conference on Smart City; 2nd IEEE International*

- Conference on Data Science and Systems*, pp. 1131–1138, Sydney, NSW, Australia, 2016.
- [34] D. Petkovic, “Temporal data in relational database systems: a comparison,” in *New advances in information systems and technologies*, pp. 13–23, Springer, Cham, 2016.
- [35] C. Zhang, Y. Xu, Y. Hu, J. Wu, J. Ren, and Y. Zhang, “A blockchain-based multi-cloud storage data auditing scheme to locate faults,” *IEEE Transactions on Cloud Computing*, 2021.
- [36] X. Zhou, W. Liang, S. Shimizu, J. Ma, and Q. Jin, “Siamese neural network based few-shot learning for anomaly detection in industrial cyber-physical systems,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5790–5798, 2021.
- [37] M. Bailleu, J. Thalheim, P. Bhatotia, C. Fetzter, M. Honda, and K. Vaswani, “SPEICHER: securing lsm-based key-value stores using shielded execution,” in *The 17th USENIX Conference on File and Storage Technologies*, pp. 173–190, Boston, MA, 2019.
- [38] Y. Li, C. Tian, F. Guo, C. Li, and Y. Xu, “Elasticbf: elastic bloom filter with hotness awareness for boosting read performance in large key-value stores,” in *The 2019 USENIX Annual Technical Conference*, pp. 739–752, Renton, WA, 2019.
- [39] J. Liao, Z. Cai, F. Trahay, and X. Peng, “Block placement in distributed file systems based on block access frequency,” *IEEE Access*, vol. 6, pp. 38411–38420, 2018.
- [40] W. Liang, J. Long, K. C. Li, J. Xu, N. Ma, and X. Lei, “A fast defogging image recognition algorithm based on bilateral hybrid filtering,” *ACM Transactions on Multimedia Computing Communications and Applications*, vol. 17, no. 2, pp. 1–16, 2021.
- [41] X. Zheng, Z. Cai, and Y. Li, “Data linkage in smart IoT systems: a consideration from privacy perspective,” *IEEE Communications Magazine*, vol. 56, no. 9, pp. 55–61, 2018.
- [42] D. Han, N. Pan, and K. C. Li, “A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection,” *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2020.
- [43] X. Zhou, Y. Li, and W. Liang, “CNN-RNN based intelligent recommendation for online medical pre-diagnosis support,” *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 18, no. 3, pp. 912–921, 2021.
- [44] M. Cui, D. Han, and J. Wang, “An efficient and safe road condition monitoring authentication scheme based on fog computing,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9076–9084, 2019.
- [45] Y. Xu, X. Yan, Y. Wu, Y. Hu, W. Liang, and J. Zhang, “Hierarchical bidirectional RNN for safety-enhanced B5G heterogeneous networks,” *IEEE Transactions on Network Science and Engineering*, 2021.
- [46] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020.
- [47] Z. Cai, X. Zheng, and J. Yu, “A differential-private framework for urban traffic flows estimation via taxi companies,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6492–6499, 2019.
- [48] M. Cui, D. Han, J. Wang, K. C. Li, and C. C. Chang, “ARFV: an efficient shared data auditing scheme supporting revocation for fog-assisted vehicular ad-hoc networks,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15815–15827, 2020.
- [49] X. Zhou, X. Xu, W. Liang et al., “Intelligent small object detection based on digital twinning for smart manufacturing in industrial CPS,” *IEEE Transactions on Industrial Informatics*, p. 1, 2021.
- [50] J. Clifford and A. Croker, “The historical relational data model (HRDM) and algebra based on lifespans,” in *The Third International 24 Conference on Data Engineering*, pp. 528–537, Los Angeles, CA, USA, 1987.

## Research Article

# A Face Occlusion Removal and Privacy Protection Method for IoT Devices Based on Generative Adversarial Networks

Wenqiu Zhu, Xiaoyi Wang, Yuezhong Wu , and Guang Zou

School of Computer Science, Hunan University of Technology, Zhuzhou 412007, China

Correspondence should be addressed to Yuezhong Wu; wuyuezhong@hut.edu.cn

Received 17 April 2021; Revised 21 May 2021; Accepted 17 June 2021; Published 1 July 2021

Academic Editor: Zhuojun Duan

Copyright © 2021 Wenqiu Zhu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The device group based on the Internet of Things (IoT) has been used in face recognition in real life, so it is more necessary to discuss the current data security issues and social hot issues. The Internet of Things device combines edge conditions and many recognizers to generative adversarial networks. On the premise of meeting the needs of partial occlusion of users, face recovery is completed through information reorganization. CelebA training set is used to simulate face occlusion, and the model is trained and tested. The results show that the method can recover the complete image of the protection for the facial privacy of specific people. At the same time, the IoT device using this method ensures that the face information is not easy to have tampered with when attacked.

## 1. Introduction

IoT is “Internet of Things.” They are built based on the expansion of the Internet, and with the Internet as the core, the client extends to any object and between objects. These devices can sense each other. By connecting various information sensing devices with the network to form a network, the data can be interconnected and shared anytime and anywhere [1, 2]. The IoT has been applied to people’s daily life. In public places, face recognition devices of IoT extract to face data and prompt other devices to get information. With the help of blockchain and cloud computing [3–5], information sharing and management between IoT devices become more convenient. Also, the application of edge computing [6–8] provides support for the rapid popularization of the IoT, which has more advantages than the traditional communication between home and public equipment sensors.

Universal recognition equipment will be applied to image recognition technology. Devices in the IoT can perceive the outside world through image recognition, which can make data collection [9, 10] more efficient, and provide users with more humanized data displays and life suggestions. At the same time, industrial IoT [11–14] also requires recognition equipment with perceptual capabilities. The equipment in

each production link handles different functions, and they interact with each other so that the production process and production plans become more flexible and reliable.

With the development of image processing technology, the predecessors proposed pixel-by-pixel filling [15], finding matching blocks [16], using image sets on the Internet to fill similar blocks [17], and suggestions based on matching block technology, such as block completion algorithm and statistical block probability repair method [18, 19]. These methods enable the device to penetrate the limited occlusion of the face when recognizing the face and accurately obtain the user’s identity information.

However, in the case of facial defects, the user must remove the occlusion for recognition. This may have potential adverse effects on the user’s psychology. In addition, identification devices will also encounter some personal privacy issues related to data collection [20, 21]. For example, in the face of flaws, users still have to perform facial authentication. Since the identification device is part of the IoT, data collection is unavoidable, and sharing with other devices will involve information security [22–24] related issues.

Machine learning [25–28] proposed a solution to improve the recognition of human faces through machine learning, so on improve the recognition ability of face



recognition equipment through fitting and classification. Later, the generative adversarial network developed based on deep learning [29, 30], through the adversarial network to improve the level of generated images and the level of image recognition, so on preventing facial spoof attacks, and at the same time further improve the restoration of the face under concealment conditions for recognizing the face to determine the identity of the user.

Therefore, an end-to-end workflow from edge recovery to face recovery is proposed, and a deep learning network based on edge conditions and multiple discriminators is proposed to judge whether the generated pixels are filled according to the required edge structure. This overcomes these challenges. Fill in the corresponding pixel information according to the integration of different levels of complete image styles and features. A complete module based on self-care mechanism is proposed and applied to Image-inpaint network. So, the face recognition device can restore the entire face from a multifeature level.

The structure of this article is as follows. The second part introduces some technical details of the implementation. The third part introduces the end-to-end deep learning network structure based on edge conditions, including multiple discriminators and self-attention mechanism. After reviewing the literature, the fourth part will introduce in detail the application of multiple local dividers in the Image-inpaint network. The fifth part includes the discussion and conclusion of our survey results.

## 2. Related Work

Under the influence of generative adversarial network technology, Pathak et al. [31] propose an Encoder-Decoder pipeline model, which uses an unsupervised visual feature learning algorithm driven by context pixel prediction to use surrounding image information. To infer the missing location, Iizuka et al. [32] propose a global discriminator and a local discriminator based on the Context-Encoder to promote the learning of the missing parts and use local convolution to increase the attention of partial blocks by the network to enhance the details of specific parts. The situational attention network proposed by Yu et al. [33] and the self-attention generation adversarial network proposed by Zhang et al. [34] solve the problem that the structure of the surrounding area is distorted, or the texture is not consistent with the fuzzy texture. They can not only synthesize new image structures but also make full use of the surrounding image features as a reference. Among them, the self-attention mechanism proposed to reference [34] can also be weighted according to the importance of features to correlate important information on each other. After that, Yu et al. [35] also combined the contextual attention mechanism and the proposed gat convolution. The discriminator is no longer a combination of local and global discriminators but uses SN-Batch GAN; on the premise of meeting the Lipschitz constraint, the information of the weight matrix of the discriminator is saved to the maximum extent so that the training process is more stable. Kun et al. [36] proposed a face completion algorithm based on a conditional genera-

tion adversarial network. The algorithm generates faces that meet the conditional features, but it is still a relatively simple information extraction based on Encoder-Decoder. Moreover, multiple convolutional blocks are not used for sufficiently deep feature extraction. Xie et al. [37] proposed an image restoration method based on a learnable two-way attention map, which can deal with irregular hole repair, and proposed to merge forward and backward attention maps into a learnable two-way attention map. To further improve the visual quality of the image, but because there is no constraint on edge information, the details of specific parts of the portrait are still not ideal. In EdgeConnect [38], Nazari et al. proposed the concept of “lining first, then color” through image restoration based on edge conditions. The repaired edge information is obtained through the edge generator, and then based on the obtained edge repair image as a condition, the incomplete image data is spliced and input into the image repair network, thereby using the edge information to restore the image. Get images of the image completion network. Its essence is to divide the steps of image restoration of high-frequency information and low-frequency information. Yet, only the discriminator that uses the network has a global identity. Compared with the local recognition network and the facial feature recognition network, the repair details are compared with the image generation, which is inferior to the method of multiple discriminators.

The spectral normalization proposed by Miyato et al. [39] reduces the calculation amount of network normalization and makes the calculation of the discriminator more stable. In addition, the reason for using multiple discriminators [32, 33] as a supervisory network is that multiple discriminators have been proven many times in practical applications to form multilevel constraints on the generated results of more aspects. And let the generator produce better results. Using partial convolution [40], there are only connections to the local area, and the receiving field adopts a connected method, and the interval between the receiving fields adopts a local connection and a convolutional connection. Compared with full convolution, this method will introduce additional parameters in multiples, but it has stronger flexibility and expressive power. Compared with a local connection, it can control the number of parameters and proposed a new convolution to replace the general convolution, which will prevent the training results from generating chessboard artifacts.

For face recognition equipment, the combination of convolutional computer vision and computer image processing can make the face recognition equipment perform better under specific facial features, detail recovery, and state recovery.

To solve the problem that the edge completion method only pays attention to the integrity of the image and ignores the visual connectivity of the complete part and the facial features, based on EdgeConnect, puts forward the following ideas:

- (a) The method of a discriminator for face parts (eyes, nose, and mouth) is proposed. After the complementary edge image and damaged image are processed by



the image completion network, the eyes, nose, and mouth of the generated complementary face image are discriminated. So the facial features of the face image are more consistent with the semantic rationality

- (b) Propose a gated convolution block based on edge condition to enhance the difference between regions. At the same time, the self-attention mechanism is used to automatically enhance the difference between occluded and nonoccluded areas. The information of the input data is enhanced according to different feature levels, to distinguish the occluded area and the nonoccluded area more accurately
- (c) Propose to use a local discriminator. When the completed image is processed by the image completion network, the completed image will have better visual connectivity as a whole

*2.1. Deep Learning.* Deep learning-based recommendation methods can incorporate multisource heterogeneous data for the recommendation, including explicit or implicit feedback data from users, user portrait and project content data, and user-generated content. Deep learning methods use multisource heterogeneous data as input and use an end-to-end model to automatically train prediction models, which can effectively integrate multisource heterogeneous data into the recommendation system, thereby alleviating the data sparseness and cold start in traditional recommendation system problems and improving the ability of the recommendation system. The application of deep learning to corpus mining is a research hotspot. After 2006, with the publication of Hinton and Salakhutdinov [41], it was wildly sought after by scholars in the artificial intelligence world. This model is based on a neural network model, but it is more complex than a simple neural model, and the problems it deals with are more complex and diverse. Deep learning methods have been successfully used in many applications in the computer field, including speech recognition, speech search, natural language understanding, information retrieval, and robotics. Mokris and Skovajsova [42] applied the neural network model to have a high degree of relevance. It retrieved Slovak-related documents, processed keyword parts of speech, and greatly improved accuracy and recall. Based on the highly nonlinear characteristics of neural network algorithms, using BP network to optimize the weight of each parameter in the entire neural network, constantly revising the weights, Xu et al. [27] constructed a personalized behaviour based on users. Latreche and Guezouli [43] use the correlation characteristics of neighbor nodes in the neural network to combine all documents into a neural network and retrieves the most relevant document according to Query.

The method (Figure 1) consists of two parts, namely, the Edge-inpaint network and the Image-inpaint network. Among them, the Edge-inpaint network is responsible for repairing the edges of the defective face image, and the Image-inpaint network is responsible for completing the face image based on the condition of the completion of the edges.

Before applying the model, the network is trained to generate the model. The data processing in the training process is divided into two steps: First, take the unmasked edge map as the target, and enter the masked, masked Canny Edge maps and masked grayscale images, through training the Edge-inpaint network model, enable the Edge-inpaint network to generate a predicted completion edge map; second, use the prediction completion edge map output by the Edge-inpaint network, combined with the incomplete color face image is input to the Image-inpaint network, and the predicted repaired face image is output. The two networks form an end-to-end solution so that the identification device based on the IoT can ensure that the user can still accurately obtain the correct information of the user when the user is covering his specific part.

### 3. Networks

*3.1. Edge Completion Generative Adversarial Network.* The Edge-inpaint network (Figure 2) is composed of an edge completion generation network (edge generator, hereinafter referred to as G1) and an edge completion discriminator network (edge discriminator, hereinafter referred to as D1). Among them, G1 network generates edge completion image, inputs masked gray image, masked edge image, and mask, takes real edge image as label, generates a completion edge image after G1 operation, and then calculates adversarial loss and feature matching loss [44] through D1, and this loss value is used to backpropagate the network associated with it. The purpose of G1 is to minimize the gap between the generated edge image and the real edge image to improve the quality of the image generated by the generator, while D1 is to expand this gap as much as possible, thus making the progress of G1 more difficult; of course, the result will be better.

G1 is composed of 3 convolutional layers, 8 residual blocks, and 3 deconvolutional layers cascaded. Among them, the convolution kernel of the convolution layer is composed of  $7*7$ ,  $4*4$ , and  $4*4$ , and the deconvolution layer is composed of convolution kernel sizes of  $4*4$ ,  $4*4$ , and  $7*7$ . Convolution both the layer and the deconvolution layer have spectral normalization processing and setting the ReLU activation function after the convolution operation. The first convolution of the convolution layer and the last convolution of the deconvolution layer are done separately reflective filling treatment.

D1 takes the real edge face image as the target (label) and fights against G1. When G1's ability becomes stronger and stronger, D1 can also improve the complementary edge image generated by G1 with reasonable parameter settings. The Canny edge detector is used to extract the edge features of the image as the expected positive samples learned by the discriminator, and the negative samples generated by the network G1 that do not meet the experimental expectations and Canny edge features are merged to improve D1 with its distinguishing ability and supervise G1 to generate an image with edge information that is more in line with the original image.

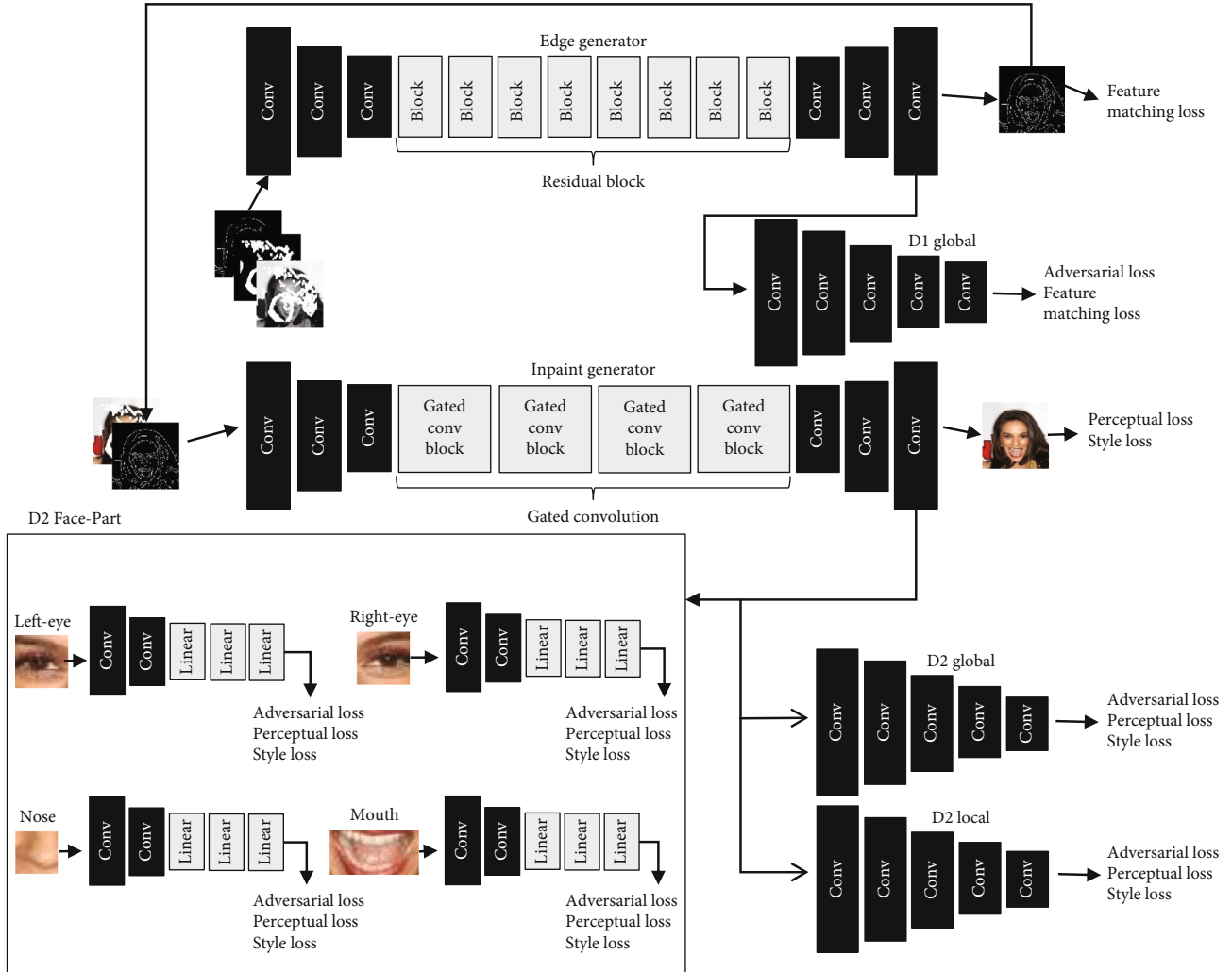


FIGURE 1: Structure of network, which has edge-GAN, inpaint-GAN, and multiple discriminators.

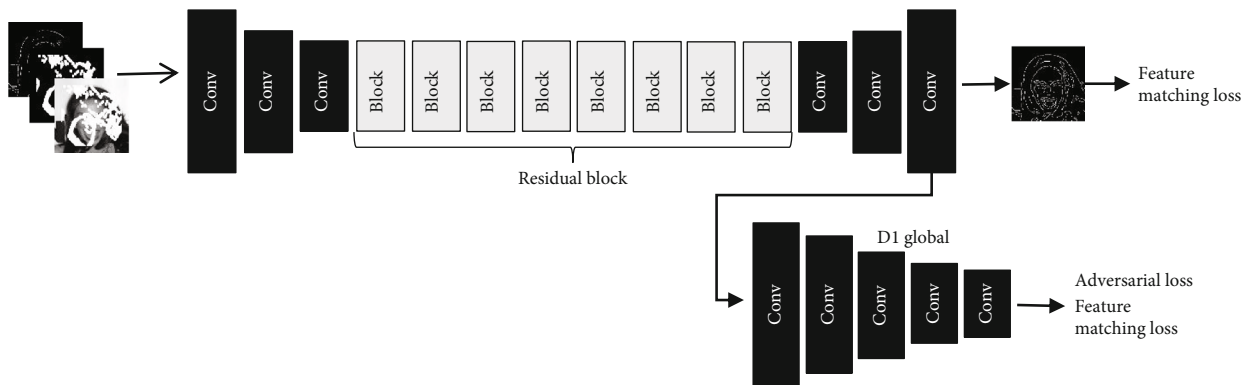


FIGURE 2: Structure of edge-GAN, which has edge-generator and edge-global discriminator.

The Edge-inpaint network allows the recognition device to reconstruct the structural information of the face from the occluded part of the face, thereby providing a basis for the subsequent feature and texture completion. Through spectral normalize processing of convolution, residual block [45] and deconvolution, and fusion of different information sources, deep texture features are extracted.

### 3.2. Image Completion Based on Self-Attention Mechanism

**3.2.1. Composition of Image-Inpaint Network.** The image completion network (Figure 3) is composed of an image completion generation network (Image-inpaint generator, referred to as G2 hereinafter) and an image completion discriminator network (Image-inpaint discriminator, hereinafter

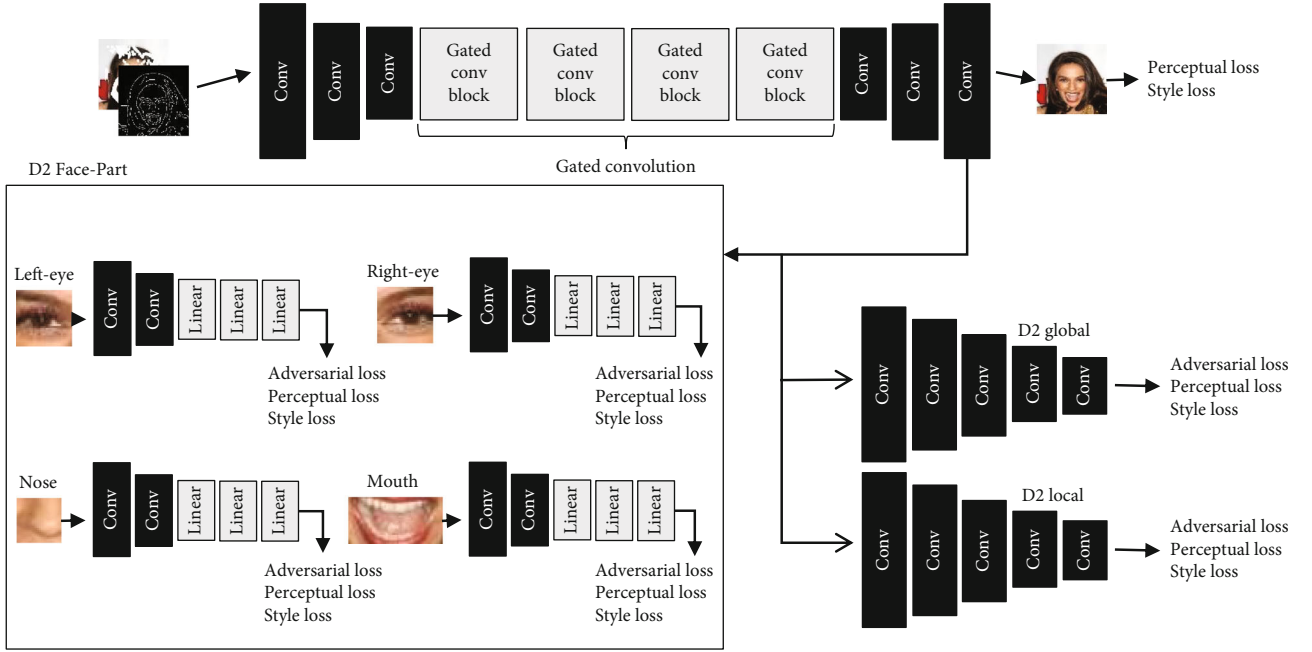


FIGURE 3: Structure of inpaint-GAN, which has inpaint-generator and multiple discriminators in inpaint-GAN, and multiple discriminator includes global discriminator (D2 global), local discriminator (D2 local), and face-part discriminator (D2 Face-Part).

referred to as D2). The role of the G2 network is to generate a complementary image, input the complementary edge map and the incomplete face image, and use the real image as a label and cascade the input data; after the G2 operation, generate the completed image and then pass the D2. Each discriminating network calculates adversarial loss, perceptual loss, and style loss [44]. The loss of the image completion network is the sum of the counter losses of the D2 Face-Part network, and this loss value is used to backpropagate the network associated with it. The purpose of G2 is to allow G2 to dynamically learn the parameters through training to effectively distinguish between the effective area and the mask area and reduce the adverse effect of the mask on the image completion so that the color and structure of the image completion are more reasonable and minimized. Generate the gap between the completed image and the real image to improve the quality of the image generated by the generator. And D2 is to widen this gap as much as possible, so that G2 and D2 identify the network combination to fight and promote the progress of G2.

G2 is composed of 3 convolutional layers, 4 proposed gated convolutions, and 3 deconvolutional layers in cascade. Among them, the convolution kernel of the convolution layer is composed of  $7 \times 7$ ,  $4 \times 4$ , and  $4 \times 4$ , and the deconvolution layer is composed of the convolution kernel size of  $4 \times 4$ ,  $4 \times 4$ , and  $7 \times 7$ . The convolution layer and the deconvolution layers all have spectral normalization processing and setting of the LeakyReLU activation function after the convolution operation. The first convolution of the convolution layer and the last convolution of the deconvolution layer are, respectively, filled with reflection.

D2 takes the real face image as the target and fights against G2. When G2's ability is getting stronger and stronger, D2 can improve its ability to discriminate the complementary image generated by G2 and use G2 to generate it

with reasonable parameter settings. The edge feature of the mask completes the image. As the expected positive samples learned by the discriminator, the negative samples generated by the network G2 that do not meet the experimental expectations and the mask edge features are merged to improve the discrimination ability of D2 and supervise G2 to generate images that are more in line with the original image.

**3.2.2. Design and Implementation of Self-Attention Mechanism.** Ordinary convolution has limitations in completing the image under any mask. It extracts local features in a sliding manner, and the pixels under the sliding window are all valid by default. But for image completion, when the window contains the boundary of the mask, its invalid pixels and effective pixels will be processed by the convolution window, which will cause the information to be blurred, and the sides of the complement part do not match the actual results.

The gated convolution module is used to automatically learn the soft occlusion mechanism from the data through self-attention, dynamically identify the effective pixel position in the image, and process the transition between the masked area and the unmasked area. The proposed gated convolution not only can retain features at long distances that the residual block has but also has the ability of the gated convolution itself to enhance the distinction between features on both sides of the edge. The following formula (1) is the operation of gated convolution [33]

$$\begin{cases} \text{Gating}_{y,x} = \sum \sum W_g \cdot I, \\ \text{Feature}_{y,x} = \sum \sum W_f \cdot I, \\ O_{y,x} = \phi(\text{Feature}_{y,x}) \odot \phi(\text{Gating}_{y,x}). \end{cases} \quad (1)$$

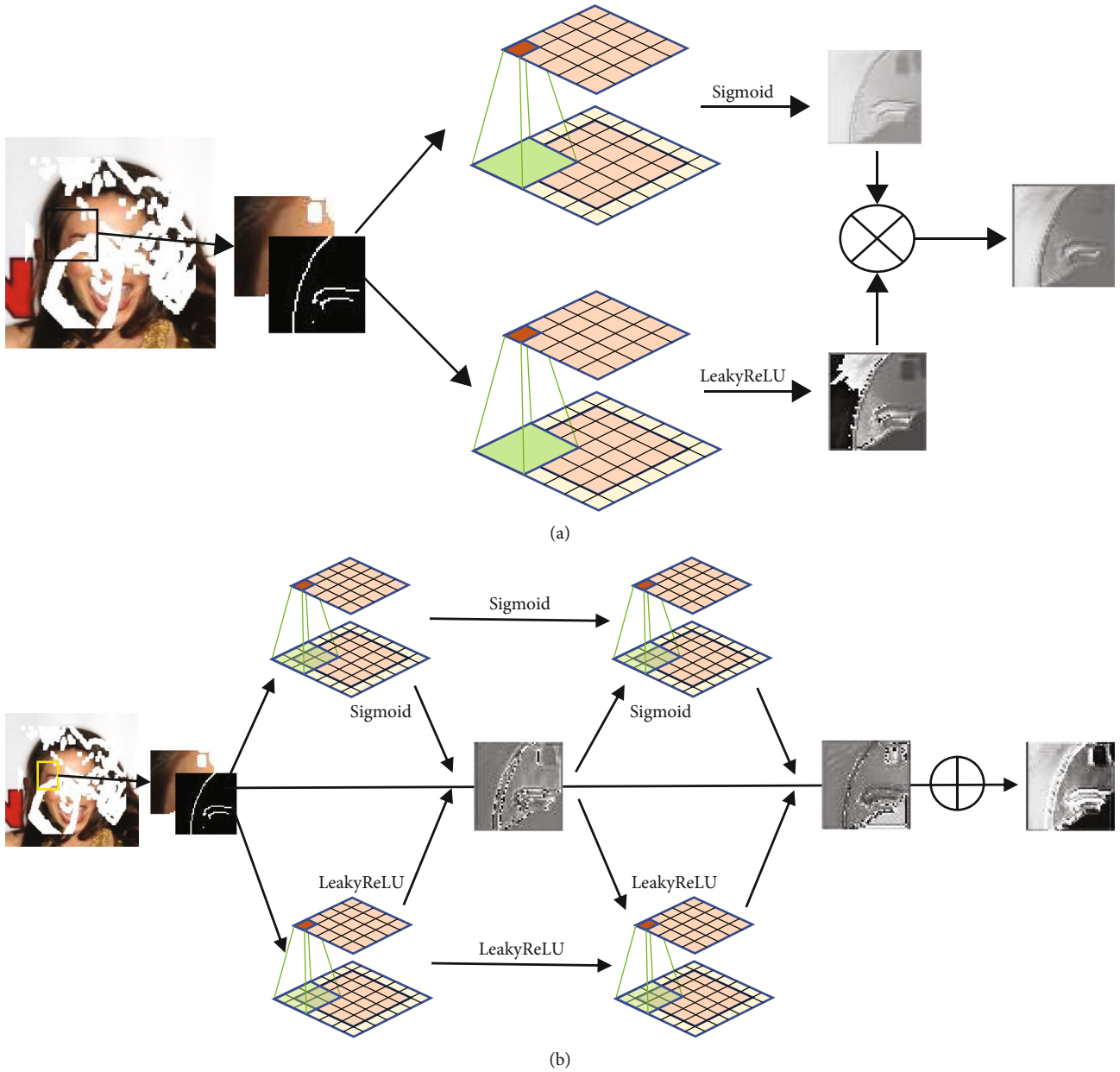


FIGURE 4: Results produced under different gated convolutions: (a) normal gated convolution; (b) proposed gated convolution.

Among them,  $y, x$  is the center point of the current sliding area;  $W_g$  is the convolution filter that selects mask and non-mask space;  $W_f$  is the convolution filter to distinguish between mask and non mask, and I/O is input convolution filter and output convolution filter, respectively. Gating convolution and sigmoid (Figure 4(a)) [46] activation function realize dynamic feature selection, that is, selecting mask coverage space and normal space; feature convolution and LeakyReLU activation function realize feature extraction, that is, select part of the transition map of the masked and non-masked areas and then use the dot product of gating and feature to more effectively select useful information. The proposed gated convolution has stronger pixel selectivity so

that the convolution can accurately describe local features even with a larger range of pixel deletions.

At the same time, the general gated convolution still has a small amount of boundary blur on both sides of the mask boundary, which will cause the problem of invalid pixels as valid pixels when the window of the gated convolution is sliding, which will cause the concealed information will be regarded as part of the face itself rather than blocked, making the device unable to effectively restore the original information of the face. On this basis, different features generated by different subgated convolution are added to the input to get clearer feature differences on both sides of the mask boundary (Figure 4(b)), to distinguish the differences on both

sides of the edge more accurately. The boundary pixels between the region and the normal region affect the visual connectivity of the whole image. If the defective part of the mask edge is close to the normal part of the pixels, gated convolution can easily confuse the two, and different types of features are strengthened by feature addition to achieving more effectiveness on both sides of the mask edge. The feature distinction of, so that the image completion network is better targeted at the completion part, and the part of the human face itself and the covered part are logically distinguished effectively.

#### 4. Discriminator Network for Partial Completion

*4.1. Local Discriminator Network Combining Structure and Texture.* Aiming at the problem that the Image-inpaint network only has a global discriminator network and the partial restoration is not ideal, a local discriminator network is proposed.

The local discriminator network proposed in this paper is a part of D2 Local in Image-inpaint network. Its network structure is the same as the D2 Global, it consists of five convolution blocks, and each convolution block contains a layer of Convolution, Spectral Normalize, and LeakyReLU (the last convolution block has no leakyrelu activation layer).

The completion part and the real part of the corresponding position are input into the global discrimination network to generate two  $15 \times 15$  matrices, and then, these matrices are input into the adversarial network. The process is calculated by

$$L_{adv,l} = E_{(I_{gt,l}, C_{comp,l})} [\ln D_2(I_{gt,l}, C_{comp,l})] + E_{comp,l} \ln [1 - D_2(I_{pred,l}, C_{comp,l})]. \quad (2)$$

Among them,  $I_{pred,l}$  is the completion part;  $I_{gt,l}$  is the real part of the corresponding position;  $C_{comp,l}$  is the local completion edge map; this formula is the loss function of the local adversarial network. It is responsible for identifying the authenticity of the complete part so that the complete result will not deviate from the authenticity.

The general local discriminator network is based on authenticity, but because it only judges the authenticity of the complete part itself, the style of the generated part is weak, and the generated part affects the visual connectivity of the whole image. Moreover, in the reconstruction of high-level feature levels, factors such as color, texture, and exact shape of the face are not taken into consideration. Therefore, it is proposed to use style loss and perceptual loss for additional constraints. The recognition device can also restore the occluded part under the condition of conforming to the subject characteristics of the face. Style loss is

$$L_{style,l} = L_{style}^{\phi,j}(\hat{y}, y) = \left\| G_j^{\phi}(\hat{y}) - G_j^{\phi}(y) \right\|_F^2, \quad (3)$$

where  $G_j^{\phi}$  is the activation map of the  $j$ -th layer of the pre-trained network and  $j$  is a set of integers from 1 to 5, which corresponds to the activation maps of the relu1\_1, relu2\_1, relu3\_1, relu4\_1, and relu5\_1 layers of the pre-trained VGG-19 [47] network. These activation maps are also used to calculate the style loss to measure the difference between the covariances of the activation maps. The Euclidean distance of each image feature is used to measure the degree of dissimilarity between perception and the real part.

Although the style loss corrects the texture and pixel completion error to a certain extent, it does not well preserve the shape and structure of the image completion part. To solve the loss of style, only the texture and color information are retained, but the shape and structure information is not effectively retained. The perceptual loss is proposed to restrict the structure and shape of the generated result. Perception loss as

$$L_{perc,l} = E \left[ \sum_i \frac{1}{N_i} \left\| \Phi_i(I_{gt}) - \Phi_i(I_{pred}) \right\|_1 \right], \quad (4)$$

where  $\Phi_i$  is the activation map of the  $i$ -th layer of the pre-training network and  $i$  is the set of integers from 1 to 4, which corresponds to the activation maps of the relu2\_2, relu3\_4, relu4\_4, and relu5\_2 layers of the pretrained VGG-19 [47] network.  $I_{gt}$  and  $I_{pred}$  are the real image and the generated image, respectively. The structure and shape features are extracted from each activation graph, and the Euclidean distance between activation is calculated to promote the reconstruction of high-level information.

Add formulas (2), (3), and (4) to obtain the total loss formula (5) of the local discriminator network and the Image-inpaint network

$$L_{local} = L_{adv,l} + L_{style,l} + L_{perc,l}. \quad (5)$$

The main function of the local discriminator network is to measure some blocks generated by the image and obtain the combined losses to ensure the semantic rationality of the complement.

Figure 5(a) is the result obtained when only formula (2) is used as the loss function; Figure 5(b) is the result obtained when formula (5) is used as the loss function, and Figure 5(c) is the original image. The processed portrait is the information after the occluded part is restored. The restored part should not only pay attention to its authenticity to the whole portrait but also consider its authenticity. Therefore, the function of formulas (3) and (4) is to pay attention to the generic structure and style of the restored part on the premise that the global discriminator network also pays attention to the generation structure and style of the generation part. Let the image completion network be subject to more restrictions in training, just as human beings learn to pay attention to more information when considering a problem.



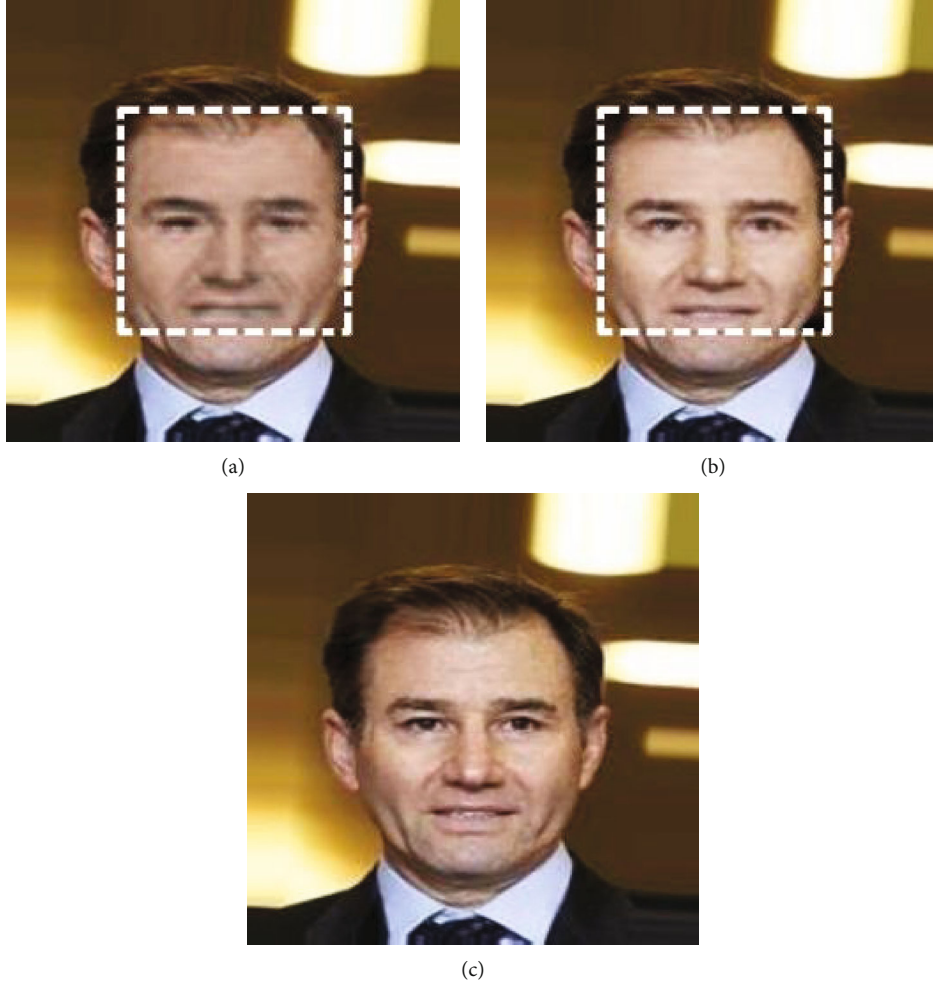


FIGURE 5: Effects under different losses: (a) adversarial loss; (b) combined losses; (c) original.

**4.2. Discriminator Network Based on Face Local Position Constraint.** Since the general local discriminator network is essentially the same as the global discriminator network, it only focuses on integrity, and it is difficult for the local discriminator network to describe the texture of the face image in detail when the face is completed. Therefore, a special local discriminator network is proposed to deal with the generation details of human face parts, so that the completed part and the whole image meet the visual connectivity.

The face-part discriminator network (D2 Face-Part) (Figure 6) is a special partial discriminator network. The face-part discriminator network is composed of four subnetworks. These four subnetworks are the left-eye discriminator network and the right-eye discriminator network, eye discriminator network, nose discriminator network, and mouth discriminator network. It targets the key parts of the human face, namely, the left eye, right eye, mouth, and nose. The four subnetworks of D2 Face-Part will extract the left eye, right eye, nose, and mouth and send them to the face recognition network. The network will be sent to the corresponding four networks, and finally, four scores will be generated. Calculate the respective adversarial losses, where the adversarial loss is 1 as true and 0 as false. After these scores are calculated for the adversarial loss, the four adversarial loss

values are added and averaged. The four values of the adversarial loss are added and averaged to obtain

$$L_{adv,fp} = \frac{1}{4} \sum_{i=1}^4 \left( E_{I_{gt,i}} [\ln D_2(I_{gt,i})] + E_{I_{pred,i}} [1 - \ln D_2(I_{pred,i})] \right). \quad (6)$$

Formula (6) is the loss function of D2 Face-Part and G2 adversarial, where  $I_{gt,i}$  is the  $i$ -th real Face-Part and  $I_{pred,i}$  is the  $i$ -th Face-Part of the completed image. The purpose of this function is to hope that G2 (image completion generation network) will pay more attention to the reliability of the generation of the facial “features” during training and to pay more attention to its effects on the microlevel of the face.

Same as the improved local network, to overcome the drawbacks of only paying attention to the true and false of the image itself, which is brought about by the counter loss, and not paying attention to its texture and structure. It is proposed to use the style loss function and the perceptual loss function for the discriminator of each part of the face so that the generated part makes the whole image have better visual connectivity. Formula (7) and formula (8) are the style loss function and the perceptual loss function of the human face, respectively.

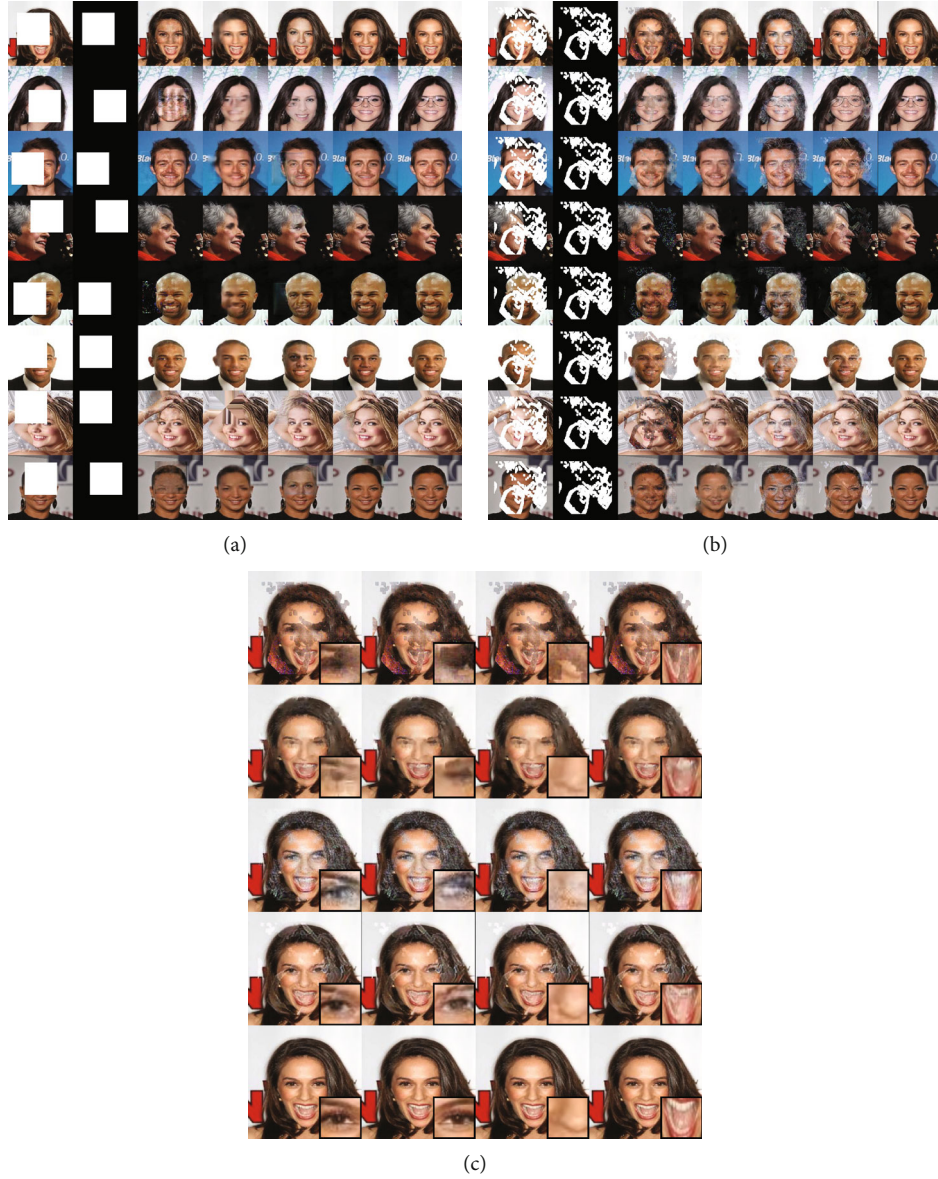


FIGURE 6: This is the result of each method under different mask conditions: (a) restoration results of different techniques under block mask; (b) restoration results of different techniques under random mask; (c) restoration Face-Part of different techniques under random mask.

$$L_{\text{style},fp} = L_{\text{style}}^{\phi_j}(\hat{y}_i, y_i) = \frac{1}{4} \sum_{i=1}^4 \left\| G_j^{\phi}(\hat{y}_i) - G_j^{\phi}(y_i) \right\|_F^2, \quad (7)$$

$$L_{\text{perc},fp} = E \left[ \frac{1}{4} \sum_{j=1}^4 \sum_i \frac{1}{N_i} \left\| \Phi_i(I_{gt,i}) - \Phi_i(I_{\text{pred},i}) \right\|_1 \right]. \quad (8)$$

The  $\hat{y}_i$  and  $y_i$  in formula (7) are the restored part and the corresponding real part, respectively, the  $i$  in formula (8) is consistent with that in formula (3), and the  $j$  is an integer set from 1 to 4, representing the four parts of the face, respectively.

Formula (7) is the style loss of different parts of the face. Its function is to calculate the style loss through the activation map to measure the difference between the covariance of the activation map. The Euclidean distance of each image feature

is used to measure the degree of perception different from the real part. Taking the features extracted in the calculation as the style, the Euclidean distance difference is calculated to constrain the texture of the face to be compensated and ensure that the texture and pixels are consistent with the theme of the whole image.

Formula (8) is the perception loss of different parts of the face. Its function is to limit the overall “features” of the completed face image, keep the structure of the restored part in line with the requirements of the original image, and improve the visual connectivity of the “features” after completion.

In order to measure the difference between the covariance of the activation map, the Euclidean distance of each image feature is used to measure the similarity between the perceptual part and the real part. The features extracted in the calculation are used as the style features of the face image, and the Euclidean distance is used to calculate the degree of

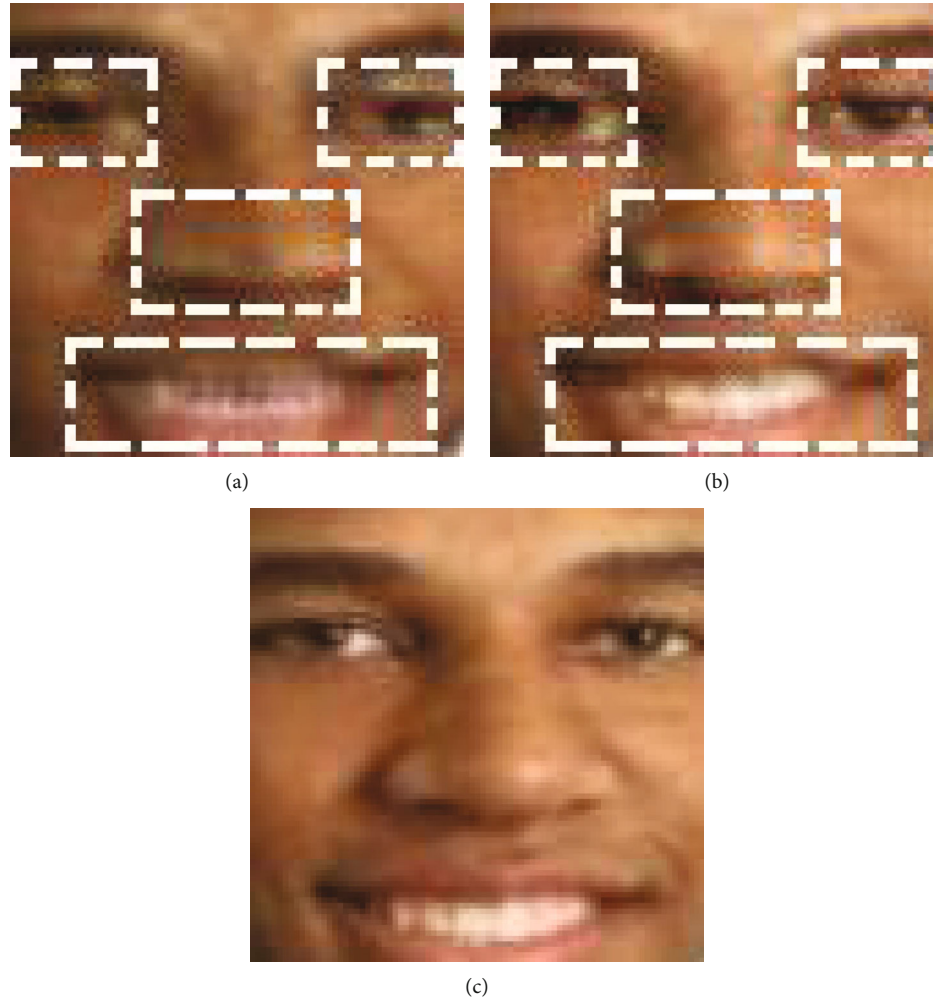


FIGURE 7: Effects under different losses: (a) adversarial loss; (b) combined losses; (c) original.

difference in style between the real Face-Part and the completed Face-Part, to compare the completed face. The location is subject to texture constraints, to ensure that the texture and pixels conform to the theme of the whole image. Constrain the overall “features” of the completed face image to improve the visual connectivity of the “features” after the completion. The face-part discriminator network also uses the normalized convolution filtering in the network to reconstruct the style of the unmasked part of the face, so that the facial features are clearer and texture. The subject of the face image is closer. The effect is shown in Figure 7.

Figure 7 shows the effect of face part generation. Each part of D2 Face-Part network is equipped with adversarial loss, style loss, and perception loss, which restrict the authenticity, texture, and structure of the image, respectively, so that the details of the eyes, nose, mouth, and other parts of the portrait are more in line with common sense that people should have.

Add formulas (6), (7), and (8) to get the total loss of G2 and D2 Face-Part losses (formula (9))

$$L_{fp} = L_{adv,fp} + L_{style,fp} + L_{perc,fp}. \quad (9)$$

In general, the discriminator network for image completion is composed of three discriminator networks, which are based on the integrity of the face image completion, the rationality of the face image completion part, and the generation of facial image “facial senses.” It is logical. Use D2 Face-Part to analyze the structure of the face, so that the structure of the glasses, nose, and mouth is closer to the real shape. Through the constraint of external loss, the overall, partial, texture, structure, and pixel supervision of G2 can be achieved.

## 5. Experiment and Evaluation

*5.1. Experimental Setting.* Use 202599 data sets in CelebA [48] for training, testing, and evaluation. Before training, each face image is rescaled to 256 pixels  $\times$  256 pixels  $\times$  3 pixels.

The experimental environment is Windows 10 as the platform, with Pytorch 1.7 implemented on Python 3.8, the processor is i5-9400F 2.9 GHz, the memory is 32 GB, and the graphics card is RTX2070 SUPER 8 GB.

The learning rate is 0.0001 by default, and the Adam [49] gradient descent method is used to backpropagate the



TABLE 1: PSNR/SSIM of Figures 6(a) and 6(b).

Figure 6 no.	Context-Encoder	Globally-Locally	EdgeConnect	Ours	Ground-Truth
a	21.03	26.88	23.96	27.89	Inf
	0.9467	0.9218	0.8653	0.9508	1
b	14.89	18.08	21.00	22.76	Inf
	0.7824	0.8871	0.7731	0.8297	1

update gradient, and the Beta 1 and Beta 2 are, respectively, 0.0 and 0.9.

**5.2. Results and Analysis.** To compare the experimental results more intuitively, the classical algorithms with better performance in recent years are adopted, which are Context-Encoder in [31], Globally-Locally in [32], and EdgeConnect in [38]. To intuitively express the superiority of the proposed complementary algorithm, the peak signal-to-noise ratio (PSNR) is used to measure the distance between the complementary image and the original image. The larger the value of PSNR, the better the performance of the complemented image. At the same time, to reflect the authenticity of the proposed algorithm in the structure of the complementary image, the structure similarity (SSIM) is used to measure the difference between the structure of the complementary image and the original image. SSIM uses 0 as the lowest score. The higher the score, the structure of the complementary image. Logically, the more it conforms to the standard of the original image structure, the highest score is 1.

Figures 6(a) and 6(b) are the results of block occlusion completion and irregular occlusion completion, respectively. There are 8 rows and 7 columns. The rows represent different test images, and the columns represent the performance of the same type or the same method in different images. Among them, the first column represents the original image occluded by a specific mask, the second column is the mask image of a specific type of occlusion original image, and the third to sixth columns are article [31], article [32], article [38], and the completion results of the proposed method under different masks. The seventh column is the original image.

Figure 6(c) has 5 rows and 4 columns, and each row represents the results of different methods. They are the Context-Encoder method of article [31], the Globally-Locally method of article [32], the EdgeConnect method of article [38], the method and original image proposed in this article. Each column represents the left eye, right eye, nose, and mouth.

**5.2.1. Analysis of Occlusion Restoration and Completion Results.** It can be seen from the results in Table 1 that the effect of the proposed method is better than that of other control groups.

From the perspective of qualitative analysis, in Figures 6(a) and 6(b), there are still some noises after the completion of the image in the third column, the recovery level of details is generally poor, and the hue and brightness of the generated part are different from that of the complete image. The fourth column of facial features is too flat, and

the feature recovery rate of each part of the face is low, which cannot reflect the facial features of the face well. The fifth column is better in the case of random occlusion, but it is not good in the case of block occlusion, and the complementary color does not match the basic tone of the whole image. The sixth column was based on the control group. In addition to basically avoiding noise, the hue and facial contour of the complementary color part are more consistent with the original image, and the detail texture of facial features is also better.

From the perspective of quantitative analysis, the reconstruction loss formula of the third column fits the surrounding texture according to its results. It is essentially a linear operation using L2 distance, and its fitting ability is not as good as that of adversarial loss. The fourth column uses multiple discriminators to calculate, which not only makes the generated part more specific but also takes into account the overall information. However, because it is unconditional input and there is no edge information as the condition, the visual connectivity of the image restoration results is poor, but its score shows that this idea is feasible. The fifth column method uses multiple loss functions and takes edge conditions as input, which greatly improves the visual connectivity of the generated results, but the results are slightly lower than the fourth column method. Based on the fifth column, the sixth column method further enhances the generated results.

**5.2.2. Analysis of the Results of Face-Part Completion.** LE, RE, N, and M in Table 2 represent the English abbreviations for the left eye, right eye, nose, and mouth, respectively. Combining the results of Figure 6(c), the proposed method has a better ability to restore Face-Part than the control group.

From the perspective of qualitative analysis, the details of the facial parts after the completion of the first line in the figure are blurred; there are obvious noises, and the structure is unclear. The complete structure of the second line is not obvious, the texture of the complete effect is flat, and the facial parts are not clear. The hue expression in the third line deviates too much from the entire image, and the supplementary details of Face-Part are not ideal. The repair effect is slightly worse when the fourth line is defective, but overall, the repair effect of the facial part is better than the control group, and the color tone and brightness are consistent with visual connectivity.

From the perspective of quantitative analysis, the Context-Encoder method in the first line only focuses on the wholeness of the local generation to fit the visual connectivity of the entire image, resulting in the inadequate generation of Face-Part (LE, RE, N, and M) details. The method

TABLE 2: PSNR/SSIM of Figure 6(c).

Face-Part	Context-Encoder	Globally-Locally	EdgeConnect	Ours	Ground-Truth
LE	18.99	18.66	16.16	19.37	Inf
	0.6798	0.6675	0.6640	0.7051	1
RE	17.74	18.94	15.28	19.19	Inf
	0.6252	0.6797	0.3602	0.7411	1
N	19.50	21.96	17.14	22.28	Inf
	0.6493	0.7736	0.5731	0.7628	1
M	20.99	23.36	21.17	23.41	Inf
	0.6565	0.8133	0.7407	0.7618	1
Average	19.30	20.73	17.44	21.06	Inf
	0.6527	0.7335	0.5898	0.7374	1

proposed in the second line also has the problem of the method in the first line, but it is more closely related to the local generation and the overall generation, and the generation effect is better. Although the method in the third row is not good in terms of data performance, it is a portrait restoration based on edge conditions, and its performance in the reconstruction of texture and structure is more in line with the look and feel of real portraits. The method in the fourth line uses a gated convolution block with a self-attention mechanism to identify both sides of the mask boundary more accurately. At the same time, it uses a loss function and multiple discriminators that focus on different factors of the portrait, giving a human-like Face-Part (LE, RE, N, and M) that are more real.

## 6. Conclusion

We have determined that GAN can be trained on external standard datasets. To generate face occlusion recovery in the adversarial network, a complete structure based on edge conditions, a convolution block based on self-attention mechanism, and a discriminator based on multiple discriminators are introduced in the GAN. The hidden part is repaired by an edge generator, and the hidden part is distinguished from the normal part by self-attention convolution block. Based on the constraints of local and facial feature parts, multiple discriminators are used to completing the recovery results of style texture and different levels. To verify the validity of this method, three methods, Context-Encoder, Globally-Locally, and EdgeConnect, are used to compare. The results show that the comprehensive level of the proposed method is higher than that of the control group.

However, the method still has some deficiencies in the details of face integrity, and the effect for small-sized parts of the face still needs to be improved. In the complex texture part, the restoring effect is also limited, and the restoring effect is relatively simple. So overcoming these problems is also our future work. We have determined that image inpainting based on edge conditions and deep learning using a GAN can effectively solve this problem. Next, we will further improve the image quality based on the latest research results and the advantages of the proposed method.

## Data Availability

The URL of the public dataset used to support the results of this study is <http://mmlab.ie.cuhk.edu.hk/projects/CelebA.html>

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This work is supported in part by the National Key R&D Program of China under grant numbers 2017YFC0821602, 2019QY1604, and 2019YFE0122600; in part by the National Natural Science Foundation of China under grant number U1836217; and in part by the Open Platform Innovation Foundation of Hunan Provincial Education Department under grant number 20K046.

## References

- [1] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.
- [2] Z. Xiao, F. Li, H. Jiang et al., "A joint information and energy cooperation framework for CR-enabled macro-femto heterogeneous networks," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2828–2839, 2020.
- [3] Y. Xu, C. Zhang, G. Wang, Z. Qin, and Q. Zeng, "A blockchain-enabled deduplicatable data auditing mechanism for network storage services," *IEEE Transactions on Emerging Topics in Computing*, p. 1, 2020.
- [4] C. Zhang, Y. Xu, Y. Hu, J. Wu, J. Ren, and Y. Zhang, "A blockchain-based multi-cloud storage data auditing scheme to locate faults," *IEEE Transactions on Cloud Computing*, p. 1, 2021.
- [5] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, "Blockchain empowered arbitrable data auditing scheme for network storage as a service," *IEEE Transactions on Services Computing*, vol. 13, pp. 289–300, 2020.
- [6] Z. Jiale, Z. Yanchao, C. Bing, H. Feng, and Z. Kun, "Survey on data security and privacy-preserving for the research of edge computing," *Journal on Communications*, vol. 39, pp. 1–21, 2018.




- [7] Z. Xiao, X. Dai, H. Jiang, and D. Wang, "Vehicular task offloading via heat-aware MEC cooperation: a game-theoretic method with correlated equilibrium," *IEEE Internet of Things Journal*, vol. 7, pp. 2038–2052, 2019.
- [8] Y. Wu, Q. Liu, R. Chen, C. Li, and Z. Peng, "A group recommendation system of network document resource based on knowledge graph and LSTM in edge computing," *Security and Communication Networks*, vol. 2020, Article ID 8843803, 11 pages, 2020.
- [9] Z. Cai and Z. He, "Trading private range counting over big IoT data," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 144–153, Dallas, TX, USA, July 2019.
- [10] X. Zhou, W. Liang, K. I. K. Wang, R. Huang, and Q. Jin, "Academic influence aware and multidimensional network analysis for research collaboration navigation based on scholarly big data," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 1, pp. 246–257, 2021.
- [11] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.
- [12] X. Zhou, X. Xu, W. Liang et al., "Intelligent small object detection based on digital twinning for smart manufacturing in industrial CPS," *IEEE Transactions on Industrial Informatics*, p. 1, 2021.
- [13] X. Yan, Y. Xu, X. Xing, B. Cui, Z. Guo, and T. Guo, "Trustworthy network anomaly detection based on an adaptive learning rate and momentum in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6182–6192, 2020.
- [14] X. Zhou, Y. Hu, W. Liang, J. Ma, and Q. Jin, "Variational LSTM enhanced anomaly detection for industrial big data," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3469–3477, 2021.
- [15] A. Telea, "An image inpainting technique based on the fast marching method," *Journal of Graphics Tools*, vol. 9, no. 1, pp. 23–34, 2004.
- [16] F. Tang, Y. Ying, J. Wang, and Q. Peng, "A novel texture synthesis based algorithm for object removal in photographs," in *Advances in Computer Science - ASIAN 2004. Higher-Level Decision Making. ASIAN 2004. Lecture Notes in Computer Science*, vol. 3321, M. J. Maher, Ed., pp. 248–258, Springer, Berlin, Heidelberg, 2004.
- [17] J. Hays and A. A. Efros, "Scene completion using millions of photographs," *Communications of the ACM*, vol. 51, no. 10, pp. 87–94, 2008.
- [18] C. Barnes, D. B. Goldman, E. Shechtman, and A. Finkelstein, "The PatchMatch randomized matching algorithm for image manipulation," *Communications of the ACM*, vol. 54, no. 11, pp. 103–110, 2011.
- [19] J. Sun, "Computing nearest-neighbor fields via Propagation-Assisted KD-Trees," in *2012 IEEE Conference on Computer Vision and Pattern Recognition*, pp. 111–118, Providence, RI, USA, June 2012.
- [20] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, pp. 577–590, 2018.
- [21] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.
- [22] Y. Xu, C. Zhang, Q. Zeng, G. Wang, J. Ren, and Y. Zhang, "Blockchain-enabled accountability mechanism against information leakage in vertical industry services," *IEEE Transactions on Network Science and Engineering*, p. 1, 2020.
- [23] Y. Xu, Q. Zeng, G. Wang, C. Zhang, J. Ren, and Y. Zhang, "An efficient privacy-enhanced attribute-based access control mechanism," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 5, pp. 1–10, 2020.
- [24] L. Qi, C. Hu, X. Zhang et al., "Privacy-aware data fusion and prediction with spatial-temporal context for smart city industrial environment," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4159–4167, 2021.
- [25] X. Yan, Y. Xu, B. Cui, S. Zhang, T. Guo, and C. Li, "Learning URL embedding for malicious website detection," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6673–6681, 2020.
- [26] X. Zhou, W. Liang, S. Shimizu, J. Ma, and Q. Jin, "Siamese neural network based few-shot learning for anomaly detection in industrial cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5790–5798, 2021.
- [27] Y. Xu, X. Yan, Y. Wu, Y. Hu, W. Liang, and J. Zhang, "Hierarchical bidirectional RNN for safety-enhanced 5G heterogeneous networks," *IEEE Transactions on Network Science and Engineering*, p. 1, 2021.
- [28] X. Zhou, Y. Li, and W. Liang, "CNN-RNN based intelligent recommendation for online medical pre-diagnosis support," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 18, no. 3, pp. 912–921, 2021.
- [29] I. Goodfellow, J. Pouget-Abadie, M. Mirza et al., "Generative adversarial networks," *Advances in Neural Information Processing Systems*, vol. 3, pp. 2672–2680, 2014.
- [30] Z. Cai, Z. Xiong, H. Xu, P. Wang, W. Li, and Y. Pan, *Generative Adversarial Networks: A Survey Towards Private and Secure Applications*, ACM Computing Surveys, 2021.
- [31] P. Krahenbuhl, J. Donahue, T. Darrell, and A. Efros, "Context-encoders: feature learning by inpainting," in *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 2536–2544, Las Vegas, NV, USA, June 2016.
- [32] S. Iizuka, E. Simo-Serra, and H. Ishikawa, "Globally and locally consistent image completion," *ACM Transactions on Graphics*, vol. 36, no. 4, pp. 1–14, 2017.
- [33] J. Yu, Z. Lin, J. Yang, X. Shen, and X. Lu, "Generative image inpainting with contextual attention," in *In Proceedings of the 2018 IEEE Conference on Computer Vision and Pattern Recognition*, pp. 5505–5514, Salt Lake City, UT, USA, 2018.
- [34] H. Zhang, I. Goodfellow, D. Metaxas, and A. Odena, "Self-attention generative adversarial networks," 2018, <https://arxiv.org/pdf/1805.08318.pdf>.
- [35] J. Yu, Z. Lin, J. Yang, X. Shen, X. Lu, and T. Huang, "Free-form image inpainting with gated convolution," in *In Proceedings of the 2019 IEEE/CVF International Conference on Computer Vision (ICCV)*, pp. 4470–4479, Seoul, Korea(South), 2019.
- [36] C. Kun, W. Fei, L. Lizhi, Y. Zhaokun, and W. Qian, "Face completion algorithm based on condition generation adversarial network," *Transducer and Microsystem Technologies(China)*, vol. 38, pp. 129–132, 2019.
- [37] C. Xie, S. Liu, C. Li et al., "Image inpainting with learnable bidirectional attention maps," in *In Proceedings of the 2019 IEEE/CVF International Conference on Computer Vision (ICCV)*, pp. 8857–8866, Seoul, Korea(South), 2019.

- [38] K. Nazeri, E. Ng, F. Joseph, F. Qureshi, and M. Ebrahimi, "EdgeConnect: generative image inpainting with adversarial edge learning," 2019, <https://arxiv.org/pdf/1901.00212v3.pdf>.
- [39] T. Miyato, T. Kataoka, M. Koyama, and Y. Yoshida, *Spectral Normalization for Generative Adversarial Networks*, International Conference on Learning Representations, Vancouver Convention Center, Vancouver Canada, 2018.
- [40] G. Liu, F. Reda, K. Shih, T.-C. Wang, A. Tao, and B. Catanzaro, "Image inpainting for irregular holes using partial convolutions," in *In Proceedings of the European Conference on Computer Vision*, pp. 89–105, 2018.
- [41] G. E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality of data with neural networks," *Science*, vol. 313, no. 5786, pp. 504–507, 2006.
- [42] I. Mokris and L. Skovajsova, "Proposal of cascade neural network model for text document space dimension reduction by latent semantic indexing," in *In Proceedings of the 2008 6th International Symposium on Applied Machine Intelligence and Informatics*, pp. 79–84, 2008.
- [43] A. Latreche and L. Guezouli, "Similarity measure for semi-structured information retrieval based on the path and neighborhood," in *In Proceedings of the 2012 International Conference on Information Technology and e-Services*, pp. 1–5, 2012.
- [44] J. Johnson, A. Alahi, and L. Fei-Fei, "Perceptual losses for real-time style transfer and super-resolution," in *In Proceedings of the Computer Vision - ECCV 2016*, pp. 694–711, Amsterdam, The Netherlands, 2016.
- [45] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *In Proceedings of the 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 770–778, Las Vegas, NV, USA, 2016.
- [46] W. Fupin, L. Wenlou, L. Ying, L. Jin, and G. Yanchao, "Face inpainting algorithm combining edge information with gated convolution," *Journal of Frontiers of Computer Science and Technology(China)*, vol. 15, pp. 150–162, 2021.
- [47] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *Computer Science*, vol. 4, pp. 1409–1421, 2014.
- [48] Z. Liu, P. Luo, X. Wang, and X. Tang, "Deep learning face attributes in the wild," in *In Proceedings of the 2015 IEEE International Conference on Computer Vision (ICCV)*, pp. 3730–3738, Sadversarial ago, Chile, 2015.
- [49] D. Kingma and J. Ba, "Adam: a method for stochastic optimization," *Computer Research Repository*, vol. 12, pp. 1–6, 2014.

## Research Article

# A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection

Yingwen Chen,<sup>1</sup> Linghang Meng,<sup>1</sup> Huan Zhou ,<sup>1</sup> and Guangtao Xue<sup>2</sup>

<sup>1</sup>College of Computer, National University of Defense Technology, Changsha 410073, China

<sup>2</sup>School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

Correspondence should be addressed to Huan Zhou; [huanzhou@nudt.edu.cn](mailto:huanzhou@nudt.edu.cn)

Received 11 December 2020; Accepted 10 June 2021; Published 1 July 2021

Academic Editor: Yaguang Lin

Copyright © 2021 Yingwen Chen et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The rapid development of wearable sensors and the 5G network empowers traditional medical treatment with the ability to collect patients' information remotely for monitoring and diagnosing purposes. Meanwhile, the health-related mobile apps and devices also generate a large amount of medical data, which is critical for promoting disease research and diagnosis. However, medical data is too sensitive to share, which is also a common issue for IoT (Internet of Things) data. The traditional centralized cloud-based medical data sharing schemes have to rely on a single trusted third party. Therefore, the schemes suffer from single-point failure and lack of privacy protection and access control for the data. Blockchain is an emerging technique to provide an approach for managing data in a decentralized manner. Especially, the blockchain-based smart contract technique enables the programmability for participants to access the data. All the interactions are authenticated and recorded by the other participants of the blockchain network, which is tamper resistant. In this paper, we leverage the K-anonymity and searchable encryption techniques and propose a blockchain-based privacy-preserving scheme for medical data sharing among medical institutions and data users. To be specific, the consortium blockchain, Hyperledger Fabric, is adopted to allow data users to search for encrypted medical data records. The smart contract, i.e., the chaincode, implements the attribute-based access control mechanisms to guarantee that the data can only be accessed by the user with proper attributes. The K-anonymity and searchable encryption ensure that the medical data is shared without privacy leaking, i.e., figuring out an individual patient from queries. We implement a prototype system using the chaincode of Hyperledger Fabric. From the functional perspective, security analysis shows that the proposed scheme satisfies security goals and precedes others. From the performance perspective, we conduct experiments by simulating different numbers of medical institutions. The experimental results demonstrate that the scalability and performance of our scheme are practical.

## 1. Introduction

Data sharing is crucial for promoting the research of disease tracking and treatment. For instance, the sharing of substantial medical data can help government agencies make correct decisions in public health or help medical research institutions conduct scientific research to promote the progress of medical science. The fight against to current epidemic of COVID-19 also proves that efficient medical information sharing among different institutions can effectively trace the disease and accelerate the vaccine development. The application of wearable medical devices and health-related mobile apps alleviate the difficulty of personal medical data collec-

tion and retrieving, but for the following stages of data management, the security and privacy of the data have become the top concern at the same time.

Traditional approaches are based on clouds to store data remotely and different institutions share the data in a centralized manner. The top two challenges for these methods are privacy and security.

For the privacy issue, any data user should not infer a specific patient private information, including the name, address, and phone number, from querying the stored medical records. If the privacy of the patient is not well protected during data sharing, the patient would be reluctant to share their medical data [1]. In addition, for sharing purposes,

the data is stored remotely on clouds. The patients and medical institutions have to trust that the cloud provider would not leak out the data, if the data is not encrypted. However, the encrypted data would hinder the sharing process.

K-anonymity [2] and differential privacy [3] are two commonly adopted techniques to protect data privacy. Comparing both, differential privacy is relatively new and got more attention in recent years due to its strong privacy guarantee. Differential privacy is usually achieved through adding noise to attributes or values [4], i.e., through simply adding or deleting some less important data in the original dataset. Though differential privacy defines an extremely strict attack model for guaranteeing privacy, the noise data it introduces may affect the statistical characteristics of the data. However, for the medical research purpose, the statistical characteristics are more important to study a disease instead of focusing on some individual patients. Therefore, the K-anonymity [2] technique is more suitable for preprocessing the medical data, which obscures some sensitive data fields without affecting the original data. The accuracy of the statistical results on the data, therefore, can be preserved. On the other hand, the medical data are encrypted and stored on untrusted clouds. Searchable encryption is a potential solution which allows the server to search on encrypted data without knowing the content of the data [5].

For the security issue, cloud-based data platforms have problems of a single point of failure, vulnerability, and inefficiency. Besides, cloud-based data sharing relies on third-party services and there may exist stealing, leakage, tampering, or misusing of data. Although existing cryptography-related solutions have solved some problems of the cloud, the single point of failure problem cannot be solved. On the other hand, the access control for medical data management is also centralized and usually based on roles. However, the RBAC (role-based access control) model requires configuring complex rules to restrict the accessibility of different types of data users. Especially, the process of configuring and updating rules is vulnerable that the attack may leverage the loophole and easily elevate privileges to obtain the grant for the entire dataset, due to the centralized data storage.

Blockchain is a distributed ledger, which has the characteristics of decentralization, tamper resistance, and reliability. Thus, blockchain is a potential solution to replace centralized cloud storage. The blockchain-based smart contract provides a decentralized manner to authenticate the data access request among participants of different institutions. The ABAC (attribute-based access control) model can be further leveraged to simplify configurations for restricting the data accessibility according to the users' assigned attributes.

In this paper, we propose a privacy-preserving scheme based on the blockchain for medical data sharing. To tackle the two challenges mentioned above, the contributions of our developed system are as follows:

- (i) We adopt the K-anonymity technique to preprocess the data for privacy preserving
- (ii) We design the scheme based on searchable encryption for storing the encrypted medical data on clouds and

enable the keyword search in a privacy-preserving manner

- (iii) We develop smart contracts based on Hyperledger Fabric, and realize the secure keyword search and the attribute-based access control model
- (iv) We implement a prototype system with smart contracts based on a chaincode of Hyperledger Fabric (the URL of source code: <https://github.com/mythsand/privacy-preserving-medical-data>) and conduct experiments with simulating different numbers of institutions
- (v) We analyze the security properties and evaluate the computational overhead

The rest of the paper is organized as follows. Section 2 explains the preliminaries related to this paper, including K-anonymity, bilinear pairings, blockchain, and access control. Then, we formulate the problem with explaining the security goal and notions. The system design and technique details are introduced in Section 4. Security analysis and experimental studies are demonstrated in Section 5 and Section 6, respectively. Section 7 presents the related work and Section 8 finally concludes the paper.

## 2. Preliminaries

*2.1. K-Anonymity.* K-anonymity was the first model proposed to protect data privacy through syntax [2]. Its main idea is to make reidentification infeasible by hiding  $K$  objects in the same group. That is to say, K-anonymity requires that each record in the anonymized data cannot be distinguished from other at least  $K-1$  records. Quasi-identifier attributes, e.g., social security numbers, state liquor identification cards, drivers' licences, and even passports or national identity cards, are concerned. Therefore, no identity in the K-anonymous dataset will be linked to fewer than  $K$  records. That is, the probability of correct reidentification is at most  $1/K$ . Several definitions of K-anonymity related to this paper are explained below. Here, we assume that all the information is in a table  $S$ , which contains multiple tuples.

*Definition 1.* (quasi-identifier attribute set). A quasi-identifier is a minimal set of attributes in table  $S$  that can be combined with external information records to reidentify personal information. This paper assumes that quasi-identifiers are known based on empirical data and epistemology.

*Definition 2.* (equivalent class). The equivalent class in table  $S$  indicates that each tuple is the same as several other tuples.

*Definition 3.* (K-anonymity property). Table  $S$  is a set of determined values of the attribute group in  $K$  that is anonymized to appear at least  $K$  times in  $S$ , i.e., each of the equivalent classes is at least  $K$  in size.

*2.2. Bilinear Pairings.* The scheme of our encrypted search is constructed based on bilinear maps, the definition of which is described as follows:



**2.2.1. Bilinear Map.** For two cyclic groups  $G_1$  and  $G_2$  of order  $p$ , there is a bilinear map  $e$  between them:  $e : G_1 * G_1 \longrightarrow G_2$ . The map relation satisfies following three properties:

- (1) **Computability:** given  $g_1, g_2 \in G_1$ , algorithms to compute  $e(g_1, g_2) \in G_2$  can finish within a polynomial time
- (2) **Bilinearity:** for any integers  $x, y \in [1, p]$ ,  $e(g^x, g^y) = e(g, g)^{xy}$
- (3) **Nondegeneracy:** if  $g$  is a generator of  $G_1$ , then  $e(g, g)$  is a generator of  $G_2$ . In other words, this can be simplified as  $e(g, g) \neq 1$

The size of  $G_1, G_2$  is determined by the security parameter.

**2.2.2. Decisional Bilinear Diffie-Hellman (DBDH) Assumption.** Suppose an adversary chooses random  $a, b, c, z \in \mathcal{Z}_p$ , the DBDH assumption [6] means that there is no adversary, who can distinguish the tuple  $(A = g^a, B = g^b, C = g^c, Z = e(g, g)^{abc})$  from the tuple  $(A = g^a, B = g^b, C = g^c, Z = e(g, g)^z)$ , within a probabilistic polynomial time with a nonnegligible advantage.

**2.3. Blockchain and Smart Contract.** The consortium blockchain provides a permissioned design, which is different from the private blockchain and the public blockchain. It does not require the same level of strict control and restriction as the private blockchain. Meanwhile, it is not completely decentralized as the public blockchain. The consortium blockchain is maintained and operated by several trusted nodes. Besides, the consortium blockchain has the advantages of promoting openness and collaboration, marvelous data control, and node management and speeding up the operation of the system. In this paper, we build a medical data sharing system based on Hyperledger Fabric. Hyperledger is an open source project under the Linux Foundation and is supported by companies such as IBM, Intel, and Sap. Hyperledger Fabric is one of the implemented blockchains. This consortium blockchain has the advantages of high throughput, low latency, and scalability. It is a popular choice in the industrial blockchain scenario.

**2.4. Access Control.** Attribute-based access control (ABAC) is a type of access control technology that considers attributes, objects, permission, and environment as input. It determines whether to grant authorization by examining whether the object contains the proper attributes. ABAC can provide fine-grained access control, which can support a large number of input decision sets, define many possible rules, and express many strategies, but with only limited computing consumption and attributes. Such flexibility can decouple the relationship between the subject and the object. For instance, an employee is given attributes in the subject's attribute set, e.g., a nurse in a certain hospital. Objects are given attributes when they are created, e.g., medical data of patients with diabetes. Object owners will define attributes to set access control rules at the beginning of the creation, e.g., all nurses in the hospital can access the medical data of patients

with diabetes. Under attribute-based access control, access decisions can be modified by simply changing the attribute value without affecting the relationship between a single subject and an object. Hence, ABAC can provide more dynamic and flexible access control management capabilities, reducing long-term maintenance costs. In addition, ABAC can be performed without any knowledge of new subjects, which means that there is no need to modify the existing rules.

### 3. Problem Formulation

**3.1. Problem Scenario.** There are four main roles in our problem scenario, data owner, medical institution, and data user. The respective responsibility and operations of these roles are as follows.

- (i) Data owners, i.e., patients, share their medical data with medical institutions, including personally identifiable information and medical data
- (ii) Medical institutions extract medical data keywords, perform keyword search, and conduct access control
- (iii) Data users are entities that need to be authorized to perform keyword searches and obtain the required data, such as research institutions, insurance companies, or government departments. Data users need to be authorized first by access control and then can perform a keyword search on medical data

**3.2. Security Goal.** Here, we address the security goals as follows in our scheme.

**3.2.1. Privacy Preserving.** With all these patient personal information and medical data involved in this scheme, the major challenge is to preserve the privacy of all patients. No matter who wants to approach the patients' health data, the identity information must be controlled or limited.

**3.2.2. Security Search.** If data users want to obtain patients' health data, they have to get through the access control mechanism. Meanwhile, the searching and query process should not leak information related to the keywords.

**3.2.3. Data Integrity and Reliability.** In addition to data privacy issues, there are data security issues. The patient's data should not be tampered and deleted after uploading, i.e., the integrity and reliability of the data should be guaranteed.

#### 3.3. Notions

- (i) **SID:** the patient identifier, which can be used to denote one specific patient, such as the social security number
- (ii) **QID:** quasi-identifier, such as zip code, address, age, gender, and birthday
- (iii)  **$M$ :** the medical institution collection, denoted as a set of  $m$  medical institutions  $M = (M_1, M_2, \dots, M_m)$
- (iv)  **$D_i$ :** the plain medical data text of  $M_i$ , denoted as a set of  $n$  data  $D_i = (D_{i,1}, D_{i,2}, \dots, D_{i,n})$



- (v)  $C_i$ : the ciphertext of medical data; medical data can be encrypted by a medical institution, denoted as  $C_i = (C_{i,1}, C_{i,2}, \dots, C_{i,n})$
- (vi)  $W$ : the keywords of medical data that can represent a medical data, denoted as a set of  $u$  keywords  $W = (w_1, w_2, \dots, w_u)$
- (vii)  $\widehat{W}$ : encrypted keyword of  $W$ , medical institutions' encrypted keyword collection, denoted as  $\widehat{W} = (\widehat{w}_1, \widehat{w}_2, \dots, \widehat{w}_u)$
- (viii)  $\widetilde{W}$  represents the queried keywords and the subset of the keywords  $W$ , denoted as a set of  $q$  keywords  $\widetilde{W} = (w_1, w_2, \dots, w_q)$
- (ix)  $T$ : the trapdoor for  $\widetilde{W}$ , denoted as  $T = (T_{w_1}, T_{w_2}, \dots, T_{w_q})$
- (x)  $K_{\text{pub}}$ : the public key
- (xi)  $K_{\text{priv}}$ : the private key
- (xii)  $\lambda$ : the security parameter

#### 4. System Design and Technique Details

To tackle the issue of privacy protection and access control for sensitive medical data, we propose and develop a system based on the consortium blockchain platform with K-anonymity and searchable encryption techniques. The technologies adopted in this paper are designed and selected for medical data and medical data application scenarios. Medical data mainly has two kinds of privacy characteristics: data privacy and identity privacy. And the application scenarios of medical data are the coexistence of multiple medical institutions, similar to the P2P network in the computer network. The following is a detailed analysis and explanation.

- (1) For data privacy, this paper extracts keywords from medical data and further encrypts and searches the keywords with a searchable encryption technology, which not only protects the privacy of data but also ensures the availability of data
- (2) As for identity privacy, the current technologies to protect identity privacy include differential privacy and K-anonymity. Based on the characteristics of medical data, K-anonymity is chosen in this paper. The main consideration is that differential privacy will change the original statistical data characteristics of medical data, and that is more important to medical data. K-anonymity can retain the statistical characteristics of data. Therefore, we choose K-anonymity
- (3) For the application scenario of medical data sharing, this paper adopts the consortium blockchain. Each medical institution is acting as one node of the consortium blockchain. The consortium blockchain is in line with the medical data sharing scenario of a

peer-to-peer network and authorized access. On the contrary to the public blockchain, the data stored and managed by the consortium blockchain can keep being secured and private, instead of being totally transparent

In this section, we first introduce the system overview and then zoom into the detailed techniques adopted.

*4.1. System Overview.* Figure 1 shows the architecture overview of our system. We introduce the consortium blockchain as the middleware to perform as the trust layer. After patients upload data, i.e., medical data, to medical institutions. The medical institutions need to preprocess the data with a K-anonymity technique to blur some sensitive data fields which can probably reflect the patient's identity. Then, the keywords are extracted from the dataset and form the index. We design a scheme based on searchable encryption to encrypt the dataset and the index, i.e., the keyword. The entire encrypted dataset is uploaded to the cloud and managed by the medical institution itself. The encrypted data are uploaded to the consortium blockchain platform, which is constructed by different medical institutions. Each medical institution acts as a participant node in the platform. We develop smart contracts and deploy them on the blockchain platform. The smart contracts provide all the related interfaces for medical institutions and data users to leverage. One of the interfaces is designed for data users to query with the keyword index. According to our searchable encryption scheme, the corresponding results can be fetched back to the data user from clouds without decrypting the secured data. The searching process is also implemented by the smart contract. Besides, the smart contract also provides the interface of access control based on the attributes of data users.

In this paper, K-anonymity and searchable encryption are different from traditional application scenarios. The implementation of K-anonymity in this paper is different from the traditional way of centralized processing and centralized storage. The process of the K-anonymity algorithm adopted in this paper is processed by distributed nodes. The results of processing are stored on the consortium blockchain, and all nodes in the blockchain network can access them. As for searchable encryption, in traditional application scenarios, the processing and calculation modes are centralized. In this paper, the searchable encryption scheme based on the blockchain platform is implemented with smart contracts, including the calculation process of trapdoor generation and keyword matching, which are also in a decentralized manner.

The consortium blockchain network in this paper is based on blockchain nodes, and each medical institution acts as one node of the blockchain network. For the newly joined nodes, i.e., medical institutions, they need to apply for certificates from the authority node and then join the blockchain network with certificates. Among them, the authority node is the root of trustworthiness in the consortium blockchain, which can be played by the authoritative management department of the medical institution.

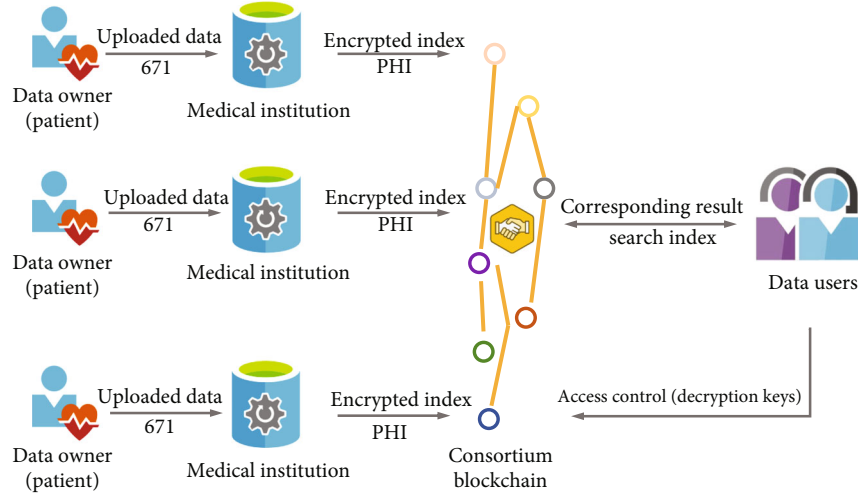


FIGURE 1: The system architecture overview.

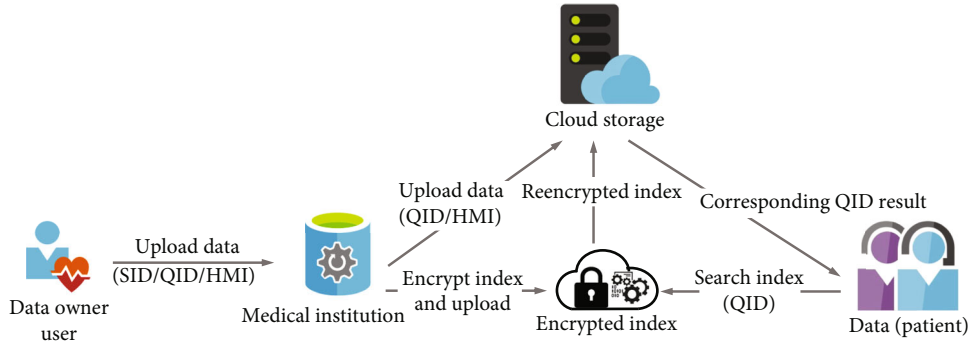


FIGURE 2: The process of medical data preprocessing, uploading, and querying with searchable encryption.

Figure 1 shows the entire architecture with multiple medical institutions. For the following parts in this section, we zoom into the details and explain how the techniques are leveraged. Hence, for a specific medical institution, Figure 2 demonstrates how the medical institution preprocesses the data and uploads the data to a remote cloud. The personal SID is firstly removed and then the K-anonymity is adopted to blur the QID. Afterwards, the preprocessed data is encrypted and uploaded to the remote cloud. Finally, data users can perform queries without decrypting the data. The related technique is described as follows.

4.2. *K-Anonymity*. Mondrian multidimensional partitioning [7] is a K-anonymous multidimensional partitioning algorithm with K-anonymous processing in two steps. In the first step, the multidimensional regions covering all the domain space attributes are defined, i.e., the partition stage constructs kd-trees [8]. The second step is to construct functions for data recoding.

The partitioning algorithm is described in Algorithm 1. In the algorithm, each dimension selects the dimension and the value of the partition. In the literature of kd-trees, one approach is to use the median as the value of the partition. The partition is completed to get k-groups, and each k-group spontaneously includes at least k records. Each k-

```

Input: Table S to be partitioned.
Output: Partitioning result.
1: Anonymize(partition)
2: if (no allowable multidimensional cut for partition) then
3:   return  $\phi$ : partition  $\rightarrow$  summary
4: else
5:   dim  $\leftarrow$  choose_dimension()
6:   fs  $\leftarrow$  frequencySet(partition, dim)
7:   splitVal  $\leftarrow$  find.median(fs)
8:   lhs  $\leftarrow$   $t \in$  partition: t.dim  $\leq$  splitVal
9:   rhs  $\leftarrow$   $t \in$  partition: t.dim  $>$  splitVal
10:  return Anonymize(rhs)  $\cup$  Anonymize(lhs)
11: end if
    
```

ALGORITHM 1: Mondrian partitioning algorithm.

group is then generalized. Thereby, the QID of each group is the same.

For the selection of parameter K in the algorithm, the principle we follow is to get the value of the K-anonymity parameter K after the practical test in the practical application scenarios, so as to protect the patient's identity privacy and not make the system query results too redundant.

TABLE 1: Patient data.

Age	Sex	Zip code	Disease
25	Male	53711	Flu
25	Female	53712	Hepatitis
26	Male	53711	Bronchitis
27	Male	53710	Broken arm
27	Female	53712	AIDS
28	Male	53711	Hang nail

TABLE 2: A 2-anonymity example.

Age	Sex	Zip code	Disease
[25–26]	Male	53711	Flu
[25–27]	Female	53712	Hepatitis
[25–26]	Male	53711	Bronchitis
[27–28]	Male	[53710–53711]	Broken arm
[25–27]	Female	53712	AIDS
[27–28]	Male	[53710–53711]	Hang nail

4.2.1. *Before Processing.* For example, supposing that the patient data structure is shown in Table 1, QID includes the age, sex, and zip code. These attributes that appear in private personal data may also appear in public datasets. If the two sets of data are linked together, the patient's private data may be leaked. Therefore, these attributes need to be processed by the K-anonymous algorithm to avoid privacy leakage.

4.2.2. *After Process.* The multidimensional anonymization of patients is shown in Table 2. It shows that with the condition of 2-anonymity, each record has another one record, whose QID attributes are exactly the same.

4.3. *Searchable Encryption.* In this paper, we assume that there are several medical institutions with different keys that participate. Then, we are faced with the problem of how to search the different key encrypted keywords in multiple medical institutions. To achieve a secure search for multiple medical institutions, we have adopted a secure search scheme that satisfies the following three conditions:

- (i) Different medical institutions encrypt keywords with their own keys
- (ii) The data user does not need to know the key when generating the trapdoor
- (iii) After retrieving the trapdoor, the cloud server can search for the corresponding data content through the keywords without knowing the specific value, as the keywords are encrypted by multiple medical institutions

The cloud server mentioned in this section refers to the computing and storage resources provided by the public cloud service provider (CSP), to form a running unit and

provide services to clients. In addition, the middle server is provided by a specific trusted organization to provide the system with completely credible and reliable services, such as secret keys and crucial information storage.

Figure 2 shows the detailed process of using searchable encryption to manage the data. It is worth mentioning that the encrypted index is stored in the consortium blockchain and the encrypted dataset is uploaded to a remote cloud managed by a third party. In order to explain the procedure shown in Figure 2, we use an example to illustrate the details of this scheme. Medical institution  $i$ , i.e.,  $M_i$ , needs to encrypt  $D_i$  into  $C_i$  with its own key before sharing medical data  $D_i$ . At the same time, in order for the data user to be able to perform search, the medical institution needs to extract the keyword  $w_{i,h}$  from the document and send the encrypted keyword  $\hat{w}_{i,h} = (E_a', E_0)$  to the middle server. The middle server is further encrypted,  $E_a'$  to  $E_a$ , and obtains  $\hat{w}_{i,h} = (E_a, E_0)$ ; then, the result is sent to the cloud server. Next, assume data user  $U$  wants to search for a document related to the keyword  $w_h'$ . Basically, he needs to generate a trapdoor  $T'_{w_h'}$  and upload it to the middle server. The middle server then reencrypts the trapdoor  $T'_{w_h'}$  to obtain  $T_{w_h'}$ , while generating secret data  $S_a$ . Then,  $T_{w_h'}$  and  $S_a$  are uploaded to the cloud server. The cloud server finally calculates  $\tilde{e}(E_o, T_3) = \tilde{e}(E_o, T_1) \cdot \tilde{e}(S_a, T_2)$  for keyword search.

4.3.1. *Encryption Construction.* The construction is based on a bilinear map. We define  $g$  to be the generators of the cyclic groups,  $G_1$  and  $G_2$ , whose orders both are  $p$ .  $\hat{e}$  is a bilinear map  $\hat{e}: G_1 \times G_1 \rightarrow G_2$ . In the process of encryption construction, the random key generation algorithm generates different keys for different inputs.  $k_{m1} \in \mathbb{Z}_p^+$ ,  $k_{m2} \in \mathbb{Z}_p^+$ ,  $k_{i,w} \in \mathbb{Z}_p^+$ ,  $k_{i,d} \in \mathbb{Z}_p^+ \leftarrow (0, 1)^*$ .  $k_{m1}$  and  $k_{m2}$  are the private keys of the middle server;  $k_{i,w}$  and  $k_{i,d}$  are the private keys used to encrypt keywords and data of medical institution  $M_i$ , respectively.  $H(\cdot)$ , located in  $\mathbb{Z}_p^+$ , is a hash function.

4.3.2. *Keyword Encryption.* The keys of different medical institutions are different in this system, and the ciphertext generated each time for the same keyword is different. Therefore, even if the key is lost, the data cannot be leaked, since the cloud server cannot obtain any information about the keyword. For the  $h$ th keyword of the medical institution  $M_i$ , i.e.,  $w_{i,h}$ , the process of encryption calculation is as follows.

$$\hat{w}_{i,h} = \left( g^{k_{i,w} \cdot r_o \cdot H(w_{i,h})}, g^{k_{i,w} \cdot r_o} \right), \quad (1)$$

where  $r_o$  is a number generated randomly each time, which is leveraged to calculate  $E_a' = g^{k_{i,w} \cdot r_o \cdot H(w_{i,h})}$  and  $E_o = g^{k_{i,w} \cdot r_o}$ .

The medical institution submits  $\hat{w}_{i,h} = (E_a', E_o)$  to the middle server, and the middle server reencrypts  $E_a'$  with its own keys,  $k_{m1}$  and  $k_{m2}$ , to obtain  $E_a$ , as follows.

$$E_a = \left( E_a' \cdot g^{k_{m1}} \right)^{k_{m2}}. \quad (2)$$

Finally, the middle server submits the  $\widehat{w}_{i,h} = (E_a, E_o)$  to the cloud server. In the entire process, the middle server is always unable to know the specific value of the keyword.

**4.3.3. Trapdoor Generation.** In the scheme that we propose, data users do not need to know the key of the medical institution and the trapdoors generated for the same keyword each time are different. The trapdoor is generated in two steps. First, the data user generates a trapdoor based on the search key and the random number and then submits the trapdoor to the middle server. Second, the middle server reencrypts the trapdoor. Here, we assume that the data user wants to search for the keyword  $w_h'$  and the encryption is calculated as follows.

$$T'_{w_h'} = \left( g^{H(w_h') \cdot r_u}, g^{r_u} \right), \quad (3)$$

where  $r_u$  is a random number generated randomly each time. After receiving the  $T'_{w_h'}$ , the middle server generates a random number  $r_m$  and reencrypts  $T'_{w_h'}$  as follows.

$$T_{w_h'} = \left( g^{H(w_h') \cdot r_u \cdot k_{m1} \cdot k_{m2} \cdot r_m}, g^{r_u \cdot k_{m1}}, g^{r_u \cdot k_{m1} \cdot r_m} \right). \quad (4)$$

Let us make  $T_1 = g^{H(w_h') \cdot r_u \cdot k_{m1} \cdot k_{m2} \cdot r_m}$ ,  $T_2 = g^{r_u \cdot k_{m1}}$ ,  $T_3 = g^{r_u \cdot k_{m1} \cdot r_m}$ , i.e.,  $T_{w_h'} = (T_1, T_2, T_3)$ . Finally, the middle server submits  $T_{w_h'}$  to the cloud server.

**4.3.4. Keyword Matching.** In the scheme that we proposed in this paper, the cloud server stores encrypted data and keywords for all medical institutions. The middle server needs to transfer a secret data  $S_a = g^{k_{m1} \cdot k_{m2} \cdot r_m}$  to the cloud server. After receiving the search request, the cloud server performs a global search to match all stored keywords, in order to obtain the corresponding medical data. The searching process is described as follows. First of all, the cloud server performs the following calculations, after getting trapdoors,  $T_{w_h'}$  and  $(E_a, E_o)$ .

$$\widehat{e}(S_a, T_2) = \widehat{e}\left(g^{k_{m1} \cdot k_{m2} \cdot r_m}, g^{r_u \cdot k_{m1} \cdot r_m}\right) = \widehat{e}(g, g)^{r_u \cdot k_{m1} \cdot k_{m2} \cdot r_u \cdot k_{m1}}. \quad (5)$$

Then, the cloud server judges whether  $w_h$  equals to  $w_h'$ , according to the following equation.

$$\begin{aligned} \widehat{e}(E_a, T_3) &= \widehat{e}\left(\left(g^{k_{i,w} \cdot r_o \cdot H(w_{i,h})} \cdot g_{k_{m1}}\right)^{k_{m2}}, g^{r_u \cdot k_{m1} \cdot r_m}\right) \\ &= \widehat{e}(g, g)^{(k_{i,w} \cdot r_o \cdot H(w_{i,h}) + k_{m1}) \cdot r_u \cdot k_{m1} \cdot r_m} \\ &= \widehat{e}(g, g)^{k_{i,w} \cdot r_o \cdot H(w_{i,h}) \cdot r_u \cdot k_{m1} \cdot r_m} \cdot \widehat{e}(S_a, T_2) \\ &= \widehat{e}\left(g^{k_{i,w} \cdot r_o}, g^{H(w_{i,h}) \cdot r_u \cdot k_{m1} \cdot r_m}\right) \cdot \widehat{e}(S_a, T_2) \\ &= \widehat{e}(E_o, T_1) \cdot \widehat{e}(S_a, T_2). \end{aligned} \quad (6)$$

**4.4. Consortium Blockchain and Attribute-Based Access Control.** The consortium blockchain is the crucial part of

the entire scheme. All new nodes must get the certification from the fabric-CA before participating in the consortium blockchain. The consortium blockchain implements a chaincode of searchable encryption and ABAC. At the same time, the blockchain exposes interfaces for users to access blockchain data, including access control interfaces and data interfaces. The functions implemented by the consortium blockchain are as follows:

- (i) The chaincode implements the function for uploading encrypted data to the ledger of the blockchain
- (ii) The chaincode provides the function of searchable encryption
- (iii) The chaincode provides ABAC to manage the permissions for user access

For the ABAC part, policy management and access control are separated. Policies may vary with the actual scenario, for instance, by increasing or decreasing the number of attributes to accommodate larger or smaller scenarios. The key part of ABAC is the attribute which can be defined as  $A \in \{S, O, P, E\}$ . The definition of each field is as follows:

- (i)  $A$  indicates the attribute. Each attribute has an identifier
- (ii)  $S$  indicates the subject's attributes, i.e., the identity and characteristics of the subject which can perform the access request, for instance, the entity's name, age, and occupation
- (iii)  $O$  indicates the object's attributes, i.e., the information related to the accessed resource, for instance, resource type, service location, and protocol
- (iv)  $P$  indicates the permission, i.e., the operation of the subject which can be performed on the object, for instance, reading, writing, and executing
- (v)  $E$  indicates the environment, i.e., the environment information when the access request is initiated, for instance, time and location

The attribute-based access control policy can be defined as  $\{S \wedge \text{or } \vee O \wedge \text{or } \vee P \wedge \text{or } \vee E\}$ , which indicates the access control rules of the subject to access the object. It expresses the required attribute set for accessing the protected resources. The above expression means that the XOR relationship among the subject, object, permission, and environment constitutes the access grants of the access control mechanism.

The attribute-based access control request can be defined as  $\{A \wedge O \wedge P \wedge E\}$ , as mentioned above, which is a set of attributes. It indicates the operation of the subject on the object under the environment. When users access the ABAC system, the attribute set constitutes the access request operation, which is used as the input parameter to initiate the access request of the access control mechanism in the system.



## 5. Security Analysis

In this section, we discuss that our scheme satisfies the following security goals.

**5.1. Privacy Preserving.** Patient’s personal information and medical data are protected by searchable encryption and attribute-based access control. Medical institutions encrypt medical data, and the consortium blockchain provides access control, which is a proper way to avoid privacy disclosure to malicious entities.

**5.2. Security Search.** Data users need to obtain authorization of access control before they can search on the consortium blockchain. Therefore, malicious entities cannot initiate searches after access control, which guarantees the security of the data.

**5.3. Data Integrity and Reliability.** The patients’ medical data with encrypted keywords are uploaded by the medical institutions to the consortium blockchain. Thus, during the process of data storage and transmission, no one can modify or read data without the authorization of the medical institutions.

**5.4. Scheme Properties.** As for scheme properties, we compare the properties of our scheme with [9, 10] of the cloud-based one and [11] of the blockchain-based one. As shown in Table 3, our scheme can meet all the scheme properties which are vital properties of medical data sharing schemes.

## 6. Experimental Study

In this section, we implement the proposed scheme on the Hyperledger Fabric platform and evaluate its performance. Especially, we simulate different numbers of medical institutions to construct the blockchain platform for testing the performance and scalability of our system. For testing purposes, we leverage the docker to build a consortium blockchain platform with Hyperledger Fabric, which is contrusted using CloudsStorm [12] in the Cloud environment. The programming language is Python3.7 and Go1.12; the Fabric edition is 1.4. For the underlying server, we set up the environment with a virtual machine from the ExoGENI [13] cloud. The entire virtual machine is only for this purpose. The configuration of the virtual machine is the type of “XOXLarge,” which contains 4 CPU cores and a 12 GB RAM.

**6.1. Computational Cost.** In order to evaluate this scheme quantitatively, we have also conducted some experiments based on our scheme. We provide the details of the computational cost of functions in Table 4.

In our scheme, the *KeyGen* function is responsible for generating the public key and private key. And, the function *Enc* is used to encrypt the keywords of medical data. The trapdoor can be generated by the function of *TdGen*. Finally, the function of *Search* is for searching the expected keyword and the result can be “True” or “False.”

Due to the fact that the computational cost of these algorithms is related to keyword numbers, we test our algorithms

TABLE 3: Scheme properties.

	Liu [9]	Wang [10]	Azaria [11]	Proposed scheme
Blockchain	N	N	Y	Y
Access control	Y	Y	N	Y
Privacy preserving	Y	Y	N	Y
Searchable encryption	N	Y	N	Y

TABLE 4: Computational cost (in milliseconds).

	<i>KeyGen</i>	<i>Enc</i>	<i>TdGen</i>	<i>Search</i>
$w = 10$	71.49	115.66	83.39	620
$w = 50$	359.70	575.78	432.45	3510
$w = 100$	712.46	1168.90	880.17	6830

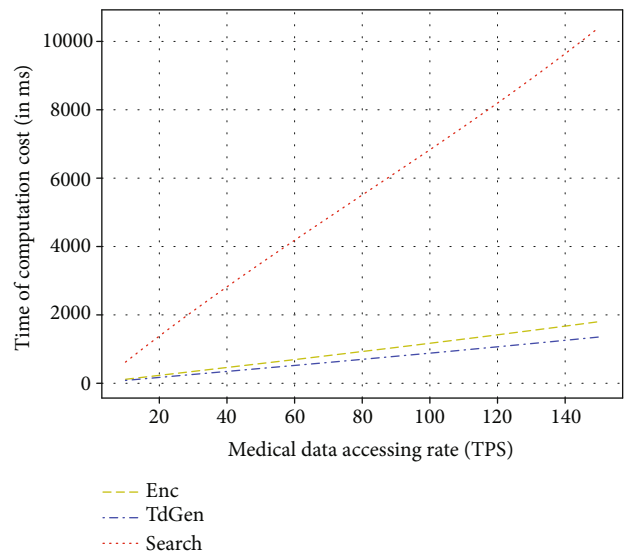


FIGURE 3: The computational cost of on-chain operations varying with different data access rates.

by setting keyword numbers as  $w = 10, 50,$  and  $100$ . As shown in Table 4, we can find out that the time cost of all functions, including *KeyGen*, *EncIndex*, *TdGen*, and *Search*, increases with the size of keyword amounts linearly.

Among these four main operations, three of them are implemented in the smart contracts of the consortium blockchain, including *Enc*, *TdGen*, and *Search*. Hence, to test the system performance for these on-chain operations, we measure the computational cost of these operations varying with different frequencies of operation requests, i.e., the medical data accessing rate in TPS (transactions per second). The number of keywords to be processed is set to once in each transaction, i.e., for each data accessing request. Five medical institutions are simulated here to construct the 5-node blockchain network. The experimental results are shown in Figure 3. It shows that the computational cost of all the on-chain operations is linear with the medical data accessing rate, which demonstrates that our system is scalable.



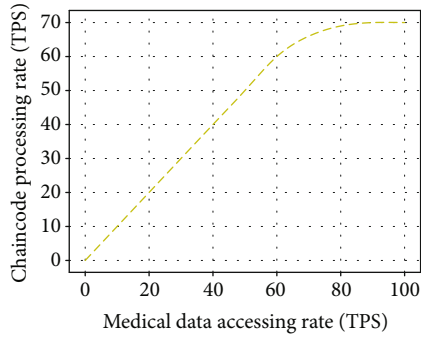


FIGURE 4: The performance of the keyword searching operation with searchable encryption under the scenario of 5 medical institutions.

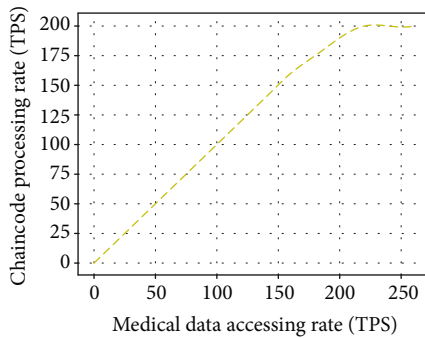


FIGURE 5: The performance of access control with the ABAC model under the scenario of 5 medical institutions.

**6.2. Performance of the Smart Contract.** In this subsection, we mainly test the performance of two types of chaincodes, i.e., smart contracts. One is designed for storing and searching the dataset, and the other is for attribute-based access control (ABAC). For this experiment, we simulate that there are five medical institutions, i.e., five nodes construct the experimental blockchain platform. Figure 4 shows the chaincode processing performance of the searching operation with searchable encryption when increasing the medical data accessing rate. In this scenario, the processing rate of the chaincode for searching operations increases linearly according to the increased medical data accessing rate. The system is able to handle all the requests when the accessing rate is not high. However, when the rate of accessing requests comes to 70 TPS, the processing rate cannot increase anymore. It demonstrates that the throughput of our system with 5 medical institutions is around 70 TPS. For the chaincode of the ABAC model, the performance is similar as shown in Figure 5. But the throughput for the ABAC chaincode is better than the chaincode with searching operations, which is around 200 TPS. As the medical information sharing is mainly for research purposes, the amount of requests is not at a large scale. Hence, the performance of our system is acceptable.

On the other hand, the memory consumption of the chaincode for realizing searchable encryption is also measured. The measurements are performed within the node where the chaincode for encryption is invoked. For testing,

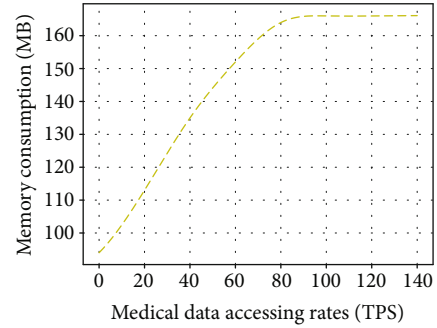


FIGURE 6: The memory consumption of the chaincode for performing operations of searchable encryption.

we input the system with different rates of medical data accessing requests. The experimental results shown in Figure 6 also demonstrate that the system is able to handle the accessing rate below of approximately 80 TPS. When the accessing rate further increases, the memory consumption stays steady afterwards. The reason is that the system has reached its capacity. Meanwhile, it is worth mentioning that the maximum memory consumption for running searchable encryption chaincodes is around 170 MB. It is, therefore, practical for each medical institution to operate a server for running the chaincode and participant of the blockchain network.

**6.3. Scalability.** In this section, we test the scalability of our implemented prototype. We still mainly test two types of chaincodes, i.e., for searchable encryption and ABAC. Since these two parts are crucial to our system, the scalability of these chaincodes can determine the scalability of the entire system. Hence, we assume various scenarios, under which there are different numbers of medical institutions. To check the trend, we simulate 5, 10, 15, and 20 medical institutions. It means that the scales of the blockchain platform are 5, 10, 15, and 20. Then, we increase the medical data accessing rate as system inputs until the chaincode processing rate is getting steady. The procedure is similar to the experiment conducted in Section 6.2. In this way, the capacity of system throughput is achieved.

Figures 7 and 8 show the experimental results of chaincodes for searchable encryption and ABAC, respectively. For both of these two types of chaincodes, the descending rates of their performance are not even linear to the increased number of blockchain participants, i.e., medical institutions. However, with the configurations of our experiments, the system capacity has not decreased much for each type of chaincode when the number of simulated medical institutions increases from 5 to 20 (70 TPS to 60 TPS and 200 TPS to 165 TPS, respectively). In practice, not all the medical institutions construct a single federation to share medical data; the scalability of our system is still feasible. However, for a large-scale federation with many institutions, the system still needs to be further optimized.

## 7. Related Work

The data privacy and security are hot topics in recent years. Some papers consider the issue related with different stages

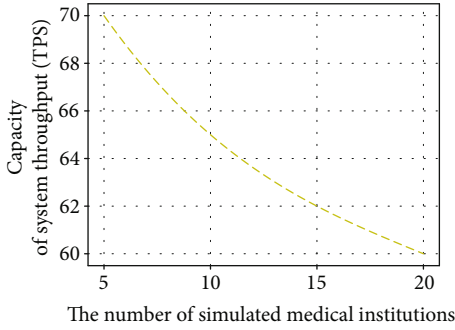


FIGURE 7: The capacity of system throughput varying with simulating different numbers of medical institutions for searchable encryption chaincodes.

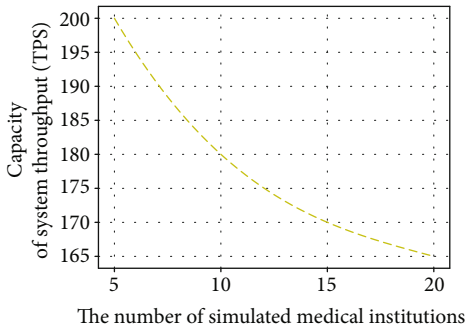


FIGURE 8: The capacity of system throughput varying with simulating different numbers of medical institutions for ABAC chaincodes.

of the data management, including data uploading [14], auditing [15], and sharing [16]. Other papers consider these issues in a special scenario, e.g., in a wireless environment [17]. We focus on the same issue in the field of medical data [18, 19].

Medical data usually includes the types of health reports, medical records, examination results, etc. These types of data not only have great research value but also have privacy preserving requirements. Meanwhile, the integrity of medical data requires assurance. We also need to guarantee that these data are not to be tampered with, destroyed, or deleted by anyone without grants. The accessibility of medical data must be controlled by the patients, but it cannot be modified by the patient. In addition to this, patient data should also be able to be circulated smoothly among medical institutions [20, 21].

**7.1. Medical Data Privacy Preserving Based on Confusion and Anonymity.** The anonymized data or differential privacy was introduced to protect the privacy of medical data [22]. Beaulieu-Jones et al. [23] used a deep neural network that introduced differential privacy to generate artificial data when sharing medical data, which solved the contradiction between data sharing and data privacy to a certain extent. However, in the context of multiple data types, the limitation of this method is that the data would be modified. Cai et al. [24] developed a differential-private framework to preserve the sensitive information for taxi companies when sharing taxi data. Sun et al. [25] proposed a method similar to the above, using differential privacy to process medical data,

training a machine learning model, and publishing the training model instead of directly publishing private data.

**7.2. Privacy Preserving of Medical Data Based on Encryption.** Searchable encryption is usually leveraged in the edge environment for mobile computing [26], through being introduced into data privacy-preserving schemes. For example, Xu et al. [27] leverage a multikeyword searchable encryption technology in medical data sharing to protect data privacy. At the same time, they utilize searchable encryption to achieve the goal of sharing. In the scenario of a body equipment, the body sensor device is leveraged to encrypt the sensor data and upload to the cloud in the stage of collecting the data segment, which is similar to the scenario described by the paper [28]. Meanwhile, the searchable encryption technology is also used to share the data. Besides, this solution only requires little resource consumption, which is suitable for the mobile devices. However, the problem of sensor device credibility should also be considered.

**7.3. Privacy Preserving Based on the Blockchain.** Blockchain is an emerging technology to enhance the trust for the legacy systems, which has been applied in the cloud service level agreement [29], crowdsourcing [30], etc. It is also applied into aspects of data storage with privacy preserving, since the blockchain has storage characteristics of high reliability, high availability, low cost, and strong disaster tolerance. Do and Ng [31] combine searchable encryption and blockchain to ensure that data cannot be tampered with and deleted. It also adopts smart contracts to implement access control and searchable encryption, which constructs the distributed system and solves the trust problem among nodes. Similarly, the consortium blockchain combines searchable encryption [32] that uses agents to achieve searchable encryption. The consortium blockchain stores keywords and ciphertext. To a certain extent, this solution guarantees the privacy-preserving requirements of medical data, which can realize the goal that the distributed medical data cannot be tampered with. In the scheme proposed by Chen et al. [33], medical data is stored on a public cloud and the index of medical data is stored on the blockchain. Data users firstly need to be authorized when they want to obtain data, so that data owners can fully control their own data. However, it is a critical problem that the public cloud is not safe. Tian et al. [34] propose the scheme of SIFF based on the fabric blockchain; SIFF guarantees the granularity of data search. This scheme ensures the privacy, availability, and integrity of medical data. Zhang and Lin [35] propose a medical data sharing architecture combining a private blockchain, which stores full data, and a consortium blockchain, which stores keywords. At the same time, searchable encryption is leveraged to search for keywords. Encrypted medical data is obtained by grants of access control. Likewise, Azaria et al. [11] use blockchain to store medical data and access control is combined with smart contracts. Utilizing blockchain ensures that medical data cannot be tampered with and provides medical data interconnection, interoperability, and data sharing features. MedChain [36] is also a medical data sharing architecture that combines blockchain and P2P networks to tackle

efficiency issues. There are two types of nodes in MedChain; one is a super node, which performs massive calculation and storage, such as large hospitals. The other is an edge node, such as clinics and community hospitals. Although this system is not yet perfect, the scheme of MedChain still improves efficiency, privacy, and security. In addition, MedBlock [37] is also a system that uses blockchain to manage medical data. It adopts a hybrid consensus mechanism, combined with Delegated Proof of Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT), which improves efficiency. It is worth mentioning that the symmetric encryption algorithm and access control are leveraged to improve privacy and security.

## 8. Conclusions

In our proposed work, we have presented a consortium blockchain-based medical data sharing system using K-anonymity, keyword searchable encryption, and ABAC to achieve data privacy-preserving and security among different medical institutions. Firstly, we leverage the K-anonymity technique to preprocess the medical data for blurring the identity information. Secondly, we present a scheme for medical data sharing using searchable encryption on keywords to ensure data security and privacy-preserving. The consortium blockchain is leveraged among different medical institutions to provide the trust layer and host the smart contract. Hence, the consortium blockchain stores the encrypted keywords which are linked to the medical data of medical institutions. The encrypted medical data can then be stored safely on remote clouds. Thirdly, we design and implement attribute-based access control with a smart contract. The blockchain-based ABAC model simplifies the configurations and secures the medical data. Furthermore, we conduct a security analysis of the proposed scheme and protocol and compare them with other related work. The security analysis demonstrates that our scheme can meet the security goals of our original design. Finally, we also implement the scheme on the Hyperledger Fabric platform. Through simulating different medical data accessing rates and different numbers of medical institutions, we evaluate the computational overhead of encryption operations, the performance of implemented chaincodes, and the scalability of our prototype. The experimental studies demonstrate that our scheme and system design are feasible and practical to encourage medical data sharing among medical institutions.

## Data Availability

Data are available using the following: <https://github.com/mythsand/privacy-preserving-medical-data>.

## Disclosure

The initial version of this paper [38] was presented at the conference of “WASA: International Conference on Wireless Algorithms, Systems, and Applications.”

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

The work is supported by the National Key Research and Development Program of China under grant 2018YFB0204301, the National Natural Science Foundation (NSF) under grant 62072306, and Open Fund of Science and Technology on Parallel and Distributed Processing Laboratory under grant 6142110200407.

## References



- [1] M. J. Steinberg and E. R. Rubin, *The HIPAA Privacy Rule: Lacks Patient Benefit, Impedes Research Growth*, Association of Academic Health Centers, 2009.
- [2] P. Samarati and L. Sweeney, *Protecting Privacy when Disclosing Information: K-Anonymity and Its Enforcement through Generalization and Suppression*, Electronic Privacy Information Center, 1998.
- [3] C. Dwork, “Differential privacy: a survey of results,” in *Theory and Applications of Models of Computation. TAMC 2008*, pp. 1–19, Springer, 2008.
- [4] J. Soria-Comas, J. Domingo-Ferrer, D. Sánchez, and S. Martínez, “Enhancing data utility in differential privacy via microaggregation-based k-anonymity,” *The VLDB Journal*, vol. 23, no. 5, pp. 771–794, 2014.
- [5] Y. Wu, J. Su, and B. Li, “Keyword search over shared cloud data without secure channel or authority,” in *2015 IEEE 8th International Conference on Cloud Computing*, pp. 580–587, New York, NY, USA, 2015.
- [6] E. Shi, J. Bethencourt, T. H. H. Chan, D. Song, and A. Perrig, “Multi-dimensional range query over encrypted data,” in *2007 IEEE Symposium on Security and Privacy (SP’07)*, pp. 350–364, Berkeley, CA, USA, 2007.
- [7] K. LeFevre, D. J. DeWitt, and R. Ramakrishnan, “Mondrian multidimensional k-anonymity,” *ICDE*, vol. 6, p. 25, 2006.
- [8] J. H. Friedman, J. L. Bentley, and R. A. Finkel, “An algorithm for finding best matches in logarithmic Expected time,” *ACM Transactions on Mathematical Software*, vol. 3, no. 3, pp. 209–226, 1977.
- [9] J. Liu, X. Huang, and J. K. Liu, “Secure sharing of personal health records in cloud computing: ciphertext-policy attribute-based signcryption,” *Future Generation Computer Systems*, vol. 52, pp. 67–76, 2015.
- [10] X. Wang, A. Zhang, X. Xie, and X. Ye, “Secure-aware and privacy-preserving electronic health record searching in cloud environment,” *International Journal of Communication Systems*, vol. 32, no. 8, article e3925, 2019.
- [11] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “Medrec: using blockchain for medical data access and permission management,” in *2016 2nd International Conference on Open and Big Data (OBD)*, pp. 25–30, Vienna, Austria, 2016.
- [12] H. Zhou, Y. Hu, X. Ouyang et al., “CloudsStorm: a framework for seamlessly programming and controlling virtual infrastructure functions during the DevOps lifecycle of cloud applications,” *Software: Practice and Experience*, vol. 49, no. 10, pp. 1421–1447, 2019.

- [13] I. Baldine, Y. Xin, A. Mandal, P. Ruth, C. Heerman, and J. Chase, "Exogeni: a multi-domain infrastructure-as-a-service testbed," in *Testbeds and Research Infrastructure. Development of Networks and Communities*, pp. 97–113, Springer, 2012.
- [14] Z. Cai and Z. Xu, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.
- [15] T. Wang, Y. Mei, X. Liu, J. Wang, H.-N. Dai, and Z. Wang, "Edge-based auditing method for data security in resource-constrained internet of things," *Journal of Systems Architecture*, vol. 114, p. 101971, 2021.
- [16] Z. Xu and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial iots," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.
- [17] X. Liu, M. S. Obaidat, C. Lin, T. Wang, and A. Liu, "Movement-based solutions to energy limitation in wireless sensor networks: state of the art and future trends," *IEEE Network*, vol. 35, no. 2, pp. 188–193, 2021.
- [18] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, "Privacy preservation in wireless sensor networks: a state-of-the-art survey," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1501–1514, 2009.
- [19] A. Ukil, "Privacy preserving data aggregation in wireless sensor networks," in *2010 6th International Conference on Wireless and Mobile Communications*, pp. 435–440, Valencia, Spain, 2010.
- [20] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in *Security and Privacy in Communication Networks. SecureComm 2010*, pp. 89–106, Springer, 2010.
- [21] D. K. Mandl, P. Szolovits, and S. I. Kohane, "Public standards and patients' control: how to keep electronic medical records accessible but private," *BMJ*, vol. 322, no. 7281, pp. 283–287, 2001.
- [22] M. Moussa and S. A. Demurjian, "Differential privacy approach for big data privacy in healthcare," in *Privacy and Security Policies in Big Data*, pp. 191–213, IGI Global, 2017.
- [23] B. K. Beaulieu-Jones, Z. S. Wu, C. Williams et al., "Privacy-preserving generative deep neural networks support clinical data sharing," *Circulation: Cardiovascular Quality and Outcomes*, vol. 12, no. 7, p. e005122, 2019.
- [24] Z. Cai, X. Zheng, and J. Yu, "A differential-private framework for urban traffic flows estimation via taxi companies," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6492–6499, 2019.
- [25] Z. Sun, Y. Wang, M. Shu, R. Liu, and H. Zhao, "Differential privacy for data and model publishing of medical data," *IEEE Access*, vol. 7, pp. 152103–152114, 2019.
- [26] Y. Guo, F. Liu, Z. Cai, N. Xiao, and Z. Zhao, "Edge-based efficient search over encrypted data mobile cloud storage," *Sensors*, vol. 18, no. 4, p. 1189, 2018.
- [27] C. Xu, N. Wang, L. Zhu, K. Sharif, and C. Zhang, "Achieving searchable and privacy-preserving data sharing for cloud-assisted e-healthcare system," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8345–8356, 2019.
- [28] F. Altaf, M. Aditia, E. Saini, B. Rakshit, and S. Maity, "Privacy preserving lightweight searchable encryption for cloud assisted e-health system," in *2019 International Conference on Wireless Communications Signal Processing and Networking (WiSP-NET)*, pp. 310–314, Chennai, India, 2019.
- [29] H. Zhou, X. Ouyang, Z. Ren, J. Su, C. de Laat, and Z. Zhao, "A blockchain based witness model for trustworthy cloud service level agreement enforcement," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, pp. 1567–1575, Paris, France, 2019.
- [30] S. Zhu, Z. Cai, H. Hu, Y. Li, and W. Li, "zkcrowd: a hybrid blockchain-based crowdsourcing platform," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4196–4205, 2019.
- [31] H. G. Do and W. K. Ng, "Blockchain-based system for secure data storage with private keyword search," in *2017 IEEE World Congress on Services (SERVICES)*, pp. 90–93, Honolulu, HI, USA, 2017.
- [32] Y. Wang, A. Zhang, P. Zhang, and H. Wang, "Cloud-assisted ehr sharing with security and privacy preservation via consortium blockchain," *IEEE Access*, vol. 7, pp. 136704–136719, 2019.
- [33] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Generation Computer Systems*, vol. 95, pp. 420–429, 2019.
- [34] H. Tian, J. He, and Y. Ding, "Medical data management on blockchain with privacy," *Journal of Medical Systems*, vol. 43, no. 2, p. 26, 2019.
- [35] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *Journal of Medical Systems*, vol. 42, no. 8, p. 140, 2018.
- [36] B. Shen, J. Guo, and Y. Yang, "Medchain: efficient healthcare data sharing via blockchain," *Applied Sciences*, vol. 9, no. 6, p. 1207, 2019.
- [37] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "Medblock: efficient and secure medical data sharing via blockchain," *Journal of Medical Systems*, vol. 42, no. 8, p. 136, 2018.
- [38] L. Meng, X. Hong, Y. Chen, Y. Ding, and C. Zhang, "K-anonymous privacy preserving scheme based on bilinear pairings over medical data," in *Wireless Algorithms, Systems, and Applications, WASA 2020*, pp. 381–393, Springer, 2020.



## Research Article

# AI-Driven Multiobjective Scheduling Algorithm of Flood Control Materials Based on Pareto Artificial Bee Colony

**Banteng Liu** <sup>1</sup>, **Junjie Lu**,<sup>2</sup> **Yourong Chen**,<sup>1</sup> **Ping Sun**,<sup>1</sup> **Kehua Zhao**,<sup>1</sup> **Meng Han** <sup>3</sup>,  
**Rengong Zhang**,<sup>4</sup> and **Zegao Yin**<sup>5</sup>

<sup>1</sup>College of Information Science and Technology, Zhejiang Shuren University, Hangzhou, Zhejiang 310015, China

<sup>2</sup>School of Computer Science and Artificial Intelligence, Changzhou University, Changzhou, Jiangsu 213164, China

<sup>3</sup>Data-Driven Intelligence Research (DIR) Lab, Kennesaw State University, Marietta, GA 30060, USA

<sup>4</sup>Zhejiang Yugong Information Technology Limited Company, Hangzhou, Zhejiang 310051, China

<sup>5</sup>College of Engineering, Ocean University of China, Qingdao, Shandong 266100, China

Correspondence should be addressed to Meng Han; [mhan9@kennesaw.edu](mailto:mhan9@kennesaw.edu)

Received 6 January 2021; Accepted 5 June 2021; Published 22 June 2021

Academic Editor: Carles Gomez

Copyright © 2021 Banteng Liu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Considering the competition between rescue points, we use artificial intelligence (AI) driven Internet of Thing (IoT) and regional material storage data to propose a multiobjective scheduling algorithm of flood control materials based on Pareto artificial bee colony (MSA\_PABC). To address the scheduling of flood control materials, the multiple types of flood control materials, the multiple disaster sites, and entertain both emergency and fairness of rescue need to be considered comprehensively. The MSA\_PABC has the constraints such as storage quantity constraint of warehouse materials, material demand constraint, and maximum transportation distance of flood control materials. We establish the scheduling optimization model of flood control materials for each disaster rescue point and the total scheduling optimization model for all flood control materials. Then, MSA\_PABC uses the modified Pareto artificial bee colony algorithm to solve the multiobjective models. Three types of initialization strategies are proposed to calculate the fitness of each rescue point and the overall evaluation value of the food source. We propose the employ bee operations such as niche technology and local search of the variable neighborhood, the onlooker bee operations such as Pareto nondominated sorting and crossover operation, the scout bee operations such as maximum evolutionary threshold, and end elimination mechanism. Finally, our proposed solution obtains the nondominated solution set and its optimal solution. The experimental results show that no matter how the number of rescue points changes, MSA\_PABC can find the nondominated solution set and optimal solution quickly. It improves the convergence rate of MSA\_PABC and material satisfaction rate. Our solution also reduces the average maximum transportation distance, the standard deviation of maximum transportation distance, and the standard deviation of material satisfaction rate. The evaluation also demonstrates MSA\_PABC outperforms the state-of-arts such as ABC (artificial bee colony), NSGA2 (nondominated sorting genetic algorithm 2), and MOPSO (multiobjective particle swarm optimization).

## 1. Introduction

China has a vast territory, and the precipitation partially concentrates. The precipitations time and space distribution are uneven, and it does not match the distribution of population and cultivated land. Therefore, disasters such as floods and typhoons occur frequently, causing a large number of people to suffer disasters and huge economic losses [1]. For instance, in 2019, 130 million people are suffered from disasters such

as typhoons. The direct economic losses were 327.09 billion RMB [2]. Zhejiang Province locates on the southeastern coast of China. Due to its special geographic location and climatic conditions, it is susceptible to typhoons and storms. However, the drainage capacity of Zhejiang Province is limited. Once the flood disasters occur, it will cause serious economic and loss of life to people. Therefore, flood prevention and rescue are particularly important [3]. In the past, rescue dispatching mainly issued dispatching instructions by means



of communication. The problem lies in low efficiency and chaotic command. Once the scale of rescue dispatching rises, its order and efficiency will be more difficult to maintain.

With the rapid development of computer technology, sensor technology, and Internet of Things technology, various industries in the market are developing in the direction of high automation and intelligence and hope to improve the service ability of the industry through AI and IOT technology [4, 5]. The future development of flood control and disaster reduction in the direction of intelligence is gradually becoming a consensus in the industry. Internet of Things technology as a basic support means to determine the quantity and availability of materials through a variety of information sensing equipment and electronic tags in the field of flood control, and upload the relevant information to the Internet platform for information interaction to achieve intelligent management of materials. At the same time, it provides data support for the subsequent solution of large-scale orderly and efficient scheduling of materials. The dynamic scheduling problem of rescue materials is NP hard in nature. It is usually solved with various artificial intelligence algorithms based on the existing Internet of Things technology [6, 7].

At present, some scholars have achieved certain results in emergency dispatch, but the characteristics of flood control and rescue scheduling determine that the applicability of artificial intelligence algorithm needs to be analyzed objectively to ensure that the application has a certain quality of service. For instance, Song et al. [8] propose a double mutation improved differential evolution algorithm with the Pareto concept and establish a multisupply point to multirescue point emergency material scheduling model in the case of limited resources to minimize the total cost of distribution expenses and the largest missing loss. Tian et al. [9] take the urgency of different needs into consideration and establish a multiobjective mathematical model for dynamic distribution scheduling. Then, they use a weighted particle swarm optimization algorithm with swarm intelligence to solve the model. However, the above algorithms are more likely to fall into local optimum with the increase of scheduling scale, which makes the reliability of rescue decline. Zhang et al. [10] propose a hybrid intelligent search algorithm based on two-dimensional NSGA-II and ant colony optimization to establish a multiobjective optimization model for concurrent allocation and scheduling of multiple emergency rescue materials. Some scholars [11–14] focus on establishing a material scheduling optimization model which considers multiple parameters and using genetic algorithms (GA), sequential linear programming algorithms (SLP), greedy algorithms, and other algorithms to solve the optimization model and obtain the optimal solution. However, the above algorithms do not consider the dynamic change of material demand in the rescue process to make the material scheduling lag behind.

Some scholars [15–18] focus on establishing multiple target optimization models, such as minimizing the transportation time of materials and maximizing reliability. Then, they use single or multiple hybrid algorithms, such as quick sorting genetic algorithm, harmony algorithm, artificial bee col-

ony algorithm, Monte Carlo algorithm, and stepwise method, to obtain the optimal scheduling schemes. Considering the processing time of emergencies, Wex et al. [19] propose a decision support model for allocating existing rescue units to emergency action centers to improve the efficiency of incident handling and reduce casualties and economic losses in the reaction phase. Considering that the emergency supplies provided to rescue points may be insufficient or excessive, Chen et al. [20] take the minimization of the loss caused by insufficient material distribution and oversupply and the minimization of vehicle scheduling costs as optimization objectives and propose a vehicle scheduling optimization model of disaster emergency logistics based on discrete bee colony. In [8–20], they use intelligent optimization algorithms to solve emergency rescue scheduling problems but do not take account of the urgency and fairness of multiobjective rescue scheduling at the same time, only meet the rescue service requirements of individual rescue points, which makes the overall rescue service quality poor, and only focus on resource allocation, without considering the unexpected factors that affect the service quality such as road damage in the rescue process.

Therefore, based on the algorithms mentioned above, we propose a multiobjective scheduling algorithm of flood control materials based on Pareto artificial bee colony (MSA\_PABC). Considering the convergence performance of the algorithm, the feasibility of the actual road transportation in the process of material allocation, and the satisfaction of the allocation between rescue points and the whole rescue, we establish the optimization model of flood control material scheduling for each disaster relief point and the optimization model of all flood control materials scheduling from the time cost, task execution reliability, and service satisfaction. According to the importance and easy measurement of service quality parameters, we select service quality parameters and establish a parameter system including four service quality parameters (transportation efficiency, satisfaction rate of disaster site, transportation reliability, and actual availability of material reserve), which is used as constraint function to guide the optimization objective of an artificial intelligence scheduling algorithm, that is, we propose the modified Pareto artificial bee colony algorithm to solve the multiobjective optimization model. In the initial phase, we propose a variety of food source initialization strategies and calculate the fitness of each rescue point and the overall evaluation value of the food source. In the employed bee phase, we use niche technology and variable neighborhood local search and other employ bee operations to strengthen the local search of the food source. In the onlooker bee phase, we use Pareto dominate sorting, crossover operation, and other onlooker operations to expand the search capabilities of high-quality food sources in areas with small distribution densities in the multidimensional solution space. In the scout bee phase, we use the maximum evolution threshold and end-elimination mechanism to continuously update old food sources to ensure the diversity of solutions. Finally, MSA\_PABC can quickly find nondominated sets and optimal solutions, thereby improving the convergence rate and material satisfaction rate and reducing the average maximum transport

distance, standard deviation of the maximum transport distance, and standard deviation of material satisfaction rate for flood control materials to achieve the overall optimal rescue service quality with practical feasibility.

## 2. Scheduling Model Establishment

The flood control emergency scheduling is a prerequisite for realizing rapid and accurate handling of dangerous situations. Therefore, it is necessary to take the actual storage of warehouse materials and situations of disasters of each region as influencing factors. According to flood control materials constraints of storage capacity, demand, and transportation, we establish the scheduling optimization model of flood control materials for each disaster rescue point and the total scheduling optimization model of all flood control materials. The details are as follows:

We set  $H_i^k$  to represent the storage capacity of flood control material  $k$  in warehouse  $i$ . Considering the number of flood control material  $k$  allocated by the storage warehouse  $i$  to all rescue points does not exceed the total storage of flood control materials  $k$  in the storage warehouse  $i$ , the storage capacity constrain of warehouse materials is

$$\sum_j W_{ij}^k \leq H_i^k, \forall i, k, \quad (1)$$

where  $W_{ij}^k$  represents the number of flood control material  $k$  allocated by warehouse  $i$  to rescue point  $j$ .

To avoid wastage and use the flood control materials effectively, it is required that the number of flood control material  $k$  from all warehouses to rescue point  $j$  does not exceed the required quantity of the flood control material  $k$  in the rescue point  $j$ . Thus, the material demand constraint is

$$\sum_i W_{ij}^k \leq J_j^k, \forall j, k, \quad (2)$$

where  $J_j^k$  represents the required quantity of the flood control material  $k$  in the rescue point  $j$ .

According to the value  $W_{ij}^k$ , we can know the storage warehouses and rescue points that need to be passed during flood control materials transportation. We assume that the transport capacity is adequate during the transportation of flood control materials. Then, according to the GIS system and the distribution of flood disasters, we determine the shortest transportation distance  $P_{ij}^k$  of the flood control material  $k$  between the storage warehouse  $i$  and the rescue point  $j$  that can avoid flooding inundated roads [21]. Thus, we can obtain the maximum transportation distance for finishing the flood control material scheduling at rescue point  $j$ .

$$D_j = \max (P_{ij}^k, \forall i, k), \quad (3)$$

where  $D_j$  represents the maximum distance required to finish the transportation of flood control materials at rescue point  $j$ .

To meet the demand for rescue points for flood control materials, the material satisfaction rate of rescue point  $j$  is

$$R_j = \frac{\sum_k \sum_i W_{ij}^k}{\sum_k J_j^k}, \quad (4)$$

where  $R_j$  represents the material satisfaction rate of rescue point  $j$ .

In the aspect of disaster rescue points, each of them hopes that the required flood control materials can meet the fastest transportation time and the maximum satisfaction rate. We establish a scheduling optimization model of flood control materials for each disaster rescue point  $j$ .

$$\begin{aligned} & \min (D_j/R_j) \\ & \text{s.t. } \sum_i W_{ij}^k \leq J_j^k, \forall k \\ & \text{Formulas(1), (3), (4)} \\ & W_{ij}^k \geq 0, \forall i, k \end{aligned} \quad (5)$$

In the aspect of flood control material scheduling management, the flood control materials can weigh the principle of urgency and fairness. Therefore, we set the standard deviation of the maximum transportation distance of flood control materials is

$$\text{Std}_w = \sqrt{\sum_j \left( D_j - \sum_j D_j/N_j \right)^2 / N_j}, \quad (6)$$

where  $\text{Std}_w$  represents the standard deviation of the maximum transportation distances of flood control materials and  $N_j$  represents the number of rescue points. The standard deviation of the satisfaction rate of flood control materials is

$$\text{Rat}_w = \sum_j \sqrt{\left( R_j - \sum_j R_j/N_j \right)^2 / (N_j)}, \quad (7)$$

where  $\text{Rat}_w$  represents the standard deviation of the satisfaction rate of flood control materials. Considering the emergency of flood control materials, it is required to send all flood control materials to all rescue points as quickly and as fully as possible. And in terms of the fairness of flood control materials, it is required that the maximum transportation distance and satisfaction rate between rescue points are not much different. The standard deviation of maximum transportation distances and the standard deviation of material satisfaction rates need to be minimized. Therefore, we establish the total scheduling optimization model of all flood control materials.

$$\begin{aligned}
& \min (D_{ave} \times (x_1 \text{Std}_w + x_2 \text{Rat}_w) / R_{ave}) \\
& \text{s.t. Formulas(1) - (4)} \\
& D_{ave} = \sum_j D_j / N_j, \\
& R_{ave} = \sum_j R_j / N_j \\
& W_{ij}^k \geq 0, \forall i, j, k
\end{aligned} \tag{8}$$

where  $D_{ave}$  represents the maximum average distance required to finish flood control materials transportation,  $R_{ave}$  represents the average material satisfaction rate of rescue points,  $x_1$  represents the distance factor,  $x_2$  represents the satisfaction rate factor, and  $x_1 + x_2 = 1$ .

### 3. Scheduling Model Establishment

Since the models (5) and (8) consider the selection of three elements, such as the storage warehouse, rescue point, and flood control material, the optimization model is complicated and involves a lot of calculations. Therefore, we use artificial intelligence to solve the optimization models (5) and (8) and obtain the optimal plan by constantly searching for the distribution scheme of reserve warehouses, rescue points, and flood control materials. The inspiration of the artificial bee colony algorithm (ABC) proposed by Karaboga et al. [22] is based on bee foraging behavior. In ABC, the artificial bee colony comprises three kinds of bees, such as employed bees, onlooker bees, and scout bees. The employed bees are associated with a specific food source. The onlooker bees observe the dance of employed bees in the hive to decide to choose a certain food source and conduct a local search for the selected food source. The scout bees randomly search for food to avoid local optimal solutions. The traditional ABC algorithm can effectively solve the optimization problem of a single objective function. It has the characteristics of a few parameters and fast convergence speed. However, according to the model (5), there are multiple rescue points. Each rescue point needs to make its optimization model as optimal as possible. The problem of flood control material scheduling optimization is a multiobjective optimization problem in which multiple rescue points compete with each other. Therefore, we introduce the Pareto nondominated sorting and propose a multiobjective scheduling algorithm of flood control materials based on Pareto artificial bee colony to solve the scheduling problem of flood control materials between rescue points. Then, we can obtain the nondominated sets and find the optimal solution in the nondominated set based on the model (5). Thus, we obtain the flood control material scheduling schemes that weigh disaster rescue points and flood control scheduling management in the case of multiple types of flood control materials and multiple disaster rescue points.

**3.1. Food Source Initialization.** Since the traditional ABC algorithm cannot be directly used to solve the scheduling problem, we precode the problem solution and uses a one-

dimensional vector coding method with variable length to solve the flood control material scheduling decision problem. The food source code is shown in Figure 1.

Where the storage warehouse represents the storage location of flood control materials in various regions, according to the location of the rescue points and the demands of flood control materials in advance, the algorithm needs to select the storage warehouse set that can meet the flood control materials all rescue points.  $a1$  represents the storage warehouse number 1.  $b1$  represents the rescue point number 1. The numbers in the table represent the amount of certain flood control materials transported. A good initial solution set can enable the algorithm to quickly find the areas with great potential in the entire solution space and speed up the algorithm's convergence. Then, it provides a variety of different types of food sources to avoid the algorithm from falling into a local optimum [23]. In the paper, we use the following three rules in the food source initialization phase.

- (1) *Large Storage Warehouse First.* Due to the different types of flood control materials stored in each storage warehouse, each flood control material is also different. According to the actual material storage quantity of the warehouse, flood control materials are distributed based on roulette rules in the same set. The warehouse with a large storage quantity can be a priority to assign scheduling tasks [24]
- (2) *Disaster Demand First.* Different rescue points have different demands for flood control materials. In the same set, according to the demand for flood control materials at each rescue point, flood control materials are preferentially distributed based on roulette rules to rescue points with high demand for materials
- (3) *Random Distribution.* Flood control materials are distributed randomly

The three rules mentioned above generate each initial solution. The solution set ratios are, respectively, set to 30%, 30%, and 40%. In the distribution process, each initial allocation value is the minimum of the warehouse material storage and material demand [25] to meet the constraint (1). Then, the food source is considered whether meets the constraint (2); if the constraint (2) is not met, the overallocated materials are reduced to avoid repeated scheduling for materials. The food sources that met the constraints (1)–(2) are obtained.

**3.2. Fitness Value Calculation.** For urgency and fairness of flood control materials' emergency scheduling, we establish a scheduling optimization model of flood control materials. In the phases of employed bees and onlooker bees, we need to calculate the fitness  $F_j$  of each rescue point and perform the operations such as niche and minimum dominating set selection, which is

$$F_j = \frac{1}{(D_j/R_j)}. \tag{9}$$

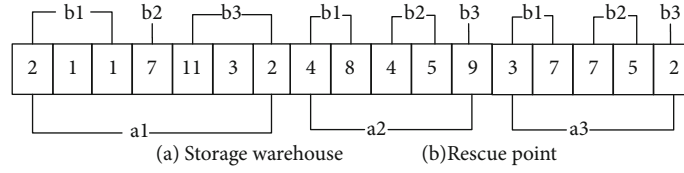


FIGURE 1: Example of one-dimensional encoding of food source.

When the algorithm is solved, according to the minimum dominating set, we obtained, calculating the overall evaluation value  $F_z$  of all food sources in its set, and select the food source with the maximum value as the optimal solution of MSA\_PABC.

$$F_z = D_{ave} \times \frac{x_1 \text{Std}_w + x_2 \text{Rat}_w}{R_{ave}}. \quad (10)$$

**3.3. Employed Bee Phase.** According to the food sources generated in Section 3.1, employed bees divide the whole food source into subcategories according to the number of rescue points. After that, employed bees search for the unknown solution space near each food source by variable neighborhood local search operation to obtain multiple child food sources. Then, we analyze the relationship between the child's food source and the father's food source and obtain the next food source. Finally, we use the elite retention and exclusion strategy in the niche to restore the food source's size to the original size. The niche operation and variable neighborhood local search operation are as follows.

**3.3.1. Niche Operation.** Niche is a conception of biology. It refers to a living environment under a specific environment. In the biological evolution process, organisms always live with the same species and breed offspring together. Niche technology divides each generation of individuals into several categories and selects some individuals with greater fitness as an outstanding representative class to form a species, then uses the elite retention and exclusion strategy in the species and between different species to generate a new generation of individual groups.

For individual fitness value  $F_j$  mentioned in Section 3.2, MSA\_PABC calculates the fitness value  $F_j$  for each food source and normalizes it. It classifies the food source into the subclass population with the highest fitness value  $F_j$  after normalization and divides the entire food source population into subcategories. For the maximum fitness value  $[F_j$  within its child species, MSA\_PABC performs the variable neighborhood search operation to enhance algorithm's the local optimization algorithm and obtains multiple new food sources. If the new food source dominates the old food source, the old food source is updated. Otherwise, if the old food source dominates the new food source, it deletes the new food source and keeps the old food sources. Then, it places the new food sources in the temporary food source set. After finishing the variable neighborhood search operation, MSA\_PABC merges the food source set and the temporary food source set into the next generation of species.

At last, MSA\_PABC calculates the number of food sources in the next generation. Suppose the number of food sources exceeds the initial size. In that case, it randomly selects multiple food sources in the population to form an exclusion member set. It calculates the similarity between other food sources and exclusion members in the next generation. It selects the current food source and calculates the number of the same value at each same code position of each exclusion committee. It chooses the maximum value as the same degree  $A_i$  of the food and calculates the difference sum of the values at the same code position of the food source. Then, it selects the maximum value as the difference degree  $B_i$  of the food source. According to the same degree, MSA\_PABC sorts those food sources from small to large. If there are multiple food sources with the same degree, it sorts those food sources from small to large according to the different degree and obtains the sorted food sources. Then, it eliminates front foods in turn until the population returns to its original size. If the eliminated food source is the optimal local solution or the optimal global solution in the offspring population, it skips the food source and reserves the elite solution.

**3.3.2. Variable Neighborhood Local Search Operation.** A variable neighborhood local search method is an improved local search method. It utilizes a neighborhood structure formed by different actions to perform an alternate search and achieves a good balance between concentration and evacuation. The maximum loop search threshold is set as the termination condition to keep the efficiency and the accuracy of the algorithm. To facilitate the search operation of variable neighborhood, the initial food source has to be transformed into a multidimensional real matrix  $Q_{ijv}$ . As shown in Figure 2, where  $i$  represents the storage warehouse (row  $a$ ),  $j$  represents the rescue point (subordinate columns  $b$ ).  $v$  represents the type of flood control material.  $Q$  represents the quantity of flood control materials (the value in Figure 2). Suppose some storage warehouses do not have a certain amount of flood control materials. In that case, the  $Q$  value is the Nan identifier; then, MSA\_PABC skips the  $N_{an}$  identifier automatically during the calculation to improve search efficiency. The Niche strategy divides the food sources into classes based on the number of rescue points (i.e.,  $b_1, b_2, b_3, \dots, b_n$ ). For rescue point  $b_i$  among food sources belonging to the  $b_i$  category, it performs the variable neighborhood search to improve the resource scheduling optimization of the rescue point and the mutual competitiveness between the rescue points. Thus, it obtains some local optimal food sources. As shown in Figure 2, we assume that it belongs to the  $b_1$  category. Then, MSA\_PABC conducts a variable neighborhood search for the flood control material



	(a): Storage warehouse			(b): Rescue point				
	b1			b2		b3		
a1	2	1	1	7	Nan	11	3	2
a2	4	8	Nan	4	5	Nan	9	Nan
a3	3	7	Nan	7	5	Nan	2	Nan

FIGURE 2: Example of multidimensional coding in b1 category of food sources.

distribution at the rescue point  $b_1$ . The specific steps of the variable neighborhood search method are described as follows.

$$Q_{iuv} = Q_{ijv} + Q_{iuv}, Q_{ijv} = 0, \forall i, \quad (11)$$

where  $Q_{ijv}$  represents quantity  $Q_{ijv}$  of flood control material  $v$  from each storage warehouse to the rescue point  $b_j$  which redistributes them to the rescue point  $b_w$ .

*Step 1.* According to the  $b_w$  category to which the food source belongs, the method determines the rescue point  $b_w$  that needs to be searched by the variable neighborhood search operation. Then, it initializes the maximum number of variable neighborhood searches and selects the first column of flood control materials in rescue point  $b_w$ . The number of neighborhood searches is 0.

*Step 2.* Getting current flood control material  $v$ , the method searches for other rescue points with the flood control materials and selects a rescue point  $b_j$  randomly.

*Step 3.* The method finds the quantity  $Q_{ijv}$  of flood control material  $v$  from each storage warehouse to the rescue point  $b_j$  and redistributes them to the rescue point  $b_w$ . The specific formula is as follows:

If  $\sum_i Q_{iuv} > J_j^v$ , the current quantity of flood control materials  $v$  which are allocated to rescue point  $j$  is too large, and the excessive flood control materials have to return to rescue point  $b_j$ . In order to reduce the transportation distance of flood control materials, we set  $L = \sum_i Q_{iuv} - J_j^v$ .

*Step 4.* The method selects a nonzero value randomly among  $Q_{iuv}, \forall i$ . If  $Q_{cuv} \geq L$ , then  $Q_{cuv} = Q_{cuv} - L, Q_{cju} = Q_{cju} + L$  and skip to step 5. Otherwise,  $Q_{cuv} = 0, Q_{cju} = Q_{cuv}, L = L - Q_{cju}$  and return to step 4.

*Step 5.* If the method has completed the search for variable neighborhoods of all flood control materials in the rescue point  $b_j$ , it skips stepping 6. Otherwise, it selects the next flood control material and skips to step 2.

*Step 6.* If the method obtains a child food source and the number of variable neighborhood searches is smaller than the maximum number of variable neighborhood searches, it

reselects the first column of flood control materials in the rescue point  $b_w$ ; then, the number of variable neighborhood searches adds 1 and skips to step 2. Otherwise, it ends and outputs multiple new food sources.

As shown in Figure 2, we assume that the demands of sandstone  $b_1$  are 20, and the demands of sandstone  $b_3$  are 30. Then,  $v = 1$  and it only represents the sandstone. There is no sandstone in  $b_2$ , and  $b_3$  has sandstone; thus,  $Q_{011} = [2, 4, 3]$ . The subscript 0 represents all of the storage warehouses  $a_1, a_2$ , and  $a_3$ . We randomly select the value of sandstone material  $b_3$  as  $Q_{032} = [2, 9, 12]$ . First, we set  $Q_{111} = 2 + 3 = 5, Q_{211} = 4 + 9 = 13$ , and  $Q_{311} = 3 + 2 = 5$ . Due to the current number of sandstone in  $b_1$  exceeds its demands, it does not meet the constraints (1) and (2). Then, we randomly select the storage warehouse and return the remaining value to the rescue point  $b_3$ . Finally, we operate on each flood control material in  $b_1$ , so as to realize variable neighborhood search operation and output new food sources.

*3.4. Onlooker Bees Phase.* MSA\_PABC calculates the fitness value  $F_j(i)$  of each rescue point for every food source by formula (9) and obtains a  $N_s \times N_j$  data matrix  $M$ . Among them,  $F_j(i)$  represents the fitness value of rescue point  $j$  in food source  $i$ .  $N_s$  represents the number of food sources.  $N_j$  represents the number of rescue points. According to each rescue point's fitness value, it sorts each column of data in the matrix  $M$  to obtain the neighbor individuals  $i + 1$  and  $i - 1$  of each element in the matrix  $M$  and their fitness values. Then, it calculates the crowdedness through the Euclidean distance value between individual  $i + 1$  and individual  $i - 1$ . That is, it calculates the sum of the differences in the individual fitness value  $F_j$  for each target. The solution with the maximum and minimum values is specified as the infinite distance, that is, the boundary solution  $d_1 = d_y = \text{infinity}$ .

$$d_i = \begin{cases} \infty, & \forall i = 1 \text{ and } y \\ \sum_{j=1}^{N_j} \frac{|F_j(i+1) - F_j(i-1)|}{F_j^{\max} - F_j^{\min}}, & 1 < i < y \end{cases}, \quad (12)$$

where  $d_i$  represents the crowdedness of the  $i$ th food source,  $y$  represents the maximum boundary index,  $F_j^{\max}$  represents the maximum fitness value of rescue point  $j$  among all food sources, and  $F_j^{\min}$  represents the minimum fitness value of rescue point  $j$  among all food sources. In the solution set, the part of solutions concentrates in a certain area and distributes sparsely in some areas; therefore, according to the crowdedness of food sources, MSA\_PABC sorts the solutions in descending order to obtain the spatial measure of food sources with surrounding neighbors. The selected probability of the food source is calculated by the formula (13).

$$P_i^{\text{con}} = \begin{cases} \frac{d_i}{\sum_{i=1}^y d_i}, & \forall d_i \neq \infty \\ 0, & d_i = \infty \end{cases}, \quad (13)$$



where  $P_i^{\text{con}}$  represents the selected probability of the  $i$ th food source in the solution set. According to the measurement results, the crossover operation is performed on the entire population, the search space is expanded, and the number of solutions at each dominating level and the Pareto curve are increased to provide more choices for decision-making. Namely, MSA\_PABC sets the crossover probability  $r$  in advance and cyclically implements the following operations until finishing the crossover of each type of flood control materials: in the range  $[0,1]$ , it randomly generates a floating-point number  $r1$ . If  $r1 < r$ , it will cross the  $k$ th element of the two selected food sources. Otherwise, it does not change the amount of flood control materials in the food source. After finishing the cross operation, it is necessary to verify whether the newly generated food sources satisfy the constraints (1) and (2). If it does not, the overallocated materials will be cut to obtain the new food sources which meet the constraints. Then, new food sources add to contemporary populations.

MSA\_PABC implements the retain Pareto nondominated strategy by formula (12), that is, it compares the fitness value of each rescue point of any two food sources. If the fitness value of each rescue point in one food source is greater than or equal to the fitness value of each rescue point in another food source, and there is at least the fitness value of one rescue point greater than the fitness value of the corresponding rescue point in another food source, it represents that the food source dominates another food source. Therefore, it can obtain a set of nondominated solution sets  $M_F$  that are not dominated by other solutions.

$$F_j(\kappa) \geq F_j(\lambda), \text{ and } \exists F_\varepsilon(\kappa) > F_\varepsilon(\lambda), j = 1, \dots, \varepsilon \dots, N_j, \quad (14)$$

where  $\kappa$  and  $\lambda$  represent the two food sources in the entire set of solution spaces and  $F_j(\cdot)$  represents the fitness value of the  $j$ th rescue point of the food source. If the number of food sources in the solution set exceeds the initial scale, it sorts the food sources in the population in descending order by the overall evaluation value  $F_z$  and eliminates the poor food source solutions to restore the population to its original scale. Otherwise, it will add the initialized food sources to bring it back to the original scale.

**3.5. Scout Bee Phase.** After completing the above two phases, scout bees select the food source in the last certain proportion of the food source population and implement the initialize operation in Section 3.1 for the same number of times to initialize the food source. Then, it adopts the greedy strategy to update old food sources. Because the entire food source population may have food sources with the same fitness value, it chooses the duplicate and redundant food source and the food source whose fitness value does not change after the maximum number  $U$  of evolution iterations. Then, it uses the food source initialization operation in Section 3.1 to initialize the food source to ensure the diversity of the entire population and prevent it from falling into a local optimum.

## 4. Algorithm Implementation

As shown in Figure 3, we mainly use the MSA\_PABC to solve the model. In the initialization phase of the algorithm, it is necessary to set the model's data and the initial parameters of the algorithm. The specific steps are as follows:

*Step 1.* MSA\_PABC obtains each warehouse point  $a$  and rescue point  $b$  in the city and obtains the number of types of materials and the number of specific materials in each warehouse. Then, it sets the initial data, such as the total number of food sources in the population, the maximum number of evolution  $U$ , the maximum number of local searches  $m1$  in the variable neighborhood, and the number of onlooker bees  $m2$ .

*Step 2.* According to the principle of large-scale storage warehouses first, disaster demands first and randomly distribution, MSA\_PABC generates the initial food source, and the proportion of food sources is 30%, 30%, and 40%. Then, it modifies the food source by reducing the excessively distributed materials so that all food sources satisfy the constraints (1) and (2).

*Step 3.* MSA\_PABC calculates the individual fitness value  $F_j$  and overall optimal evaluation value  $F_z$  of food sources.

*Step 4.* MSA\_PABC enters the employed bee phase. According to the number of rescue points, it divides the entire food source population into  $N_j$ -independent child populations by the niche technology. It implements the variable neighborhood search operation to find a locally optimal solution for each food source. Thereby, it obtains  $m1$  food sources. If the new food source dominates the old food source, then it updates the old food source. If the old food source dominates the new food source, then it deletes the new food source. Otherwise, it temporarily stores new food sources without changing the old food source and puts them in temporary food source collections. Completing the variable neighborhood search operation merges the food source set with the temporary food source set. Subsequently, it eliminates similar food sources through the elite retention strategy and the niche exclusion strategy to restore the food source collection's size to its original size.

*Step 5.* MSA\_PABC enters the onlooker bee phase. Calculating the crowdedness among food sources by formula (11) to determine the selected probability of each food source, it implements the following operation for  $m2$  times and obtains  $m2 * 2$  child food sources: it chooses a food source based on the rules of roulette and selects the neighbor food source with nearest European distance; then, it performs across the operation to generate two food sources and corrects the new two food sources to obtain two-child food sources satisfying the constraints (1) and (2). The  $m2 * 2$  child food sources and the food sources in the current population combine into a food source set, and MSA\_PABC performs the Pareto dominance strategy on the food source set to obtain a nondominated solution set. According to the overall evaluation

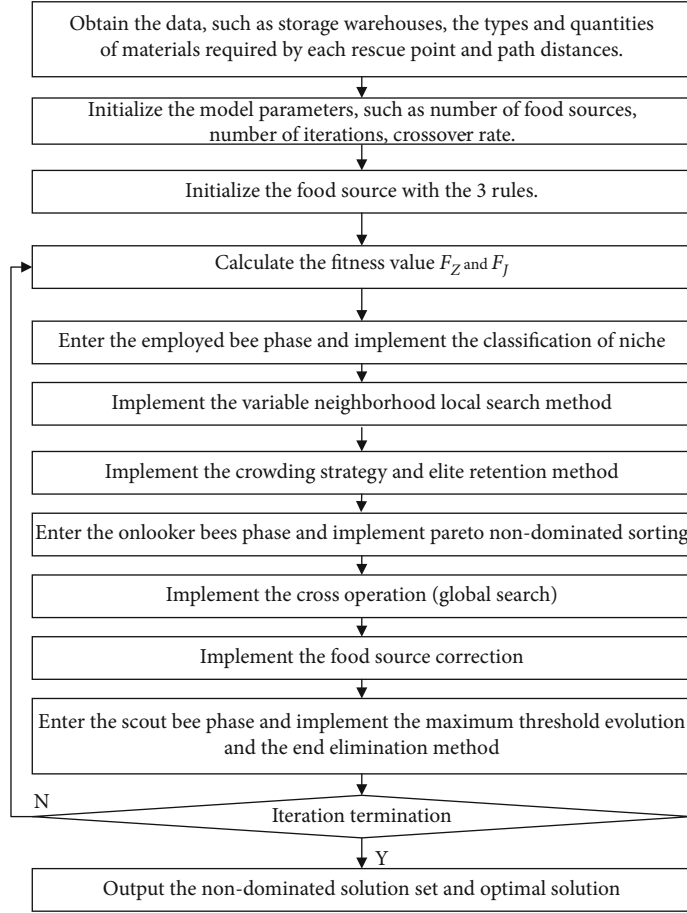


FIGURE 3: Algorithm flow chart.

optimal value  $F_z$ , it eliminates the poor food source solution so that the population number returns to the original size.

*Step 6.* MSA\_PABC enters the scout bee phase. It implements the final elimination method to rerandomly initialize a certain proportion of the food sources at the end of the ranking. Then, it uses the greedy strategy to update the old food sources. After  $U$  iterations, if the food source's overall value does not change, it reinitializes the food source. Simultaneously, the current population retains and updates the new global optimal solution and historical optimal solution based on the greedy strategy.

*Step 7.* MSA\_PABC determines whether the number of loop iterations is equal to the maximum number of iterations. It outputs a nondominated solution set and outputs the optimal solution for an overall evaluation. Otherwise, it goes to step (3).

## 5. Algorithm Simulation

*5.1. Simulation Parameters Selection.* To test and verify the performance of MSA\_PABC, as shown in Figure 4, we adopt the factual information of all storage warehouses and flood control materials in the management information system of flood control materials and rescue teams in Zhejiang Province of China developed by Zhejiang Yugong Information Technology Co., Ltd. Then, according to the actual disaster

situation, it randomly generates disaster scenarios of different rescue point locations and required flood control materials. Using the simulation parameters shown in Table 1, we carry out simulation experiments in simulated disaster scenarios. We analyze the distribution of nondominated solution sets and the convergence of MSA\_PABC, the effects of the number of food sources, crossover probability, the maximum number of evolutions, and end elimination ratio on the optimal solution evaluation value in 10 different disaster scenarios. Then, we calculate the average maximum transportation distance, the average material satisfaction rate of rescue points, the standard deviation of maximum transportation distance, the standard deviation of satisfaction rate, and the number of earliest completed convergence iterations of MSA\_PABC, ABC (artificial bee colony), NSGA2 (nondominated sorting genetic algorithm 2), and MOPSO (multiobjective particle swarm optimization) in 10 different disaster scenarios. We take the average value as the simulation result value. Among them, ABC utilizes the traditional artificial bee colony algorithm to solve the optimization model (8) and obtain the optimal solution. NSGA2 carries out the fast nondominated sorting strategy with elite retention. It selects the solution with the most extensive evaluation value as the final solution in the nondominated solution set. MOPSO realizes the scheduling optimization of flood control materials through the second set and adaptive grid method and selects

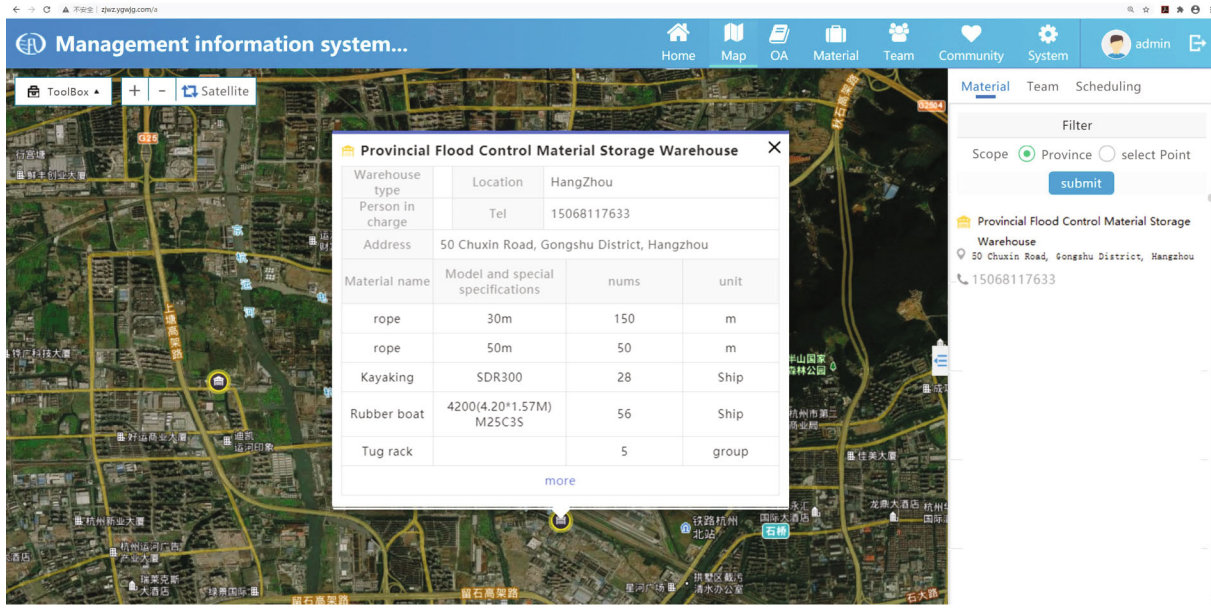


FIGURE 4: The management information system of flood control materials and rescue teams in Zhejiang Province of China.

TABLE 1: Simulation parameter table.

Parameter	Value
Number of food sources	50
Crossover probability	0.2
Maximum evolution times	2
End elimination ratio	0.1
Maximum iteration times	50
Number of rescue points	2-6
Material types	1-40
Number of exclusion member	2
Maximum loop search threshold	20

the final resolution according to the evaluation value. The average maximum transport distance is the average of the maximum transport distance of all rescue points. The intermediate material satisfaction rate is the average of the material satisfaction rates of all rescue points. The earliest number of iterations to complete convergence is the minimum number of iterations required when the algorithm converges to the optimal value. The standard deviation of the maximum transport distance, the standard deviation of the satisfaction rate, and the evaluation value of the optimal solution are calculated by formulas (6), (7), and (10), respectively.

## 5.2. Simulation Result Analysis

**5.2.1. Nondominated Solution Set and Convergence Analysis.** We choose a disaster scene randomly and selects the number of rescue points as 10 and other parameters in Table 1 to calculate the nondominated solution set of MSA\_PABC and analyze its convergence. When the number of rescue points is greater than 2, the rescue points compete, and their fitness values are as optimal as possible. Since the number of rescue

points is 10 and it has more spatial dimensions, for the convenience of data display, we divide the rescue points into 2 groups and calculate the normalized fitness value sum of the 2 groups in the nondominated set. Then, it analyzes the Pareto distribution of those 2 groups of rescue points. As shown in Figure 5, the scheduling problem of flood control materials is the distribution problem of rescue points and warehouses. Therefore, it is a combination of multiple distribution schemes and is discrete. Its optimal Pareto nondominated solution set does not present continuous dense data points and only offers a distribution of 10 points. However, its data points achieve the optimal fitness value without reducing the fitness values of another group and still show the Pareto curve’s characteristics. As shown in Figure 6, MSA\_PABC uses a niche method and variable neighborhood local search method in the employed bee operation to improve the convergence ability and ensure that the offspring can optimally inherit the current optimal food source as far as possible. In the onlooker bee phase, MSA\_PABC uses a crossover strategy to enhance global search capability. In the scout bee phase, MSA\_PABC sets the bee colony’s maximum evolution threshold and uses an end elimination mechanism to update food sources with low evaluation values and delete food sources that cannot be evolved again. It expands the search capability, and the food source can grow faster in a favorable direction. Simultaneously, through the calculation of congestion and the maintenance of Pareto nondominated sets, MSA\_PABC can quickly find and retain the optimal food source in history and improve its convergence accuracy. Therefore, MSA\_PABC can discover the optimal evaluation value of the food source after 24 iterations.

### 5.2.2. The Influence of Parameters on MSA\_PABC

(1) *The Influence of the Number of Food Sources on MSA\_PABC.* We select the number of food sources 20, 30, 40, 50,

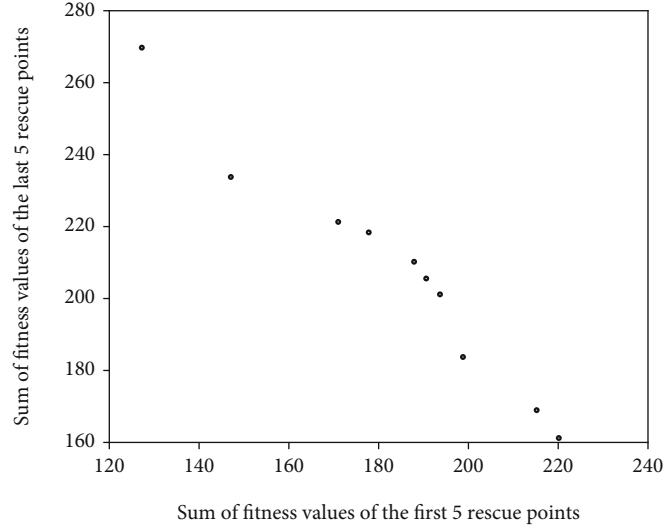


FIGURE 5: Distribution diagram of nondominated solution set in MSA\_PABC.

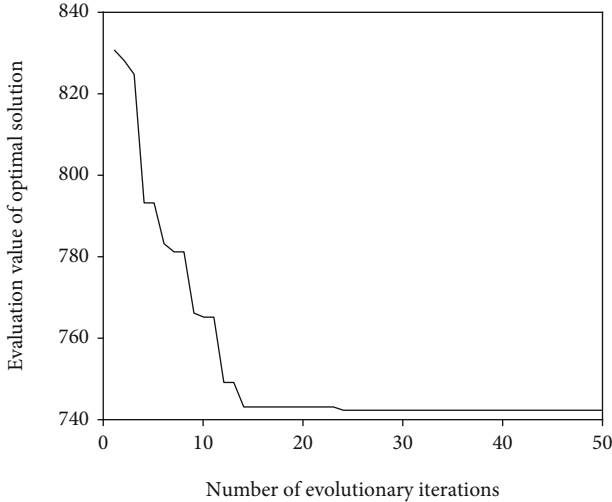


FIGURE 6: Convergence diagram of evaluation value of optimal solution in MSA\_PABC.

60. The number of rescue points 2, 3, 4, 5, 6, and other parameters in Table 1 calculate the average evaluation value of output solution in 10 disaster scenarios with different materials and analyze the influence of the number of food sources.

As shown in Figure 7, when the number of rescue points is 2, MSA\_PABC can converge to the current optimal solution and obtain the optimal solution when solving the low-dimensional answer of flood control material scheduling. The evaluation values of the output solutions under different numbers of food sources remain the same. However, with the increase in the number of rescue points, the data dimension increases. When the number of food sources is small and the number of algorithm iterations is limited, in the process of searching for the optimal solution, the output solution is easy to fall into the optimal local solution, and the maximum

fitness value of the output solution is more considerable. Therefore, under different numbers of rescue points, when the number of food sources is 20, the output solution's evaluation value is the largest. As the number of food sources increases, the evaluation value of the output solution becomes smaller. When the numbers of food sources are 50 and 60, MSA\_PABC can obtain the current optimal solution. The evaluation value of the output solution is the smallest, and the difference is not large. Therefore, we choose 50 food sources for a simulation experiment.

(2) *The Influence of Crossover Probability on MSA\_PABC.* We choose the crossover probability 0.1, 0.2, 0.3, 0.4, 0.5, the number of rescue points 2, 3, 4, 5, 6, and other parameters in Table 1 analyze the crossover probability's influence on the evaluation value of output solution.

As shown in Figure 8, when the number of rescue points is 2, MSA\_PABC has better convergence when solving multi-objective low-dimensional data. They converge to the optimal solution under different crossover probability, and their evaluation values of output solution remain consistent. In the explanation of high-dimensional discrete problems of flood control materials, the low cross probability is difficult to achieve the goal of crossover, and the small number of food sources in the nondominated set and the high cross probability destroy the overall quality of the food source, which makes the algorithm more tend to be random. It also reduces the convergence of MSA\_PABC and converges to the optimal local solution within a limited number of iterations. Therefore, under the number of rescue points, when the crossover probability is 0.2, the output solution's evaluation value is the smallest. When the crossover probability is 0.1, its evaluation value of the output solution is second. As the crossover probability increases after 0.2, the output solution's evaluation value becomes more extensive. Thus, we choose the crossover probability 0.2 for a simulation experiment.



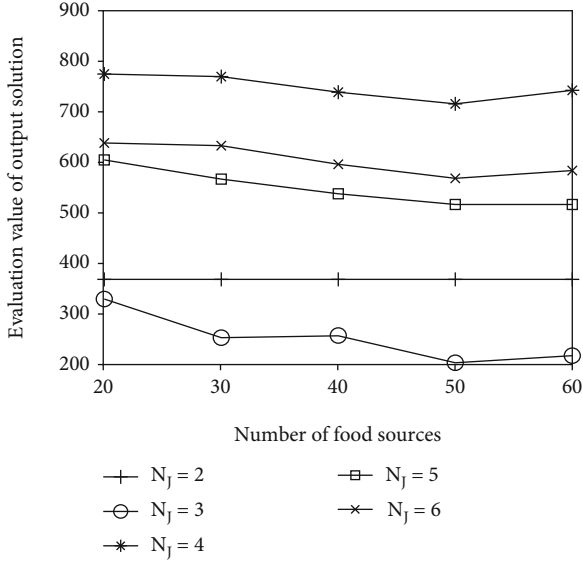


FIGURE 7: The influence of the number of different food sources on the evaluation value of output solution in MSA\_PABC.

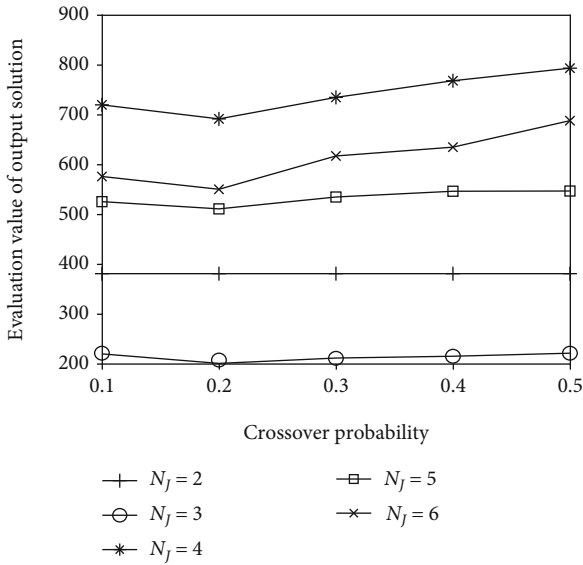


FIGURE 8: The influence of different crossover probabilities on the evaluation value of output solution in MSA\_PABC.

(3) *The Influence of the Maximum Number of Evolutions on MSA\_PABC.* We select the maximum number of evolutions 1, 2, 3, 4, 5, and the number of rescue points 2, 3, 4, 5, 6, and other parameters in Table 1 analyze the influence of the maximum number of evolutions on the evaluation value of output solution.

As shown in Figure 9, although a minimal evolution threshold will improve the searchability of the solution space, it is a high probability to prevent high-quality solutions from being effectively inherited to the next generation of populations. It destroys the convergence effectiveness of MSA\_PABC. However, a considerable evolution threshold will

decrease the solution space’s searchability as the number of algorithm iterations increases. Therefore, under different numbers of rescue points, when the maximum number of evolutions is 2, its evaluation value of the output solution is the smallest. As the maximum number of evolutions increases from 2, the output solution’s evaluation value becomes more extensive, so we choose the maximum number of evolutions 2 for the simulation experiment.

(4) *The Influence of the End Elimination Ratio on the MSA\_PABC.* We select the different end elimination ratios 0.05, 0.1, 0.15, 0.2, and 0.25, the number of rescue points 2, 3, 4, 5, 6, and other parameters in Table 1 analyze the influence of different end elimination ratios the evaluation value of output solution.

As shown in Figure 10, the too small end elimination ratio is not conducive to eliminate the part inadequate solutions and reduce the convergence speed. And it converges to the optimal local solution within a limited number of iterations. The too large end elimination ratio will cause many solution sets to be reinitialized, thereby reducing the food source’s overall quality. Therefore, under different numbers of rescue points, when the end elimination ratio is 0.2, the output solution’s evaluation value is the smallest. When the end elimination ratio is less than 0.2, its evaluation value of the output solution becomes larger as the end elimination ratio decreases. When the end elimination ratio is greater than or equal to 0.2, the evaluation value of the output solution becomes larger. So we choose the end elimination ratio of 0.2 for the simulation experiment.

5.2.3. *Algorithm Performance Comparison.* In Section 5.2.2, when we choose the number of food sources 50, the crossover probability 0.2, the maximum number of evolutions 2, and the end elimination ratio 0.2, we can find the optimal solution of MSA\_PABC, and the evaluation value of the output solution is the smallest. Therefore, we choose those parameters, the number of rescue points 2, 3, 4, 5, 6, respectively, the corresponding material types 4, 13, 18, 23, 40, and the parameters in Table 1 calculate the average maximum transportation distance, the average material satisfaction rate of rescue points, the standard deviation of maximum transportation distance, the standard deviation of satisfaction rate, and the number of earliest completed convergence iterations in MSA\_PABC, ABC, NSGA2, and MOPSO under 10 randomly generated different disaster scenarios. The average values are used as the simulation results.

As shown in Figures 11 and 12, no matter how the number of rescue points changes, the average maximum distance of MSA\_PABC is lower than that of ABC, NSGA2, and MOPSO. The material satisfaction rate of MSA\_PABC is larger than that of ABC, NSGA2, and MOPSO. That is because MSA\_PABC uses the transportation distance and material satisfaction rate as the fitness parameters for calculating each rescue point and takes the optimal fitness values of multiple rescue points as a multiobjective problem. To solve the multiobjective problem, MSA\_PABC uses niche technology to group the offspring in the employing bee



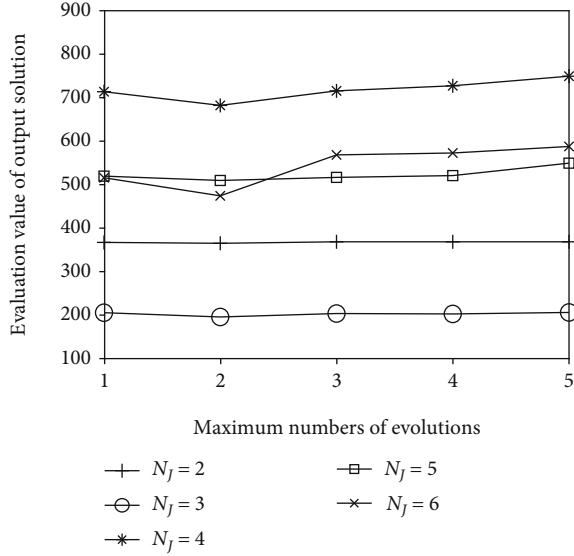


FIGURE 9: The influence of different maximum numbers of evolutions on the evaluation value of output solution in MSA\_PABC.

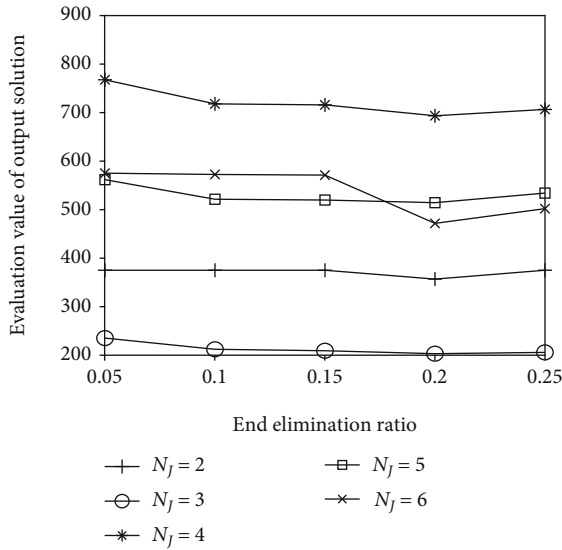


FIGURE 10: The influence of different end elimination ratio on the evaluation value of output solution in MSA\_PABC.

phase. MSA\_PABC also maintains the diversity of the population and improves the generation efficiency of Pareto non-dominated solutions. Then, MSA\_PABC uses variable neighborhood search operation and crossover operation to improve the algorithm's global search capabilities and local update capabilities and ensure the solution's quality. It uses the Pareto control strategy to avoid falling into the optimal local solution. Therefore, MSA\_PABC can find the optimal solution within the maximum number of iterations of 50.

As shown in Figures 13 and 14, regardless of the number of rescue points, the standard deviation of the maximum transportation distance and material satisfaction rate of MSA\_PABC are lower than those of ABC, NSGA2, and

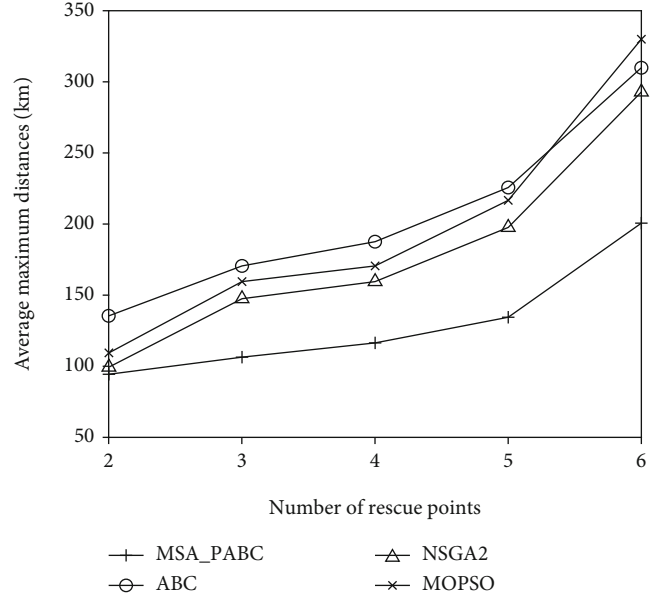


FIGURE 11: Comparison of average maximum distances.

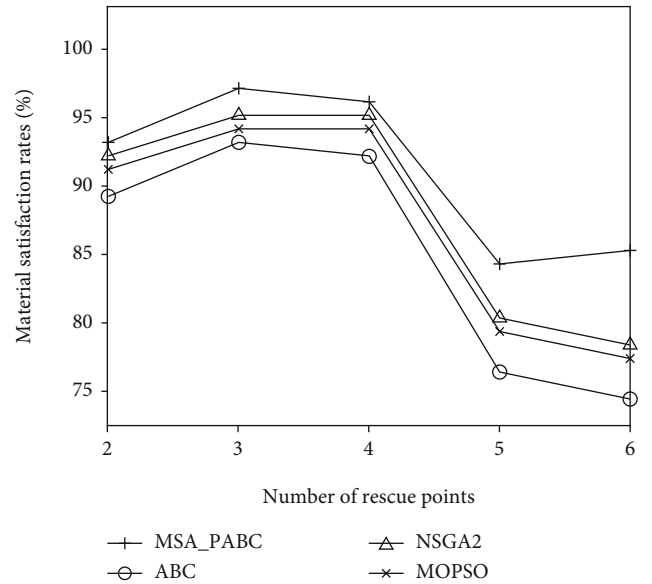


FIGURE 12: Comparison of material satisfaction rates.

MOPSO. That is because MSA\_PABC solves the multiobjective problem of competition among rescue points through a modified Pareto artificial bee colony algorithm to find a non-dominated set covering multiple schemes. In the nondominated location, MSA\_PABC takes the standard deviation of the maximum transport distance and the material satisfaction rate as parameters of the overall evaluation value. It balances the maximum transportation distance among rescue points and the secular satisfaction rate and achieves the rescue points' fairness. However, ABC only considers the comprehensive indicators of flood control material schedule but does not consider the right among rescue points, resulting in a higher standard deviation of the maximum transportation distance and material satisfaction rate. NSGA2 and

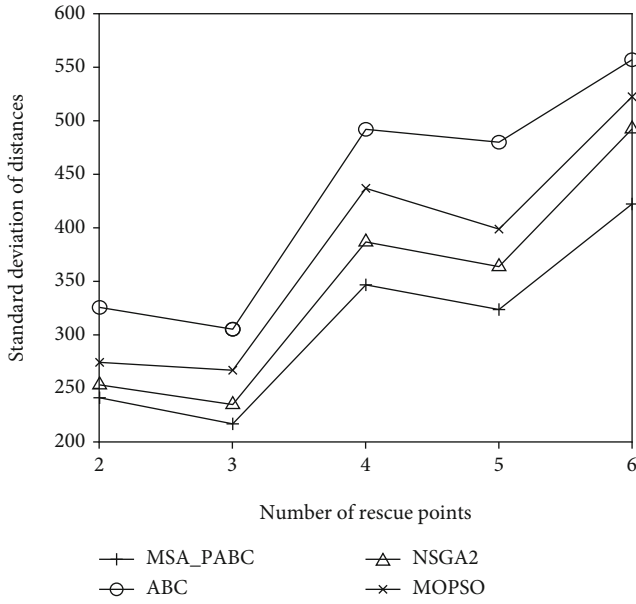


FIGURE 13: Comparison of standard deviation of maximum transport distances.

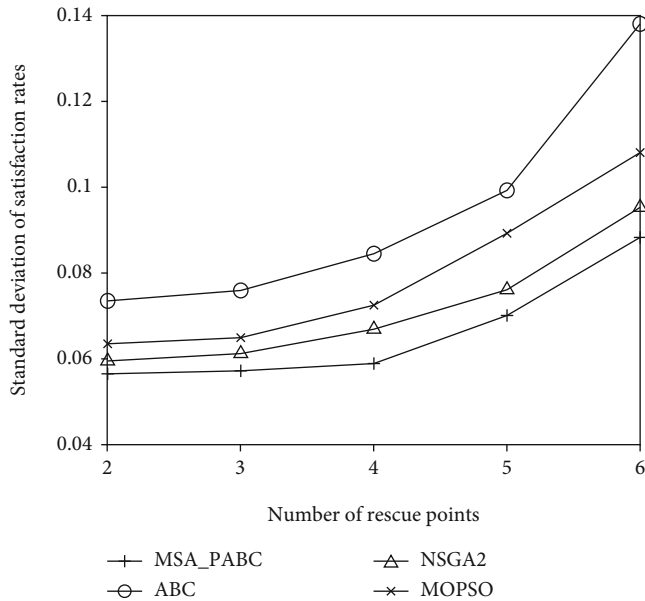


FIGURE 14: Comparison of standard deviation of material satisfaction rates.

MOPSO use the Pareto strategy to solve the multiobjective problems; their standard deviations are smaller than ABC but are significantly worse when solving the high-dimensional issues, resulting in a larger standard deviation than that of MSA\_PABC.

As shown in Figure 15, regardless of the number of rescue points, the number of the earliest completed convergence iterations of MSA\_PABC is lower than that of ABC, NSGA2, and MOPSO. This is because MSA\_PABC uses multistrategy food source initialization in the initialization phase and uses the niche technology, variable neighborhood search opera-

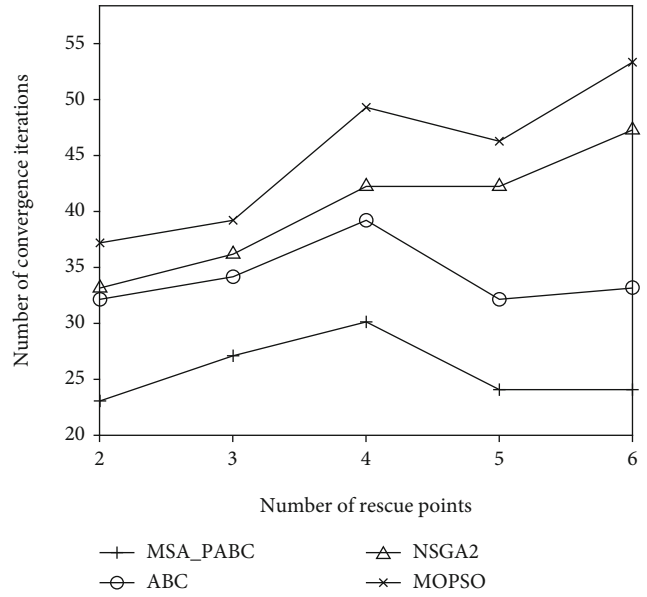


FIGURE 15: Comparison of the number of earliest completed convergence iterations.

tion, and crossover operation in the employed bee phase. It uses the Pareto nondominated sorting, crossover operation, and other operations in the onlooker bee phase. It uses the end elimination mechanism and evolution threshold in the scout bee phase. Therefore, MSA\_PABC can find the optimal solution in a short number of iterations, and its number of the earliest completed convergence iterations is the smallest. ABC directly finds better food sources nearby to update the optimal evaluation value. Its search ability is low, and it takes a long time to converge. It is also easy to fall into the optimal local solution. Although NSGA2 and MOPSO can search and approach the Pareto boundary, their traditional crossover, mutation, and other operations have low search efficiency, resulting in slow convergence. Therefore, their numbers of earliest completed convergence iteration are higher than that of ABC.

## 6. Conclusion

In the paper, we propose a multiobjective scheduling algorithm of flood control materials based on the Pareto artificial bee colony. First of all, considering the constraints, such as distance constraint from multiple storage warehouses to multiple rescue points, storage capacity constraint of warehouse materials, and material requirement constraint, we establish the scheduling optimization model of flood control materials for each disaster rescue point and the total scheduling optimization model of all flood control materials. Then, we use the modified Pareto artificial bee colony algorithm for solving the multiobjective model. That is, we propose a variety of food source initialization strategies, fitness value calculation of food sources, the employed bee operation including niche technology and variable neighborhood local search, onlooker bee operation including Pareto dominates sorting, crossover operations, and scout bee operation

including maximum evolution threshold and end elimination mechanism. Through the food source initialization strategies, we obtain the nondominated solution set under the scheduling problem of multiple disaster sites and various flood control materials and obtain an optimal solution from the nondominated solution set. Finally, we analyze the distribution of nondominated solution sets and the convergence of MSA\_PABC and analyze the influence of the number of food sources, crossover probability, maximum evolution times, and end elimination ratio on the evaluation value of output solution in MSA\_PABC. Finally, we compare the average maximum transportation distance, the average material satisfaction rate of rescue points, the standard deviation of maximum transportation distance, the standard deviation of satisfaction rate, and the number of earliest completed convergence iterations in MSA\_PABC, ABC, NSGA2, and MOPSO.

The simulation results show that no matter how many rescue points change, MSA\_PABC can quickly find the nondominated sets and optimal solutions. It also improves the convergence rate and the material satisfaction rate and reduces the average maximum transport distance of flood control materials, the standard deviation of the maximum transport distance, and the standard deviation of material satisfaction rate. However, the time complexity of MSA\_PABC is high, so in the future, we aim to use the heuristic algorithm to solve the optimal model and find the optimal solution, which reduces the calculation time of the algorithm.

## Data Availability

The data used to support the findings are available upon the authors' reasonable request.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This work was supported by the Public Welfare Technology Application and Research Projects of Zhejiang Province of China under Grant No. LGF19F010006 and Grant No. LGG20F010009, the Natural Science Foundation of Zhejiang Province of China under Grant No. LQ18F030006, and the Project Intelligentization and Digitization for Airline Revolution #2018R02008.

## References

- [1] W. Wang, J. Yang, L. Huang, D. Proverbs, and J. Wei, "Intelligent storage location allocation with multiple objectives for Flood control materials," *Water*, vol. 11, no. 8, pp. 1537–1618, 2019.
- [2] S. Cui, S. Liu, X. Tang, and T. Zhu, "Emergency material allocation problem considering post-disaster impact," in *2019 8th International Conference on Industrial Technology and Management (ICITM)*, pp. 290–294, Beijing, China, 2019.
- [3] J. Li, Z. Cai, J. Wang, M. Han, and Y. Li, "Truthful incentive mechanisms for geographical position conflicting mobile crowdsensing systems," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 2, pp. 324–334, 2018.
- [4] X. Xu, S. He, M. Han, R. M. Parizi, and G. Srivastava, "Budget feasible roadside unit allocation mechanism in vehicular ad-hoc networks," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pp. 1–5, 2020.
- [5] Y. Zhou, M. Han, L. Liu, Y. Wang, Y. Liang, and L. Tian, "Improving iot services in smart-home using blockchain smart contract," in *018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 81–87, Halifax, Canada, 2018.
- [6] B. Liu, W. Chen, M. Han et al., "Nonlinear time series prediction algorithm based on ad-ssnet for artificial intelligence-powered internet of things," *International Journal of Distributed Sensor Networks*, vol. 17, no. 3, 2021.
- [7] L. Liu and M. Han, "Privacy and security issues in the 5g-enabled internet of things," in *5G-Enabled Internet of Things*, pp. 241–268, CRC Press, 2019.
- [8] S. Xiaoyu, Z. Mingxi, C. Chunguang, Z. Ming, and Information Amp, Control Engineering Faculty, Shenyang Jianzhu University, School Of Management, and Shenyang Jianzhu University, "Improved differential evolution algorithm to solve bi-objective emergency material scheduling problem," *Information and Control*, vol. 48, no. 1, pp. 107–114, 2019.
- [9] T. Jun, M. A. Wen-Zheng, W. Ying-Luo, and W. Kan-Liang, "Emergency supplies distributing and vehicle routes programming based on particle swarm optimization," *Systems Engineering-Theory & Practice*, vol. 31, no. 5, pp. 898–906, 2011.
- [10] G. F. Zhang, Y. Q. Wang, Z. P. Su, and J. G. Jiang, "Modeling and solving multi-objective allocation-scheduling of emergency relief supplies," *Control and Decision*, vol. 32, no. 1, pp. 86–92, 2017.
- [11] G. Chai, J. Cao, W. Huang, and J. Guo, "Optimized traffic emergency resource scheduling using time varying rescue route travel time," *Neurocomputing*, vol. 275, no. 31, pp. 1567–1575, 2018.
- [12] F. S. Chang, J. S. Wu, C. N. Lee, and H. C. Shen, "Greedy-search-based multi-objective genetic algorithm for emergency logistics scheduling," *Expert Systems with Applications*, vol. 41, no. 6, pp. 2947–2956, 2014.
- [13] J. Wang and C. Jin-Jing, "Optimal synergetic regulation method and its use for rescuing materials against marine perils based on greedy algorithm," *Journal of Safety and Environment*, vol. 13, no. 5, pp. 254–258, 2013.
- [14] L. Zhang, C. Li, and B. Chen, "Optimization strategy of emergency resources scheduling of hierarchical multiple disaster sites during continuous consumption," *Journal of Dalian University of Technology*, vol. 275, no. 31, pp. 501–510, 2017.
- [15] Y. Hong, "Research on emergency resource scheduling in smart city based on hpsa algorithm," *International Journal of Smart Home*, vol. 9, no. 3, pp. 1–12, 2015.
- [16] G. A. O. H. Z. Yi-bing and L. I. Ning, "Study on model for emergency materials dispatching of earthquake disaster based on multi-demand centers," *China Safety Science Journal*, vol. 23, no. 1, pp. 161–165, 2013.
- [17] N. A. Kallioras, N. D. Lagaros, and M. G. Karlaftis, "An improved harmony search algorithm for emergency inspection scheduling," *Engineering Optimization*, vol. 46, no. 11, pp. 1570–1592, 2014.

- [18] S. Xiaoyu, Z. Qing, and C. Chunguang, "Improved bee colony algorithm for solving double layer emergency resource scheduling," *Information & Control*, vol. 44, no. 6, pp. 729–773, 2015.
- [19] F. Wex, G. Schryen, S. Feuerriegel, and D. Neumann, "Emergency response in natural disaster management: allocation and scheduling of rescue units," *European Journal of Operational Research*, vol. 235, no. 3, pp. 697–708, 2014.
- [20] C. Tian and Y. Lin, "Typhoon disaster emergency logistics vehicle dispatching optimization simulation under big data background," *Journal of Catastrophology*, vol. 34, no. 1, pp. 194–197, 2019.
- [21] M. Han, Z. Duan, and Y. Li, "Privacy issues for transportation cyber physical systems," in *Secure and Trustworthy Transportation Cyber-Physical Systems*, pp. 67–86, Springer, Singapore, 2017.
- [22] D. Karaboga and B. Basturk, "On the performance of artificial bee colony (ABC) algorithm," *Applied Soft Computing*, vol. 8, no. 1, pp. 687–697, 2008.
- [23] H. Fengcai, D. U. Ying, and L. Yang, "Artificial bee colony algorithm and its application," *Journal of Jilin University(Information ence Edition)*, vol. 34, no. 4, pp. 468–476, 2016.
- [24] J. Li, X. Guo, L. Guo, S. Ji, M. Han, and Z. Cai, "Optimal routing with scheduling and channel assignment in multi-power multi-radio wireless sensor networks," *Ad Hoc Networks*, vol. 31, pp. 45–62, 2015.
- [25] M. Yan, S. Ji, M. Han, Y. Li, and Z. Cai, "Data aggregation scheduling in wireless networks with cognitive radio capability," in *2014 Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pp. 513–521, Singapore, 2014.

## Research Article

# Multiscale Anchor-Free Region Proposal Network for Pedestrian Detection

Zhiwei Cao <sup>1</sup>, Huihua Yang <sup>1</sup>, Weijin Xu <sup>1</sup>, Juan Zhao <sup>2</sup>, Lingqiao Li <sup>3</sup>,  
and Xipeng Pan <sup>3</sup>

<sup>1</sup>School of Artificial Intelligence, Beijing University of Posts and Telecommunications, Beijing 100876, China

<sup>2</sup>China Mobile Research Institute, Beijing 100053, China

<sup>3</sup>School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004, China

Correspondence should be addressed to Huihua Yang; [yhh@bupt.edu.cn](mailto:yhh@bupt.edu.cn)

Received 27 February 2021; Revised 19 March 2021; Accepted 5 April 2021; Published 26 April 2021

Academic Editor: Yingjie Wang

Copyright © 2021 Zhiwei Cao et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Pedestrian detection based on visual sensors has made significant progress, in which region proposal is the key step. There are two mainstream methods to generate region proposals: anchor-based and anchor-free. However, anchor-based methods need more hyperparameters related to anchors for training compared with anchor-free methods. In this paper, we propose a novel multiscale anchor-free (MSAF) region proposal network to obtain proposals, especially for small-scale pedestrians. It usually has several branches to predict proposals and assigns ground truth according to the height of pedestrian. Each branch consists of two components: one is feature extraction, and the other is detection head. Adapted channel feature fusion (ACFF) is proposed to select features at different levels of the backbone to effectively extract features. The detection head is used to predict the pedestrian center location, center offsets, and height to get bounding boxes. With our classifier, the detection performance can be further improved, especially for small-scale pedestrians. The experiments on the Caltech and CityPersons demonstrate that the MSAF can significantly boost the pedestrian detection performance and the log-average miss rate (MR) on the reasonable setting is 3.97% and 9.5%, respectively. If proposals are reclassified with our classifier, MR is 3.38% and 8.4%. The detection performance can be further improved, especially for small-scale pedestrians.

## 1. Introduction

Pedestrian detection played an important role in self-driving vehicle tasks by assisting drivers to judge whether there are pedestrians in the front of the driving area. Therefore, pedestrian detection performance directly affects pedestrian safety [1–4]. In recent years, with the research and development of convolutional neural networks (CNN), pedestrian detection methods based on CNN have shown rapid progress. According to the regression starting status, pedestrian detection can be divided into anchor-based [5–9] and anchor-free [10–16] detection methods.

Based on the number of the detection stages, anchor-based methods can be divided into two-stage [9, 17–20] and one-stage [6, 21, 22] detection methods. In two-stage detection, region proposals are generated firstly, and then,

the proposals are classified by a classifier. In one-stage detection, the final detection results can be obtained via only one step; pedestrian detection can skip the classification stage and predict bounding boxes with confidence scores directly.

The most impressive anchor-based method is the region proposal network (RPN) [7], which was first proposed in Fast-RCNN [7]. The regression starting status of RPN is predefined by a set of anchor boxes with multiple scales and ratios, and then, the anchors are transformed according to the learning parameters into proposals. Multiscale anchors can avoid the problem of scale imbalance [23] caused by the width and height range of ground truth. Although RPN can achieve excellent performance, it needs to design anchor boxes manually, which will affect the generalization ability of the model.

Different from anchor-based methods, anchor-free start regression from a point and do not require hyperparameters



about anchors. At the same time, with the help of focal loss [24] to solve the problem of the imbalance between positive and negative samples in training, many remarkable anchor-free detection methods have been developed, such as CSPNet [12], FCOS [14], and FSAF [25]. Among these methods is CSPNet, a single-scale anchor-free detector which is efficient on pedestrian detection datasets. However, as Figure 1 presents the height and the area of the pedestrians in the Caltech and CityPersons datasets, we observe most of the pedestrians in the dataset are small, which leads to scale imbalance [23]. CSPNet is insufficient for handling with scale imbalance, because it is a single-scale detection head and only concatenation is used to fuse these multiscale feature maps on different stages.

Inspired by RPN and CSPNet, we design a multiscale anchor-free detection head (MSAF) on adaptive channel feature fusion (ACFF) to generate proposals at different scales of features. The deeper the network is, the more difficult it is to detect small pedestrians. As we all know, different feature layers have different receptive field sizes. If multiscale regression is trained on the same feature layer, the size of ground truth and actual receptive fields do not match. Fortunately, within the feature extract module, the predict boxes do not necessarily need to correspond to the actual receptive fields of each layer. We design the multiscale detection head so that specific feature maps learn to be responsive to the particular scale of the pedestrians.

The main contributions of this work are summarized as follows: first, we propose an effective approach, named adapted channel feature fusion, to extract channel features at different levels so that only useful channel features are kept for fusion. Second, we propose a multiscale anchor-free method to replace the anchor-based method. It is used to reduce the hyperparameters that exist in anchor-based and address the scale imbalance problem. Third, a RCNN classifier is proposed to further improve the detection performance, especially small-scale pedestrian detection. Fourth, our detection method achieves state-of-the-art performance on the Caltech database [26] and competitive performance on the CityPersons [27] pedestrian benchmark.

## 2. Related Work

In this section, we mainly introduce anchor-based and anchor-free pedestrian detection methods based on the feature extraction and detection head. In the step of pedestrian classification, the description of how to select backbone and design classifier to address various problems is also highlighted.

**2.1. Anchor-Based Methods.** Anchor-based methods need a set of predefined anchors with different scales and ratios for regression training, and then, the anchors are transformed according to the training parameters into proposals. In two-stage pedestrian detection, generating high-quality proposal boxes is the first key step; then region proposals are classified by a classifier. The most representative method is RPN which is first introduced in Fast-RCNN [7]. RPN [19] takes a smooth L1 loss for regression training and is imple-

mented on the final high-level feature layers. MS-CNN [17] sets RPN modules on different level layers of backbone to pay more attention to small object detection. FPN [9] uses the top-down feature fusion method to build a feature pyramid and generate bounding boxes with RPN on different levels. We can also find that RPN based on feature fusion can significantly improve the detection performance. SDS-RCNN [28] applies semantic segmentation to RPN and RCNN to boost pedestrian detection accuracy. SSA-CNN [29] proposes a self-attention mechanism to connect the RPN and RCNN stages to improve pedestrian detection performance. AR-Ped [5] utilizes a stackable decoder-encoder module consisting of top-down and bottom-up pathways for feature fusion to improve the precision of the RPN stage. Repulsion [30] and aggregation [31] loss are designed on the RPN to tackle occluded pedestrians in crowded scenes.

In one-stage pedestrian detection, bounding boxes are predicted with only one step. SSD [6] predicts the detect results at different levels of features with a prior anchor. YOLOv3 [22] and YOLOv4 [21] predict the object on three different scale branches, and feature fusion architecture like FPN is used to detect small-scale objects. RetinaNet [24] also take the feature fusion architecture like FPN to object detection, and focal loss is proposed to address the foreground-background class imbalance.

**2.2. Anchor-Free Methods.** There are two ways to find objects in anchor-free detection. The first way is to use the center point or region of the pedestrian to predict the length from the bounding box boundary. YOLOv1 [13] predicts pedestrians on the final layer of backbone and detect objects in a grid cell if the center of pedestrian falls into. UnitBox [32] takes Intersection over Union (IoU) loss as detection head to predict proposals and avoid the box-level scale imbalance and optimizes the L2 loss in DenseBox [33]. CSPNet [12] extracts multiscale features with concatenation on different stages, and pedestrian detection is simplified as a straightforward center and scale prediction task through convolutions. Wang [15] appends some adaptations on CSPNet to improve the robustness of the method. CSID [16] proposes a pedestrian detector with a novel identity-and-density-aware non-maximum suppression (NMS) algorithm to refine the detection results. FCOS [14] selects FPN as feature fusion architecture and defines the inside of bounding box as positive.

The second way is to predict key points on heatmaps as detection head. CornerNet [11] takes an hourglass network for multiscale feature fusion and detects a pedestrian as a pair of key points on heat maps. CenterNet [10] adapts CornerNet's detection head as a triplet of keypoints to predict bounding boxes. ExtremeNet [34] also uses an hourglass network to extract features and predict four extreme points and one center point for each pedestrian.

**2.3. Classifier.** In the step of pedestrian classification, different types of classifiers have been designed to address various problems. In order to get better classification accuracy, we design different convolutional neural network architectures according to the application scenarios, such as MobileNet

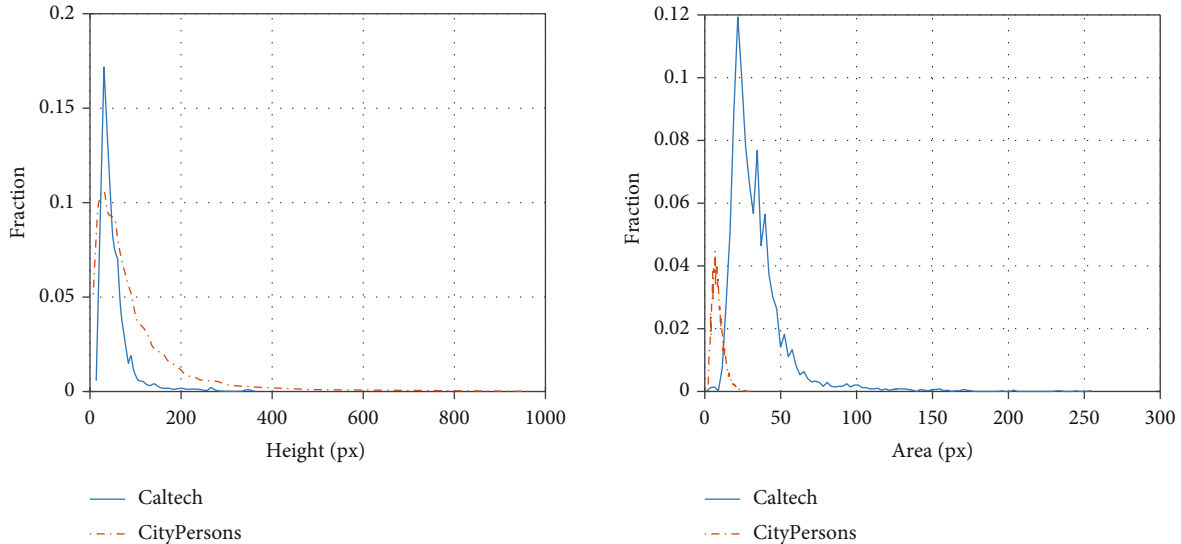


FIGURE 1: The left is pedestrian height distribution in the Caltech and CityPersons. The right is pedestrian area distribution in the Caltech and CityPersons where  $x$  axes are in  $\sqrt{\text{px}}$ .

[35], VGGNet [36], GoolgeNet [36], ResNet [37], and DenseNet [38]. In order to ensure that for any size of input regions, it can always produce the same size region features, RoIPooling [19] and RoIAlign [39] are designed, and the shared features are directly classified according to the Region of Interest (RoI).

To detect the small objects, RPN+BF [20] uses the cascaded Boosted Forest for pedestrian classification to mine hard negative examples and handle the small number of instances. In another approach, scale-aware [8] weights are predicted and a large-scale subnetwork and a small-scale subnetwork are combined into a unified framework to solve the multiscale pedestrian classification problem and achieve state-of-the-art performance on the Caltech dataset. In order to improve detection performance with feature fusion, BCN [28] combines semantic segmentation and classification together to perform pedestrian classification. SA-RCNN [29] uses self-attention to perform feature extraction for pedestrian classification and achieves good results. A previous study [40] designs a hyperlearner, which is a new type of feature fusion framework, to extract features, and uses additional pedestrian features to improve the detection performance. To handle the occlusion problem in pedestrian detection, a new partial occlusion-aware pooling unit [31] is used in classification. To address the IoU distribution imbalance, in Cascade R-CNN [41], several RCNN networks are cascaded based on different IoU thresholds, and the detection results are continuously optimized to improve the detection performance.

### 3. Baseline Method

CSPNet [12] is a single-scale anchor-free pedestrian detector. It can directly obtain the detection results by predicting the center location, the height of bounding boxes, and center offsets with single scale. The architecture consists of two modules: the feature extraction and the detection head.

The feature extraction module uses CNN to extract feature maps for pedestrian detection. In this paper, ResNet-50 is used as the backbone of feature extraction; its convolution layers can be divided into five stages according to the pooling stride. Given an input image of size  $H \times W$ , the feature resolution of stage  $i$  is  $(H/2^i) \times (W/2^i)$ . The experiment results show that the best detection performance can be obtained by deconvolution the features of stages 3, 4, and 5 into the same resolution  $(H/4) \times (W/4)$  before concatenation.

The detector head is used to generate the bounding box, which contains three branches: the first branch is to predict the classification score of the bounding box and determine the center location of the proposal. The second branch is used to predict the height of the bounding box and then use the aspect ratio to get the bounding box. The third branch is used to predict the center offsets of the bounding box and adjust the center location. The center offsets is defined as  $(\Delta x, \Delta y) = ((x_k/r) - \lfloor x_k/r \rfloor, (y_k/r) - \lfloor y_k/r \rfloor)$ . The details are provided in Figure 2(b). In the training process, the modified focal loss is used as the loss function in the classification task, and smooth L1 is used as the regression loss function in the height and center offsets prediction task.

## 4. Our Approach

In this section, we introduce an adaptive channel feature fusion method to extract channel features at different levels and propose a multiscale anchor-free region proposal network to generate proposals. The proposed network has fewer hyperparameters than anchor-based methods and can significantly boost detection performance, especially for small objects.

*4.1. Adapted Channel Feature Fusion for Feature Extraction.* In CSPNet, only concatenation is used to fuse the features on different levels. Currently, the common feature fusion methods are element-wise sum (SUM) or concatenation. As

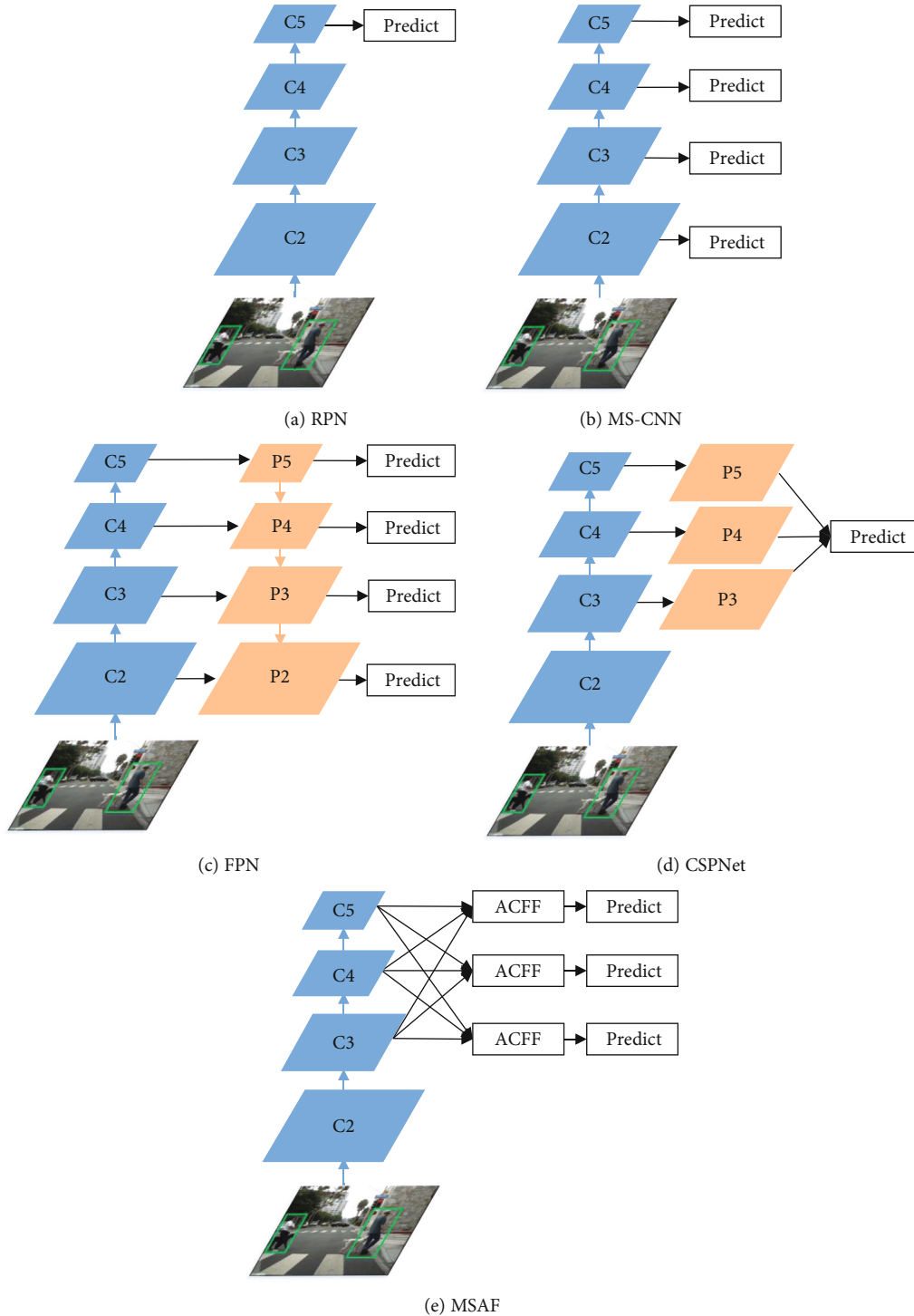


FIGURE 2: An illustration and comparison of different methods for generating proposals. Our MSAF is used to extract features based on ACFF and predict bounding boxes on different scales; after that, NMS is applied to generate final proposals with IoU threshold of 0.5.

we all know, different feature layers have distinct abilities, and the low-level feature maps can provide more precise localization information while the high-level maps contain more semantic information. Therefore, here, we introduce ACFF, which can not only adaptively select channel features on different scales for fusion but also boost the feature discrimination. The detail of ACFF can be found in Figure 3.

Two steps are needed to implement the ACFF. In the first step, the features of different levels are scaled to the same resolution and then concatenated on the channel dimension. If you want to get the fused feature of the  $i$ -th level, you need to scale the features of the other two adjacent different levels to the same resolution as the  $j$ -th level and then get the concatenated feature maps, because the features at three

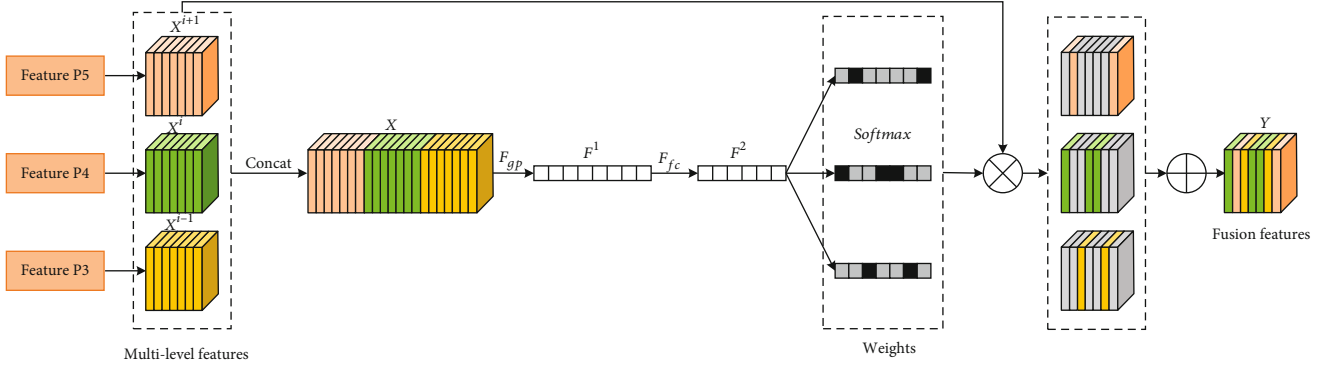


FIGURE 3: Illustration of adapted channel feature fusion. The first stage of ACFF is to concatenate features with equivalent scales along channel dimension. Then, the second stage uses learning weights to aggregate features in an adaptive way.

levels in detect backbone have different resolutions as well as different numbers of channels. The concatenated feature maps can be presented as

$$X = \text{Concat}(X^{i-1}, X^i, X^{i+1}), \quad (1)$$

where  $X^i$  is defined as the feature of the  $i$ -th level and  $X^i \in \mathbb{R}^{(H/r) \times (W/r) \times C}$ ,  $r$  is stride, and  $r = 2^i$ .

For example, let us assume that channel feature fusion is performed at the fourth level. If the resolution of the feature to be fused is smaller than that of the target feature, deconvolution is used to enlarge the feature, and then  $1 \times 1$  convolution layer is used to compress the channel to 256. If the resolution of the feature to be fused is greater than that of the target feature, we use a  $3 \times 3$  convolution layer with a step size of 2 to reduce the feature resolution and channel dimension.

In the second step, the global average pooling (GAP) is used to generate channel feature vectors  $F^1$ . The  $c$ -th channel element from GAP is calculated by the following formula:

$$F_c^1 = \text{GAP}(X_c). \quad (2)$$

Then, a new compact feature  $F^2$  is created to adaptively learn the fusion weights of different level features. This is achieved by a fully connected (FC) layer with the lower dimension:

$$\mathbf{z} = F^2 = \text{FC}(F^1), \quad (3)$$

where  $F^1 \in \mathbb{R}^C$ ,  $F^2 \in \mathbb{R}^{C'}$ , and  $C' = \max(C/r, L)$  is a typical setting in our experiment.

Further, softmax is used for normalization, and the learned weights  $\alpha_c$ ,  $\beta_c$ , and  $\gamma_c$  are used to select the corresponding level features for final fusion  $F_c$ . Note that  $\alpha_c$ ,  $\beta_c$ , and  $\gamma_c$  is simple a scale value at channel  $c$  and  $\alpha_c, \beta_c, \gamma_c \in [0, 1]$ .

$$\alpha_c = \frac{e^{\mathbf{A}_c \cdot \mathbf{z}}}{e^{\mathbf{A}_c \cdot \mathbf{z}} + e^{\mathbf{B}_c \cdot \mathbf{z}} + e^{\mathbf{C}_c \cdot \mathbf{z}}}, \quad (4)$$

$$F_c = \alpha_c \cdot X_c^{i-1} + \beta_c \cdot X_c^i + \gamma_c \cdot X_c^{i+1},$$

where  $F_c \in \mathbb{R}^{(H/r) \times (W/r)}$ ,  $\alpha_c + \beta_c + \gamma_c = 1$ , and  $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathbb{R}^{C \times C'}$ . With this method, the features at all the levels are adaptively aggregated at each scale. The output of ACFF can be used as the input of MSAF and RCNN.

**4.2. Multiscale Anchor-Free Detection Head.** Scale imbalance occurs in the pedestrian dataset because certain sizes of the objects or input bounding boxes are overrepresented [23]. Taking the Caltech [26] and CityPersons [27] datasets as examples, the height of the pedestrians ranges from 30 px to 350 px and 35 px to 965 px; the distribution of the pedestrian heights at different scales is imbalance. Approximately 80% of the pedestrians in the Caltech and 64% of the pedestrians in the CityPersons are less than 112 px in height. The detailed statistical information is provided in Figure 1. The scale imbalance problem suggests that a single scale of visual processing is not sufficient for detecting objects at different scales. If single-scale regression is used to predict the height, the constraint range is too large and may cause a deviation in the prediction results, like CSPNet in Figure 2(d). Two popular approaches have been used for multiscale predictions. The first approach is the prediction on the same layer. For example, in RPN [19], as shown in Figure 2(a), the detection head is on the end of the backbone with different aspect ratios and scales to train. The second approach is to predict on different level layers at multiple scales as shown in Figures 2(b) and 2(c). The detection head is different for each feature layer. For example, in MS-CNN [17], FPN [9], and FCOS [14], detection head is attached to each level on the feature pyramid to obtain proposals.

To address shortcoming of scale imbalance, we propose MSAF to assign the ground truth in different scale-spaces for forward and backward as shown in Figure 2(e). The MSAF is based on a convolutional network that produces bounding boxes with scores followed by an NMS step to produce the final detection. Three branches are attached to the final feature maps  $F$  to predict the pedestrian location, height, and center offsets at each scale. The width can be calculated with an aspect ratio and height. According to the statistics of pedestrian detection bounding box annotations [26, 27], the aspect ratio is generally set to 0.41. In this detection head, we attach a  $3 \times 3$  convolution layer on the fusion

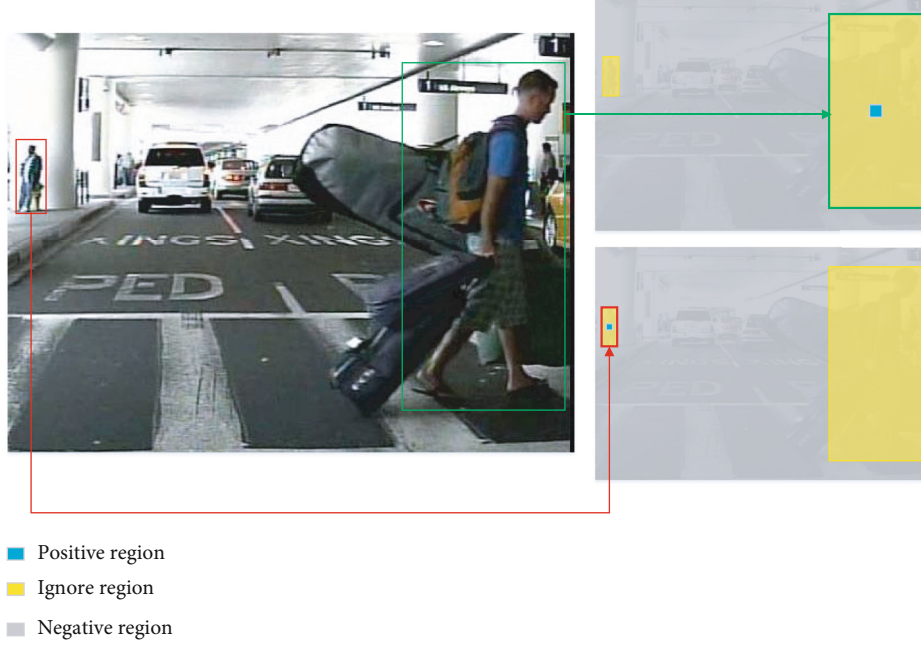


FIGURE 4: An illustration of MSFA ground truth. The ground truth is assigned to different levels of features according to the height of pedestrians. The positive region, negative region, and ignore region are defined. The top right ground truth is small scale, and the bottom right ground truth is large scale.

feature  $F$ , and then three head map layers are appended to predict location, height and offset with  $1 \times 1$  convolution kernel.

During training, we must determine how to assign the ground truth to the corresponding scale. To handle different object scales, we refer to the formula in FPN [9]. If the ground truth height is  $h$ , we assign it to the scale  $k$  according to

$$k = \left\lceil k_0 + \log_2 \left( \frac{h}{224} \right) \right\rceil, \quad k_0 = 4. \quad (5)$$

Taking the Caltech as example, the ground truth bounding boxes are assigned into three scales: 56~112 px, 112~224 px, and 224 px~. An illustration example of assigning pedestrians to different levels according to different scales of pedestrians is depicted in Figure 4. The red ground truth is assigned to the low-level features, and the green ground truth is assigned to the high-level features for prediction.

To predict the center location, we define the positive region, ignore region, and negative region for center ground truth. If the point falls into the center region of the pedestrian, it is assigned to positive samples for training. The center region is the area with a pedestrian center as the center within a radius of 2. The ignore region is the location where the ground truth bounding box is not assigned in this scale  $k$  and ground truth bounding box excluding positive samples. If the positive and ignore regions are excluded in the image, the rest are negative regions. The whole illustration can be found in Figure 4.

The modified focal loss is used as the loss function to predict center location as follows:

$$L_{\text{loc}} = -\frac{1}{P} \sum_{i=1}^{W/r} \sum_{j=1}^{H/r} a_{ij} (1 - p_{ij})^\gamma \log(\hat{p}_{ij}), \quad (6)$$

$$a_{ij} = \begin{cases} 1, & y_{ij} = 1, \\ (1 - M_{ij})^\beta, & \text{otherwise.} \end{cases}$$

In the above,  $P$  is the number of positive samples.  $\gamma$  and  $\beta$  are the focusing hyperparameters, and we experimentally set  $\gamma = 2$  and  $\beta = 4$  as suggested in [12].  $M_{ij}$  is a 2D Gaussian mask centered at the location  $(i, j)$ , and the mask is proportional to the height and width of the individual objects. If  $y_{ij}$  is equal to 1,  $\hat{p}_{ij}$  is set to  $p_{ij}$ , and  $\hat{p}_{ij}$  is set to  $1 - p_{ij}$  otherwise.

To predict pedestrian height and center offsets, the pedestrian height in scale  $k$  is redesigned as  $h_k = \log((h - 28(k - 2))/(7 \times 2^{k-1}))$ . We select the smooth L1 loss for height and offset prediction:

$$L_{\text{box}} = \frac{1}{P} \sum_{i=1}^P \text{Smooth L1}(b, \hat{b}), \quad (7)$$

where  $b = (\Delta x, \Delta y, h_k)$  and  $\hat{b} = (\Delta \hat{x}, \Delta \hat{y}, \hat{h}_k)$  represent the offset and height from ground truth and prediction of positive samples, respectively.

To sum up, the optimization objective in scale  $k$  is

$$L_k = \alpha_{k1} L_{\text{loc}} + \alpha_{k2} L_{\text{box}}. \quad (8)$$



TABLE 1: Comparison of different feature fusion methods on the Caltech with only single-scale detect head.

Method	ResNet-50	
	IoU = 0.5	IoU = 0.75
Concat	4.54	25.76
SUM	4.66	30.87
ACFF	4.13	26.23

TABLE 2: Comparison of different region proposal methods on the Caltech dataset under the reasonable and all setting.

Method	ResNet-50		VGG-16	
	Reasonable	All	Reasonable	All
RPN [20]	—	—	10.67	64.22
MS-CNN [17]	—	—	9.47	63.59
SDS-RPN [28]	—	—	8.17	61.29
SSA-RPN [29]	—	—	8.30	61.77
AR-RPN [5]	—	—	7.16	59.98
CSPNet [12]	4.54	56.94	5.29	60.06
FPN [9]	4.32	56.16	5.09	59.98
MSAF (ours)	3.97	55.93	4.91	58.86

The final objective loss function is a multitask loss in different scales to be optimized as follows:

$$L = \sum_{k=1}^{C1} L_k, \quad (9)$$

where  $C1$  corresponds to the max scale of pedestrian height in function (5).

**4.3. RCNN Classifier.** The RCNN classifier is used to classify the proposals generated by the MSAF as pedestrian or non-pedestrian. We take the object classifiers from [5, 20, 28, 29] as references to construct the RCNN classifier. We resize the object to a fixed resolution and then use it as the input of the classifier to determine whether it is a pedestrian based on the final score. As shown in Figure 1, the height of most pedestrians is less than 112 px. If the image is resized to  $224 \times 224$  px as the input, the information of the image will be distorted, degrading the classification performance. To alleviate this problem, we cropped the object from the image, added 25% padding, and resized it to  $112 \times 112$  px as the input. VGG-16 [32] without the pool5 layer is chosen as the backbone since the size of the receptive field of VGG-16 is the same as that of the pedestrian. ACFF is used to extract features to improve the discrimination ability of the model; the detail can be found in Section 4.1.

## 5. Experiments

In this section, we first introduce the implementation details, evaluation metrics, and dataset information. Then, the ablation studies about the MSAR and ACFF are reported. Finally,

TABLE 3: Comparisons on different RCNN classifiers with new annotations under the reasonable setting.

Method	VGG-16		ResNet-50	
	112	224	112	224
RPN-BF [20]	4.26	4.66	—	—
SDS-RCNN [28]	3.84	4.08	—	—
AR-Ped [5]	3.96	4.09	—	—
RCNN	3.47	3.63	3.79	3.85
RCNN+ACFF (ours)	3.38	3.58	3.71	3.89

we also give a detailed description of the benchmark comparison experiments.

**5.1. Training, Inference, and Implementation Details.** The whole detect framework is implemented on Keras. In MSAF stage, the ResNet-50 is used as backbone to predict the bounding boxes. Specifically, our MSAF is trained using the adaptive moment estimation (Adam) algorithm for 100 K iterations with an initial learning rate of 0.0001 and a learning policy for the steps. Each minibatch is constructed from an  $N = 16$  image. It is trained with multiscale input image in the scale between 0.6 and 1.5. Whole image is taken as input to predict height, offset, and locations. We first select bounding boxes with score above 0.01 and then use NMS with threshold 0.5 for final processing. In RCNN stage, VGG-16 is selected as backbone and is trained with the stochastic gradient descent (SGD) algorithm for 120 K iterations with an initial learning rate of 0.001 and a learning policy for the steps. After 60 K iterations, the learning rate is set to 0.0001. The weight decay and momentum are set as 0.0005 and 0.9, respectively. No more than 20 proposals are selected from MSAF for each SGD minimatch, and these are selected according to the scores in a descending order. To carry out the experiments, an Intel Xeon E5-2620 @ 2.1 GHz CPU server with 48 GB of memory and two TITAN RTX (24 GB) GPUs are used.

**5.2. Evaluation Metrics.** To evaluate MSAF, two benchmark datasets, Caltech [26] and CityPersons [27], are selected for the experiment and comparison. The log-average miss rate over False Positive Per Image (FPPI) ranging in  $[10^{-2}, 10^0]$  (denoted as  $MR^2$ ) [26] is used to evaluate the pedestrian detection performance. A lower miss rate indicates better detection performance. The evaluation settings are from Caltech and CityPersons, respectively. Generally speaking, we need to focus on the height in the reasonable setting is greater than 50 pixels and in the all setting is greater than 20 pixels.

**5.2.1. Caltech.** The Caltech pedestrian dataset [26] consists of approximately 10 hours of  $640 \times 480$  30 Hz video taken from a vehicle driving through regular traffic in an urban environment. Approximately 250,000 frames with a total of 350,000 bounding boxes and 2300 unique pedestrians were annotated. We extract one out of every 4 frames from the raw videos (acquiring a total of 42782 images) to form the training set and one frame out of every 30 frames from the raw videos (acquiring a total of 4024 images) to form the test

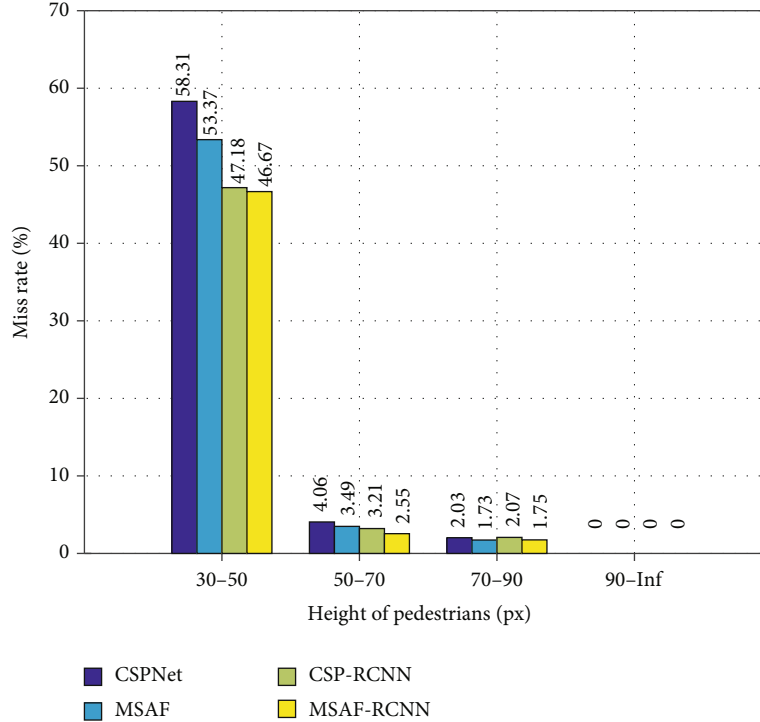


FIGURE 5: Comparison of  $MR^{-2}$  distribution with different pedestrian height on Caltech.

set. The new annotations [42] from the Caltech dataset are used on the experiments.

**5.2.2. CityPersons.** The CityPersons [27] is built upon Cityscapes dataset. It is a large and diverse set of stereo video sequences and is collected in urban street scenes. The dataset contains a total of 5000 images, and the resolution is  $2048 \times 1024$ , more than 35k person and 13k ignore regions. The split of train, validation, and test subsets is the same as that of Cityscapes. The training subset has 2975 images and was recorded across 18 different cities in three different seasons and various weather conditions. The validation subset was created from 3 different cities and has 500 images. The test subset was collected from 6 different cities and has 1575 images.

**5.3. Ablation Study.** In this section, we conduct ablation experiments on Caltech to evaluate the performance of each component of the proposed method. For the proposals, we focus on analyzing the impact of the MSAF and ACFF. For the classifier, we evaluate the impact of classification on the overall performance.

**5.3.1. ACFF for Region Proposals.** To assess the importance of ACFF, we compare it with other feature fusion methods: SUM and concatenation [43]. ResNet-50 is taken as backbones in these experiments. The three feature fusion methods contain the same detector head from CSPNet [12].

It can be observed from Table 1 that ACFF has the best performance when it is used to feature fusion and the performance of feature fusion using SUM and Concat is similar. ACFF can adaptively select different levels of channel fea-

tures for fusion, which can improve the performance of pedestrian detection. If ResNet-50 is taken as the backbone,  $MR^{-2}$  of ACFF on the Caltech is 0.41% higher than concatenation and 0.53 higher than SUM when IoU is 0.5.

**5.3.2. Importance of MSAF.** To highlight the excellent performance of MSAF, it is compared with RPN [19], SDS-RPN [28], SSA-RPN [29], AR-RPN [5], and CSPNet [12] on the Caltech dataset under the reasonable and all setting. The detailed results are given in Table 2.

Compared with other methods, MSAF is state-of-the-art as shown in Table 2, the  $MR^{-2}$  is 3.97% under the reasonable setting, and the  $MR^{-2}$  is 55.93% under the all setting when the backbone is ResNet-50. MSAF also gets the best performance when the backbone is VGG-16 and the  $MR^{-2}$  is 4.91% under the reasonable setting and the  $MR^{-2}$  is 58.86% under the all setting. Through the experimental comparison on two different backbones, we find that the region proposal methods on ResNet-50 are better than those on VGG-16. Compared with methods CSPNet, FPN (the same detection head as MSAF), and MSAF, it can be observed that the effect of multiscale is better than that of single scale. Multiscale regression can effectively improve the detection performance.

**5.3.3. Importance of RCNN Classifier.** To evaluate the influence of our classifier on the detection performance, MSAF is used to extract the proposals as the inputs and our RCNN classifier is compared with other classifiers from RPN+BF [20], SDS-RCNN [28], and AR-Ped [5]. The comparison experiments are performed on the Caltech dataset with different resolutions, and the results are given in Table 3.

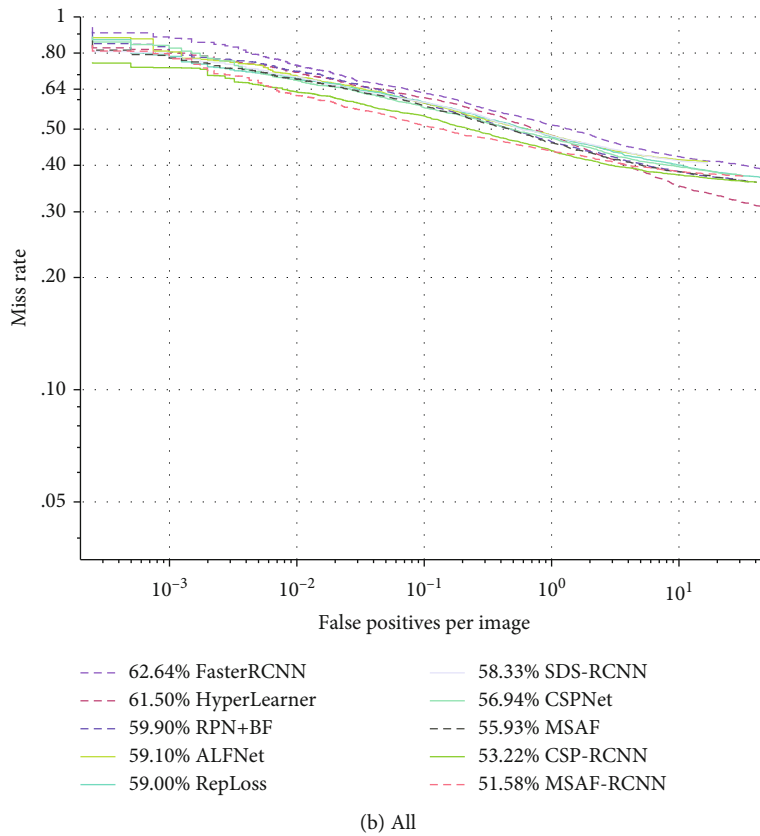
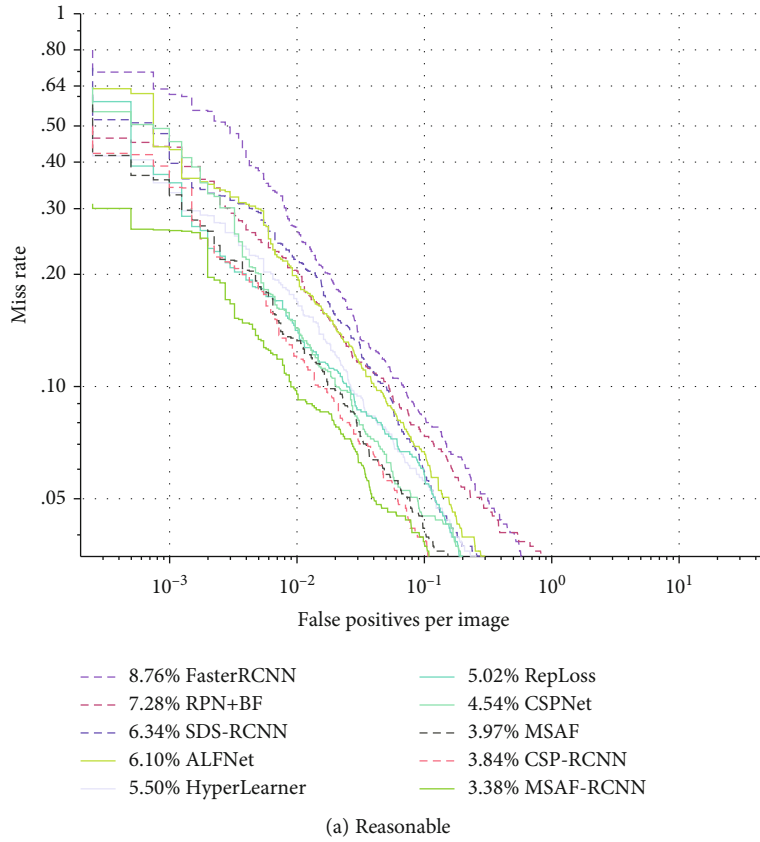


FIGURE 6: Comparison with the state-of-the-arts on the Caltech using new annotations. (a) is the results for the experiment performed on the reasonable setting; (b) shows the results of the experiment performed on the all setting.

TABLE 4: Comparison of our method with the state-of-the-art methods on the CityPersons.

Method	Backbone	Reasonable (%)	Heavy (%)	Partial (%)	Bare (%)	Small (%)	Medium (%)	Large (%)
Faster-RCNN [19]	VGG-16	15.4	—	—	—	25.6	7.2	7.9
RetinaNet [30]	ResNet-50	15.6	49.98	—	—	—	—	—
CornerNet [30]	Hourglass-54	21.0	56.0	—	—	—	—	—
Repulsion Loss [30]	ResNet-50	13.2	56.9	16.8	7.6	—	—	—
CSPNet [12]	ResNet-50	11.0	56.9	10.4	7.3	16.0	3.7	6.5
ACSP [15]	ResNet-50	9.3	46.3	8.7	5.6	—	—	—
CSID [16]	ResNet-50	8.8	46.6	8.3	5.8	—	—	—
MSAF (ours)	ResNet-50	9.5	48.4	9.3	6.2	15.5	3.5	6.2
MSAF-RCNN (ours)	ResNet-50	8.4	46.9	8.6	5.5	15.1	3.3	6.4

From Table 3, compared with the other methods, our method has the highest detection accuracy and better robustness. We observe that the  $MR^{-2}$  in our RCNN classifier is 3.38% when the resolution is  $112 \times 112$  px. The detection performance using  $112 \times 112$  px as input is better than that using  $224 \times 224$  px as input when VGG-16 is taken as backbone on the Caltech. If ACFF is used for feature fusion, the classification effect can be further improved from the method RCNN and RCNN+ACFF. In addition, we find that two-stage detection can significantly improve the performance with our classifier compared with one-stage detection.

**5.3.4. Small Object Detection.** In order to further illustrate the effectiveness of our method MSAF in small object detection, we make a comparison with CSPNet, CSPNet-RCNN, and MSAF-RCNN at different pedestrian heights in Figure 5. As shown in the figure, small-scale pedestrian detection is difficult; the higher the pedestrian’s height is, the better the detection effect is. The performance improvement in CSPNet and MSAF between 30 and 50 pixels is about 5% and 0.5% between 30 and 50 pixels. When the height is between 70 and 90 pixels, the improvement is not obvious. The improvement gap on small object detection using our RCNN classifier is large when the height between 30 and 50 pixels, about 11% improvement over CSPNet-RCNN and 7% improvement over MSAF.

#### 5.4. Benchmark Comparison

**5.4.1. Caltech.** The performance of MSAF was evaluated on the Caltech [26] and CityPersons pedestrian [27] benchmarks. As depicted in Figure 6(a), our MSAF-RCNN achieves the state-of-the-art result under the reasonable setting and the  $MR^{-2}$  is 3.38%. Without the RCNN classifier, the  $MR^{-2}$  of the MSAF is 0.45% higher than that of CSPNet. We also find that the  $MR^{-2}$  of the CSPNet-RCNN decreases from 4.54% to 3.97%. Figure 6(b) shows that our MSAF-RCNN obtained the best result, with an  $MR^{-2}$  (%) of 51.58% for the all setting. Compared with other region proposal methods, the gap between MSAF and CSPNet in  $MR^{-2}$  is about 1%. All of these show that MSAF can achieve better performance on Caltech dataset. The anchor-free method MSAF can replace anchor-based method to generate pro-

posals. At the same time, it can alleviate the scale imbalance problem.

**5.4.2. CityPersons.** The experimental results in Table 4 show that our MSAF displays overall performance improvement compared with CSPNet, and the  $MR$  decreases to 9.5% on the reasonable set. This also shows that the effect of MSAF as one-stage detection is not better than that of ACSP [15] and CSID [16]. However, we find that our MSAF-RCNN achieves state-of-the-art performance on the reasonable setting and the second best performance on the heavy set and partial set. This shows that our RCNN classifier significantly improves the performance based on the proposals obtained from MSAF. As shown in the small column in Table 4, our MSAF can effectively detect small objects.

## 6. Conclusions

To improve the pedestrian detection performance, a multi-scale anchor-free region proposal network is proposed in this paper. ACFF is used to extract features firstly, and then MSAF detector head is used for training according to the height of pedestrians. Through experimental comparisons, we know that multiscale detection is easier to detect small-scale pedestrians than single-scale detection. In addition, the RCNN classifier is taken for further improvement. Compared with other detection methods, we find that the performance of two-stage detection is significantly better than that of one-stage detection. Overall, our detection method achieved state-of-the-art performance on Caltech with new annotations and obtains competitive performance on CityPersons.

## Data Availability

The raw/processed data required to reproduce these findings cannot be shared at this time as the data also forms part of an ongoing study. Requests for data, please send email to corresponding author.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This research was supported in part by the National Key R&D Program (Grant No. 2018AAA0102600), the National Natural Science Foundation of China (Grant Nos. 62002082, 61866009, and 61906050), and Guangxi Natural Science Foundation (Grant Nos. 2019GXNSFAA245014 and 2020GXNSFBA238014).

## References

- [1] Z. Cai and Z. He, "Trading private range counting over big IoT data," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 144–153, Dallas, TX, USA, 2019.
- [2] Z. Cai, X. Zheng, and J. Yu, "A differential-private framework for urban traffic flows estimation via taxi companies," *IEEE Transactions on Industrial Informatics*, vol. 15, pp. 6492–6499, 2019.
- [3] D. Gerónimo, A. M. López, A. D. Sappa, and T. Graf, "Survey of pedestrian detection for advanced driver assistance systems," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, pp. 1239–1258, 2010.
- [4] Y. Wang, Y. Gao, Y. Li, and X. Tong, "A worker-selection incentive mechanism for optimizing platform-centric mobile crowdsourcing systems," *Computer Networks*, vol. 171, article 107144, 2020.
- [5] G. Brazil and X. Liu, "Pedestrian detection with autoregressive network phases," 2018, <https://arxiv.org/abs/1812.00440>.
- [6] G. Cao, X. Xie, W. Yang, Q. Liao, G. Shi, and J. Wu, "Feature-fused SSD: fast detection for small objects," 2017, <https://arxiv.org/abs/1709.05054>.
- [7] R. B. Girshick, "Fast R-CNN," in *2015 IEEE International Conference on Computer Vision (ICCV)*, pp. 1440–1448, Santiago, Chile, 2015.
- [8] J. Li, X. Liang, S. Shen, T. Xu, J. Feng, and S. Yan, "Scale-aware fast R-CNN for pedestrian detection," *IEEE Transactions on Multimedia*, vol. 20, pp. 985–996, 2018.
- [9] T. Lin, P. Dollár, R. B. Girshick, K. He, B. Hariharan, and S. J. Belongie, "Feature pyramid networks for object detection," in *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 936–944, Honolulu, HI, USA, 2017.
- [10] K. Duan, S. Bai, L. Xie, H. Qi, Q. Huang, and Q. Tian, "Centernet: keypoint triplets for object detection," *2019 IEEE/CVF International Conference on Computer Vision (ICCV)*, 2019, pp. 6568–6577, Seoul, Korea (South), 2019.
- [11] H. Law and J. Deng, "Cornersnet: detecting objects as paired keypoints," in *Computer Vision – ECCV 2018*, V. Ferrari, M. Hebert, C. Sminchisescu, and Y. Weiss, Eds., vol. 11218 of Lecture Notes in Computer Science, pp. 765–781, Springer, Cham, 2018.
- [12] W. Liu, S. Liao, W. Ren, W. Hu, and Y. Yu, "High-level semantic feature detection: a new perspective for pedestrian detection," 2019, <https://arxiv.org/abs/1904.02948>.
- [13] J. Redmon, S. K. Divvala, R. B. Girshick, and A. Farhadi, "You only look once: unified, real-time object detection," in *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 779–788, Las Vegas, NV, USA, 2016.
- [14] Z. Tian, C. Shen, H. Chen, and T. He, "FCOS: fully convolutional one-stage object detection," in *2019 IEEE/CVF International Conference on Computer Vision (ICCV)*, pp. 9626–9635, Seoul, Korea (south), 2019.
- [15] W. Wang, "Adapted center and scale prediction: more stable and more accurate," 2020, <https://arxiv.org/abs/2002.09053>.
- [16] J. Zhang, L. Lin, Y. Chen, Y. Hu, S. C. H. Hoi, and J. Zhu, "Attribute-aware pedestrian detection in a crowd," 2019, <http://arxiv.org/abs/1910.09188>.
- [17] Z. Cai, Q. Fan, R. S. Feris, and N. Vasconcelos, "A unified multi-scale deep convolutional neural network for fast object detection," in *Computer Vision – ECCV 2016*, B. Leibe, J. Matas, N. Sebe, and M. Welling, Eds., vol. 9908 of Lecture Notes in Computer Science, pp. 354–370, Springer, Cham, 2016.
- [18] Z. Cao, H. Yang, J. Zhao, X. Pan, L. Zhang, and Z. Liu, "A new region proposal network for far-infrared pedestrian detection," *IEEE Access*, vol. 7, pp. 135023–135030, 2019.
- [19] S. Ren, K. He, R. B. Girshick, and J. Sun, "Faster R-CNN: towards real-time object detection with region proposal networks," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 39, pp. 1137–1149, 2017.
- [20] L. Zhang, L. Lin, X. Liang, and K. He, "Is faster R-CNN doing well for pedestrian detection?," in *Computer Vision – ECCV 2016*, Lecture Notes in Computer Science, B. Leibe, J. Matas, N. Sebe, and M. Welling, Eds., pp. 443–457, Springer, Cham, 2016.
- [21] A. Bochkovskiy, C. Wang, and H. M. Liao, "Yolov 4: optimal speed and accuracy of object detection," 2020, <https://arxiv.org/abs/2004.10934>.
- [22] J. Redmon and A. Farhadi, "Yolov 3: an incremental improvement," 2018, <https://arxiv.org/abs/1804.02767>.
- [23] K. Oksuz, B. C. Cam, S. Kalkan, and E. Akbas, "Imbalance problems in object detection: a review," 2019, <https://arxiv.org/abs/1909.00169>.
- [24] T. Lin, P. Goyal, R. B. Girshick, K. He, and P. Dollár, "Focal loss for dense object detection," in *2017 IEEE International Conference on Computer Vision (ICCV)*, pp. 2999–3007, Venice, Italy, 2017.
- [25] C. Zhu, Y. He, and M. Savvides, "Feature selective anchor-free module for single-shot object detection," in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 840–849, Long Beach, CA, USA, 2019.
- [26] P. Dollár, C. Wojek, B. Schiele, and P. Perona, "Pedestrian detection: an evaluation of the state of the art. IEEE trans," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 34, pp. 743–761, 2012.
- [27] S. Zhang, R. Benenson, and B. Schiele, "Citypersons: a diverse dataset for pedestrian detection," in *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 4457–4465, Honolulu, HI, USA, 2017.
- [28] G. Brazil, X. Yin, and X. Liu, "Illuminating pedestrians via simultaneous detection and segmentation," in *2017 IEEE International Conference on Computer Vision (ICCV)*, Venice, Italy, 2017.
- [29] C. Zhou, M. Wu, and S. K. Lam, "Ssa-cnn: semantic self-attention cnn for pedestrian detection," 2019, <https://arxiv.org/abs/1902.09080>.
- [30] X. Wang, T. Xiao, Y. Jiang, S. Shao, J. Sun, and C. Shen, "Repulsion loss: detecting pedestrians in a crowd," 2017, <https://arxiv.org/abs/1711.07752>.
- [31] S. Zhang, L. Wen, X. Bian, Z. Lei, and S. Z. Li, "Occlusion-aware R-CNN: detecting pedestrians in a crowd," in *Computer*



- Vision – ECCV 2018*, V. Ferrari, M. Hebert, C. Sminchisescu, and Y. Weiss, Eds., vol. 11207 of Lecture Notes in Computer Science, pp. 657–674, Springer, Cham, 2018.
- [32] J. Yu, Y. Jiang, Z. Wang, Z. Cao, and T. S. Huang, “Unitbox: an advanced object detection network,” in *Proceedings of the 24th ACM international conference on Multimedia*, pp. 516–520, Amsterdam, the Netherlands, 2016.
- [33] L. Huang, Y. Yang, Y. Deng, and Y. Yu, “Densebox: unifying landmark localization with end to end object detection,” 2015, <https://arxiv.org/abs/1509.04874>.
- [34] X. Zhou, J. Zhuo, and P. Krähenbühl, “Bottom-up object detection by grouping extreme and center points,” in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 850–859, Long Beach, CA, USA, 2019b.
- [35] A. G. Howard, M. Zhu, B. Chen et al., “Mobilenets: efficient convolutional neural networks for mobile vision applications,” 2017, <https://arxiv.org/abs/1704.04861>.
- [36] K. Simonyan and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” in *3rd International Conference on Learning Representations, ICLR 2015*, San Diego, CA, USA, 2015.
- [37] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” in *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 770–778, Las Vegas, NV, USA, 2016.
- [38] G. Huang, Z. Liu, L. van der Maaten, and K. Q. Weinberger, “Densely connected convolutional networks,” in *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 2261–2269, Honolulu, HI, USA, 2017.
- [39] K. He, G. Gkioxari, P. Dollár, and R. B. Girshick, “Mask R-CNN,” in *2017 IEEE International Conference on Computer Vision (ICCV)*, pp. 2980–2988, Venice, Italy, 2017.
- [40] J. Mao, T. Xiao, Y. Jiang, and Z. Cao, “What can help pedestrian detection?,” in *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 6034–6043, Honolulu, HI, USA, 2017.
- [41] Z. Cai and N. Vasconcelos, “Cascade R-CNN: high quality object detection and instance segmentation,” 2019, <https://arxiv.org/abs/1906.09756>.
- [42] S. Zhang, R. Benenson, M. Omran, J. H. Hosang, and B. Schiele, “How far are we from solving pedestrian detection?,” in *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 1259–1267, Las Vegas, NV, USA, 2016b.
- [43] Z. Zou, Z. Shi, Y. Guo, and J. Ye, “Object detection in 20 years: a survey,” 2019, <https://arxiv.org/abs/1905.05055>.

## Research Article

# Traceable Multiauthority Attribute-Based Encryption with Outsourced Decryption and Hidden Policy for CIoT

Suhui Liu <sup>1</sup>, Jiguo Yu <sup>2,3,4</sup>, Chunqiang Hu <sup>5,6</sup> and Mengmeng Li<sup>1</sup>

<sup>1</sup>School of Computer Science, Qufu Normal University, Rizhao, 276826 Shandong, China

<sup>2</sup>School of Computer Science and Technology, Qilu University of Technology (Shandong Academy of Sciences), Jinan, Shandong 250353, China

<sup>3</sup>Shandong Computer Science Center (National Supercomputer Center in Jinan), Jinan, Shandong 250014, China

<sup>4</sup>Shandong Laboratory of Computer Networks, Jinan 250014, China

<sup>5</sup>School of Big Data and Software Engineering, Chongqing University, Chongqing 400044, China

<sup>6</sup>Key Laboratory of Dependable Service Computing in Cyber Physical Society, Ministry of Education (Chongqing University), China

Correspondence should be addressed to Jiguo Yu; [jiguoyu@sina.com](mailto:jiguoyu@sina.com) and Chunqiang Hu; [chu@cqu.edu.cn](mailto:chu@cqu.edu.cn)

Received 31 October 2020; Revised 1 January 2021; Accepted 7 April 2021; Published 21 April 2021

Academic Editor: Yingjie Wang

Copyright © 2021 Suhui Liu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Cloud-assisted Internet of Things (IoT) significantly facilitate IoT devices to outsource their data for high efficient management. Unfortunately, some unsettled security issues dramatically impact the popularity of IoT, such as illegal access and key escrow problem. Traditional public-key encryption can be used to guarantees data confidentiality, while it cannot achieve efficient data sharing. The attribute-based encryption (ABE) is the most promising way to ensure data security and to realize one-to-many fine-grained data sharing simultaneously. However, it cannot be well applied in the cloud-assisted IoT due to the complexity of its decryption and the decryption key leakage problem. To prevent the abuse of decryption rights, we propose a multiauthority ABE scheme with white-box traceability in this paper. Moreover, our scheme greatly lightens the overhead on devices by outsourcing the most decryption work to the cloud server. Besides, fully hidden policy is implemented to protect the privacy of the access policy. Our scheme is proved to be selectively secure against replayable chosen ciphertext attack (RCCA) under the random oracle model. Some theory analysis and simulation are described in the end.

## 1. Introduction

In traditional public key encryption schemes, the encryptor encrypts the message with the public key of the decryptor; hence, only the decryptor who owns the corresponding decryption key can decrypt the data. In other words, this type of scheme relies on the public key certificate system which we all know is pretty difficult to manage. In 1984, Shamir first proposed the identity-based encryption (IBE) where the encryptor uses the identity of the decryptor as his/her public key [1]. In [2], Boneh et al. proposed an IBE using the elliptic curve pairing, which greatly promoted the development of this field. Although the IBE solves the public key management problem, it still cannot achieve one-to-many private data sharing. Unfortunately, this kind of application is

extremely common in ubiquitous Internet of Things (IoT) scenarios.

To tackle this issue, Sahai et al. first proposed a fuzzy identity encryption scheme [3], which is later developed into the attribute-based encryption (ABE). There are two types of ABE, the first one is named as ciphertext-policy attribute-based encryption (CP\_ABE) and the other one is key-policy attribute-based encryption (KP\_ABE). CP\_ABE was proposed by Waters, in which the encryptor needs to know nothing about who can decrypt the ciphertext exactly, and he/she just encrypts the message with a self-defined access policy [4]. Any decryptor can decrypt correctly as long as its attribute set meets the access policy in the ciphertext. In other words, in CP\_ABE schemes, data owners own the right to design who can decrypt fully.

IoT, which acts as the bridge between the physical world and the cyber world, enables the creation of a bunch of smart applications [5], such as smart city, smart industry, and smart health care system. Considering that most IoT devices are resource constrained and cannot handle the huge amount of data locally and efficiently, the cloud storage server is included in the IoT and forms a new paradigm, the cloud-IoT, where the cloud or a resource-adequated server provides useful services like storage and computing. ABE schemes with a single attribute authority do not adequately address the needs of the ubiquitous IoT devices properly. In [6], Chase first proposed a multiauthority ABE scheme. However, Chase's scheme still requires the trusted central authority (CA), which can decrypt any ciphertext that it wants to decrypt. Later, Chase et al. improve their scheme by removing the CA and achieve a truly decentralized ABE scheme [7].

In [8], Lewko et al. proposed a distributed ABE scheme, which not only realizes multiauthority attribute-based encryption (MAABE) but also proves the system security with dual system encryption methodology. Unfortunately, the application of ABE in IoT still faces an important challenge: IoT devices with limited resources cannot afford the huge number of bilinear pairing operations in ABE schemes. Therefore, Green et al. proposed an outsourced ABE scheme which ensures the data security while minimizing the computational burden of equipments [9].

In this paper, a multiauthority attribute-based encryption scheme with white-box traceability and verifiable outsourced decryption was proposed for cloud IoT. Compared with the existing ABE schemes, our scheme has the following contributions:

- (i) As there is a great quantity of attributes used in the decryption key generation, each attribute authority controls a set of disjoint attributes independently in our scheme. The central authority is only responsible for generating the public parameters, and the right to decide who can decrypt is hold by the data owners directly
- (ii) Our scheme uses the linear secret sharing schemes (LSSS) to allow any monotone access structures. More importantly, to protect the privacy of IoT users, our scheme realizes fully hidden access policy
- (iii) Considering the needs of resource-constrained IoT devices, our scheme outsources most decryption works to the cloud by the verifiable outsourcing technology
- (iv) Our scheme adopts the Boneh-Boyen short signature algorithm to implement the user traceability mechanism. In other words, we use a white-box trace algorithm to tackle the private key leaking issue

*1.1. Paper Organization.* Section 2 summarizes many related works, and Section 3 introduces all preliminaries of our scheme including some complexity assumptions. The system model and security models are presented in Section 4. In Section 5, we propose the concrete construction and a simple

application of our scheme. Section 6 outlines the proof of indistinguishability, verifiability, fully hiding, and traceability of our scheme. We compare our scheme with some other schemes about the storage and computation costs in Section 7. Section 8 contains the conclusion.

## 2. Related Work

Many works have been proposed since Sahai et al. first proposed the attribute-based encryption [3]. ABE schemes can be classified into two categories generally: the key-policy attribute-based encryption (KP\_ABE) and the ciphertext-policy attribute-based encryption (CP\_ABE) [4, 16]. Because CP\_ABE allows the data owner to decide the access policy, it has been treated as the most promising solution to solve the access control issue in the cloud storage. In ABE schemes, the key pair of data users is generated by attribute authorities (AAs). Thus, the security of ABE schemes is based on the trust of the attribute authorities. To tackle the huge amount of data users contained in IoT, multiauthority attribute-based encryption (MA\_ABE) was proposed, which can manage the huge amount of attributes in a more efficient way [6, 17–19], where each attribute authority controls an unique set of attributes independently. To achieve both the data confidentiality and the data authentication in the body area network, Hu et al. proposed a fuzzy attribute-based signcryption scheme [20].

Another characteristic of IoT is that most devices are resource-limited [21–23]. As we all know that the decryption overhead of ABE schemes rises along with the attribute number involved in the access policy. Obviously the expensive pairing computations are unacceptable for most IoT devices. Therefore, some ABE schemes using the proxy reencryption concept have been proposed [24–26]. In [9], Green et al. proposed an outsourced ABE scheme, which outsources most decryption overheads to a trusted third-party server, but outsourced ABE schemes all rely on a semitrusted server to semidecrypt that leads to a serious problem: how to ensure the semidecrypted data is correct and not altered. In [27], Lai et al. proposed a verifiable outsourced ABE while this scheme requires heavy costs for decryption. Recently, Li et al. improved an ABE scheme to achieve not only verifiable outsourced decryption but also lightweight user decryption [10], but all outsourced schemes mentioned above rely on a central authority to manage and generate user decryption key. In [11], Belguith et al. proposed an outsourced multiauthority attribute-based encryption scheme. In [28], Deng et al. proposed an efficient outsourced attribute-based signcryption scheme which also solves the user revocation problem.

In the cloud-assisted IoT environment, data owners store private data in the shared cloud. In most ABE schemes, the access policy is uploaded to the cloud server in plaintext along with the encrypted data. This may reveal private information of the encryptor and the decryptor. In [29], Nishide et al. proposed an ABE scheme with partially hidden access policy, but this scheme has poor expressiveness.

When it comes to application in the real world, a common issue of ABE schemes needs to be considered: the leakage of

decryption keys. In other words, how to trace/recover the global identity of the guilty user who leaks its secret key to a malicious or illegal user. There are two tracing approaches, white-box traceability and black-box traceability, that can be used to solve this issue. In [30], Hinek et al. used the Boneh-Boyen signature [31] to achieve the white-box traceability. Liu et al. proposed a white-box traceable ABE [32] and a black-box traceable ABE with highly expression [33]. In [12], Liu et al. proposed a traceable and revocable ABE scheme which is more practical for real application. In [34], Yu et al. proposed a traceable ABE scheme with white-box traceability to manage data stored in the cloud storage. In [13], an efficient large-universe MA\_CP\_ABE with white-box traceability was proposed. While in [35], Qiao et al. proposed a traceable ABE scheme with black-box traceability for fog computing.

All traceable ABE schemes mentioned above have a shared issue: their decryption computation burden are intolerable for IoT devices. In [14], an ABE scheme with outsourced decryption designed for electronic health systems was proposed by Li et al. However, Li's scheme did not consider the privacy of access policies which might contain sensitive personal information of users. We compare our scheme with some existed ABE schemes in Table 1. In a word, our ABE scheme achieves selective replayable CCA security and provides multiple practical functions, such as fully hidden policy, outsourced decryption, and traceability.

### 3. Preliminaries

In this section, we provide all mathematical preliminaries needed for our scheme.

**3.1. Bilinear Maps.** Let  $\mathbb{G}$  and  $\mathbb{G}_T$  be two multiplicative cyclic groups of prime order  $p$ . Let  $g$  be a generator of  $\mathbb{G}$  and  $e$  be a bilinear map,  $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ , with the following three properties [15]:

- (1) Bilinearity: for all  $u, v \in \mathbb{G}$  and  $a, b \in \mathbb{Z}_p$ , we have  $e(u^a, v^b) = e(u, v)^{ab}$ , where  $\mathbb{Z}_p$  is the integers modulo  $p$
- (2) Nondegeneracy:  $e(g, g) \neq 1$ , where 1 is the unit of  $\mathbb{G}_T$
- (3) Computability: there is a polynomial time algorithm to efficiently compute  $e(u, v)$  for any  $u, v \in \mathbb{G}$

We say  $\mathbb{G}$  is a bilinear group if the group operation in  $\mathbb{G}$ , and the bilinear map  $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$  is both efficiently computable. Notice that the map  $e$  is symmetric since  $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$ .

### 3.2. Access Structure

**Definition 1.** (access structure). Let  $P = \{P_1, \dots, P_n\}$  be a set of parties. A collection  $\mathbb{A} \subseteq 2^{\{P_1, \dots, P_n\}}$  is monotone if  $\forall B, C : \text{if } B \in \mathbb{A} \text{ and } B \subseteq C, \text{ then } C \in \mathbb{A}$ . An access structure is a collection  $\mathbb{A}$  of nonempty subsets of  $\{P_1, \dots, P_n\}$ , such as  $\mathbb{A} \subseteq$

$2^{\{P_1, \dots, P_n\}} \setminus \emptyset$ . The sets in  $\mathbb{A}$  are called authorized sets, and the sets not in  $\mathbb{A}$  are called unauthorized sets [9].

### 3.3. Linear Secret Sharing Schemes (LSSS)

**Definition 2.** (linear secret sharing schemes (LSSS)). A secret-sharing scheme  $\prod$  over a set of parties  $\mathbb{P}$  is called linear over  $\mathbb{Z}_p$  if

- (1) The shares of a secret  $s \in \mathbb{Z}_p$  for each party form a vector over  $\mathbb{Z}_p$
- (2) There exists a matrix  $\mathbb{M}$  with  $l$  rows and  $n$  columns called the share-generating matrix for  $\prod$  and a function  $\rho$  which maps each row of the matrix to an associated party. That is, for  $i = 1, \dots, l$ , the value  $\rho(i)$  is the party associate with the row  $i$ . When we consider the column vector  $v = (s, r_2, \dots, r_n)$  where  $r_2, \dots, r_n \in \mathbb{Z}_p$  is randomly chosen, then  $\mathbb{M}v$  is the vector of  $l$  shares of the secret  $s$  according to  $\prod$ . The share  $(\mathbb{M}v)_i$  belongs to the party  $\rho(i)$

According to [9], every linear secret-sharing scheme based on the above definition also enjoys the linear reconstruction property defined as follows: Let  $\prod$  be an LSSS for the access structure  $\mathbb{A}$ . Let  $S \in \mathbb{A}$  be any authorized set, and let  $I \subset \{1, 2, \dots, l\}$  be defined as  $I = \{i : \rho(i) \in S\}$ . Then, there exist constants  $\{\omega_i \in \mathbb{Z}_p\}_{i \in I}$  such that if  $\{\lambda_i\}$  are valid shares of any secret  $s$  according to  $\prod$ , then  $\sum_{i \in I} \omega_i \lambda_i = s$ . It is shown in [9] that these constants  $\{\omega_i\}$  can be found in polynomial time in the size of the share-generating matrix  $\mathbb{M}$ .

**3.4. One-Way Anonymous Key Agreement.** One-way anonymous key agreement [15] scheme can be used to guarantee anonymity of the access structure. This scheme only ensures the anonymity of one participant. Assume that there are two participants Alice ( $ID_A$ ) and Bob ( $ID_B$ ) in this scheme. And the master secret of the key generation center (KGC) is  $s$ . When Alice wants to keep anonymity, the process is listed as follows:

- (1) Alice calculates  $Q_B = H(ID_B)$ . A random number  $r_a \in \mathbb{Z}_p^*$  is chosen to generate the pseudonym  $P_A = Q_A^{r_a}$  and computes the session key  $K_{A,B} = e(d_A, Q_B)^{r_a} = e(Q_A, Q_B)^{s \cdot r_a}$ . Finally, she sends her pseudonyms  $P_A$  to Bob
- (2) Bob uses his secret key  $d_B$  to calculate the session key  $K_{A,B} = e(P_A, d_B) = e(Q_A, Q_B)^{s \cdot r_a}$ , where  $d_i = H(ID_i)^s \in \mathbb{G}$  is his private key for  $i \in \{A, B\}$ , and  $H : \{0, 1\}^* \rightarrow \mathbb{G}$  is a strong collision-resistant hash function

### 3.5. Complexity Assumptions

**Definition 3.** Strong Diffie Hellman problem (q-SDH). Let  $\mathbb{G}$  be a multiplicative cyclic group of order  $p$  with a generator  $g$ . Given a random  $x \in \mathbb{Z}_p^*$  and a  $q + 1$  tuple  $(g, g^x, g^{x^2}, \dots, g^{x^q})$ ,

TABLE 1: Function comparison.

Scheme	[10]	[11]	[12]	[13]	[14]	[15]	Our scheme
Multiauthority	No	Yes	No	Yes	No	Yes	Yes
Access policy	AND gates	LSSS	LSSS	LSSS	LSSS	LSSS	LSSS
Fully hidden policy	No	No	No	No	No	Yes	Yes
Outdecryption	Yes	Yes	No	No	Yes	No	Yes
Security	RCCA	Selective RCPA	Selective CPA	Static security	Selective CPA	Selective CPA	Selective RCCA
Traceability	No	No	Yes	Yes	Yes	No	Yes

the problem of computing a pair  $(c, g^{1/x+c})$ , where  $c \in \mathbb{Z}_p^*$ , is called the  $q$ -strong Diffie Hellman problem [13].

*Definition 4.* Computational Diffie Hellman problem (CDH). Let  $\mathbb{G}$  be a multiplicative cyclic group of order  $p$  with a generator  $g$ . Given two group elements  $g^a, g^b \in \mathbb{G}$  where  $a, b \in \mathbb{Z}_p$  are two random integers. The problem of calculating  $g^{ab}$  from  $g^a$  and  $g^b$  is called Computational Diffie Hellman problem [11].

*Definition 5.* Decisional Bilinear Diffie Hellman problem (DBDH). Let  $\mathbb{G}$  be a multiplicative cyclic group of order  $p$  with a generator  $g$ . Given three group element  $g^a, g^b$ , and  $g^c \in \mathbb{G}$  where  $a, b$ , and  $c \in \mathbb{Z}_p^*$  are three random integers. The problem of distinguishing tuples of the form  $(g^a, g^b, g^c, e(g, g)^{abc})$  and  $(g^a, g^b, g^c, e(g, g)^z)$  for some random integer  $z$  is called the Decisional Bilinear Diffie Hellman problem [11].

## 4. System Definition

*4.1. System Model.* The system model of our scheme is illustrated in Figure 1, and the associated five entities are described as follows:

- (1) Central Trusted Authority (CTA): the CTA is only used to generate the public parameter, and it cannot decrypted any data
- (2) Attribute authorities (AAs): each AA controls a set of attributes. Multiple attribute authorities work together to generate the user's decryption key. Besides, attribute authorities can use a trace algorithm to recover the global identity of the guilty user who leaks its private decryption key
- (3) Cloud storage service provider (CS): the CS is responsible to store the encrypted data. Moreover, CS performs the outsourcing decryption for users
- (4) Data owner (DO): the owner of the data which is responsible to encrypt and upload the data to CS
- (5) Data user (DU): the party who wants to access data

Table 2 summarizes notations used in our scheme. Assume that there are  $n$  authorities in our scheme and each

attribute is associated with an unique AA, such that  $S_{A,AA_i} \cap S_{A,AA_j} = \emptyset$  for  $\forall i, j$  and  $\bigcup S_{A,AA_j} = S_A$ .

*4.2. System Procedure.* Our MAABE scheme with outsourced decryption and hidden policy contains the following five phases:

- (1) *System initialization* : this phase includes two algorithms. Firstly, the CTA runs the  $setup(\lambda) \rightarrow PP$  algorithm to generate the global parameters  $PP$ , where  $\lambda$  is the security parameter. Then, each AA runs the  $Setup_{auth}(PP) \rightarrow (sk_{AA_j}, pk_{AA_j})$  algorithm to generate their own key pairs, which is consisted with a private key and a public key
- (2) *Encryption* : the DO runs the  $Encrypt(PP, \{pk_{AA_j}\}, MSG, (\mathbb{M}, \rho)) \rightarrow CT$  algorithm to encrypt the message  $MSG$ , and then it uploads the ciphertext to the cloud server
- (3) *Keygeneration* : this phase contains two algorithms. Firstly, each related AA runs the  $Keygen(PP, \{sk_{AA_j}, pk_{AA_j}\}, \text{GID}, S_{\text{GID},j}) \rightarrow sk_{\text{GID},j}$  algorithm independently to generate the decryption key for the DU with identity  $\text{GID}$ . Then, all results are sent to the user

To outsource the decryption work to the cloud, the user runs the  $Keygen_{out}(PP, sk_{\text{GID}}, (\mathbb{M}, \rho), CT) \rightarrow ok_{\text{GID}}$  algorithm to generate its outsourced decryption key.

- (4) *Decryption* : this phase is divided into two steps. Firstly, the CS runs the  $Decrypt_{out}(PP, ok_{\text{GID}}, (\mathbb{M}, \rho), CT) \rightarrow CT'$  algorithm to partially decrypt the ciphertext. The second step is performed by the user, who runs the  $Decrypt(CT', osk_{\text{GID}}) \rightarrow MSG$  algorithm to get the plaintext
- (5) *Trace* : to begin with, each  $AA_j$  verifies the format of the decryption key that needed to be traced, and then it runs the  $Trace(PP, sk_{\text{GID}}, \{pk_{AA_j}\}) \rightarrow \text{GID}$  algorithm to output the global identity ( $\text{GID}$ ) of the guilty user

*4.3. Security Models.* We define four security models of our MAABE scheme in this section.

- (1) *Confidentiality*: the confidentiality of data is the basic security requirement of a scheme, which is used to resist malicious adversaries to gain extral information from



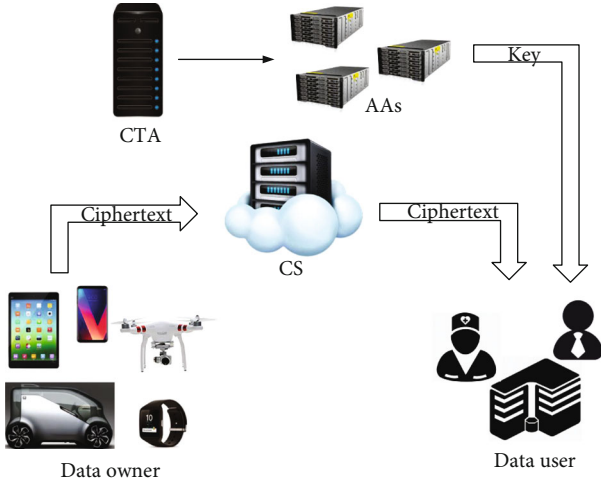


FIGURE 1: System model and procedure.

TABLE 2: Notations.

Notation	Meaning
$S_{AA}$	The universe set of attribute authorities
$S'_{AA}$	The set of corrupted attribute authorities
$S_{AA,GID}$	The set of attribute authorities related to the user GID
$S_A$	The universe set of attributes
$AA_j$	An attribute authority
$S_{A,AA_j}$	The attribute set controlled by $AA_j$
$GID$	The global identity of a user
$S_{GID}$	The attribute set related with user GID
$P$	The public parameter
$sk_{AA_j}$	Secret key related to $AA_j$
$pk_{AA_j}$	Public key related to $AA_j$
$MSG$	Message
$(M, \rho)$	The LSSS access matrix and its row label function
$\phi$	Access control structure
$S_\phi$	The attribute set related with $\phi$
$CT$	The ciphertext
$sk_{GID}$	The secret key of user $GID$
$ok_{GID}$	The outsourced decryption key ( $\{opk, osk\}$ )

the ciphertext. Our scheme adopts the replayable chosen-ciphertext security (RCCA) defined in [36] by Canetti et al. as this type of security is sufficient enough and not to be too strict. Two restrictions are followed in this experiment: all decryption key queries cannot satisfy the challenge access structure fixed in the initialization phase by the adversary. And the attribute authorities can only be corrupted statically by the adversary.

The selective secure against chosen ciphertext attack of our scheme is achieved if no probabilistic polynomial time

(PPT) adversary can win the  $\text{Exp}^{\text{Conf}}$  security experiment described in Figure 2 between an adversary  $\mathbb{A}$  and a challenger  $\mathbb{C}$  with nonnegligible advantage.

(2) *Verifiability*: our scheme is verifiable if there is no PPT adversary that can win the  $\text{Exp}^{\text{Verif}}$  security experiment described in Figure 3 between an adversary  $\mathbb{A}$  and a challenger  $\mathbb{C}$  with nonnegligible advantage.

(3) *Fully hidden*: in our scheme, the CS knows nothing about the access policy, and the user only knows if his/her attributes satisfy the access policy. Our scheme is an outsourced ABE with fully hidden policy if there is no PPT adversary that can win the  $\text{Exp}^{\text{Hide}}$  security experiment described in Figure 4 between an adversary  $\mathbb{A}$  and a challenger  $\mathbb{C}$  with nonnegligible advantage. The goal of the adversary is to recover the correct access policy without the required decryption key.

(4) *Traceability*: our scheme is a traceable ABE if there is no PPT adversary can win the  $\text{Exp}^{\text{Trace}}$  security experiment described in Figure 5 between an adversary  $\mathbb{A}$  and a challenger  $\mathbb{C}$  with nonnegligible advantage.

*Definition 6.* An outsourced ABE scheme is RCCA-secure against static corruption of the attribute authorities if  $\text{Adv}_{\mathbb{A}}[\text{Exp}^{\text{Conf}}(1^\xi)]$  is negligible for all PPT adversaries.

*Definition 7.* An outsourced ABE scheme is verifiable if  $\text{Adv}_{\mathbb{A}}[\text{Exp}^{\text{Verif}}(1^\xi)]$  is negligible for all PPT adversaries.

*Definition 8.* An outsourced ABE scheme achieves policy private if  $\text{Adv}_{\mathbb{A}}[\text{Exp}^{\text{Priv}}(1^\xi)]$  is negligible for all PPT adversaries.

*Definition 9.* An outsourced ABE scheme is traceable if  $\text{Adv}_{\mathbb{A}}[\text{Exp}^{\text{Trace}}(1^\xi)]$  is negligible for all PPT adversaries.

## 5. Construction and Application

The concrete construction of our MAABE scheme is presented in this section. Firstly, the CTA and all AA perform initialization and generate the PP and the public keys of AAs. Then, the DO can encrypt its data with an access structure. Before accessing the data, the DU needs to request its decryption key to the AAs. Next, the DU can access the data and decrypt successfully with the help of the cloud pre-decrypting for the DU first. Finally, the trace algorithm is used to reform the global identity of a guilty data user by the AAs. This section also contains a simple application in the end.

### 5.1. Concrete Construction

#### 5.1.1. Phase I: System Initialization

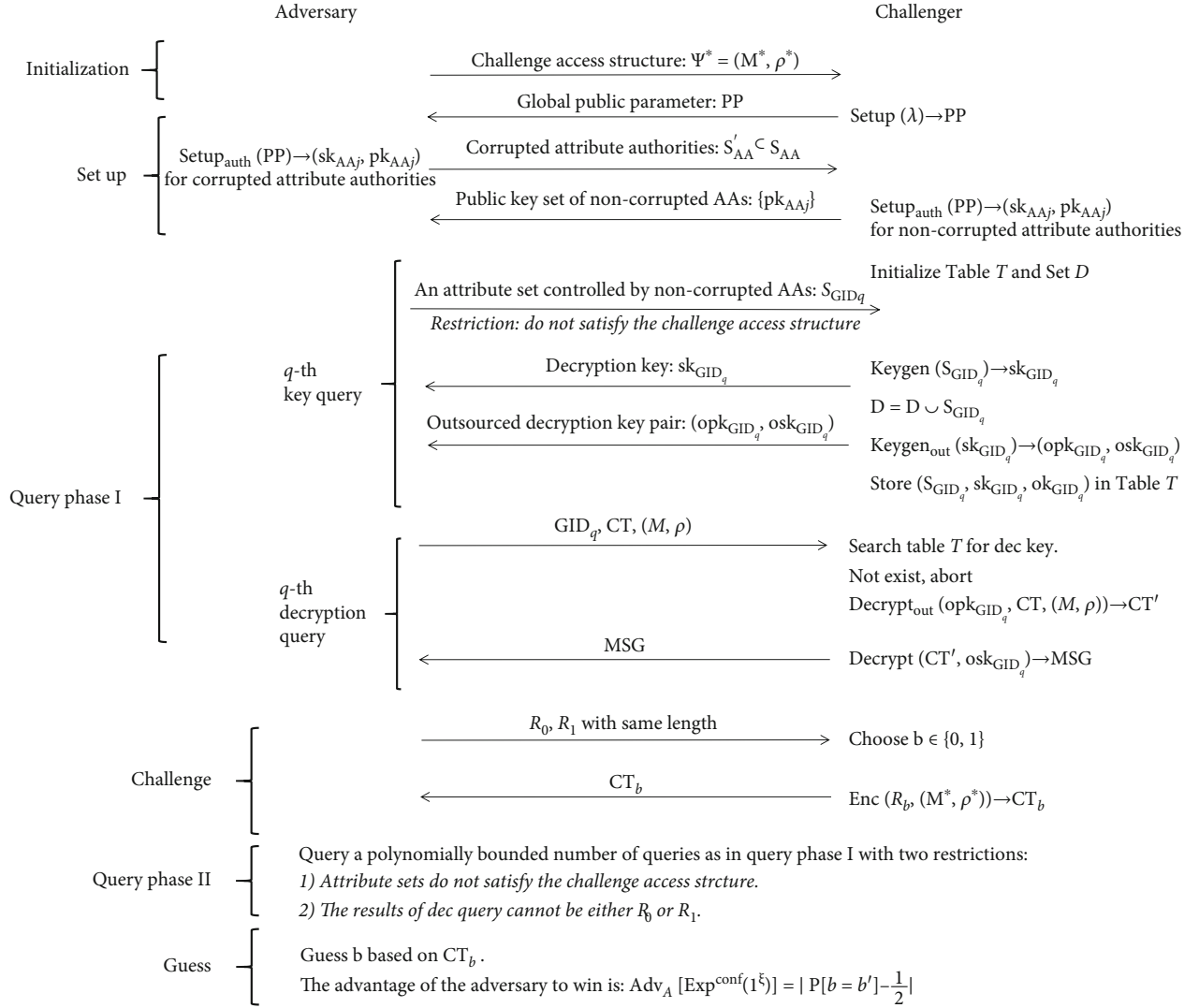


FIGURE 2: Confidentiality security model.

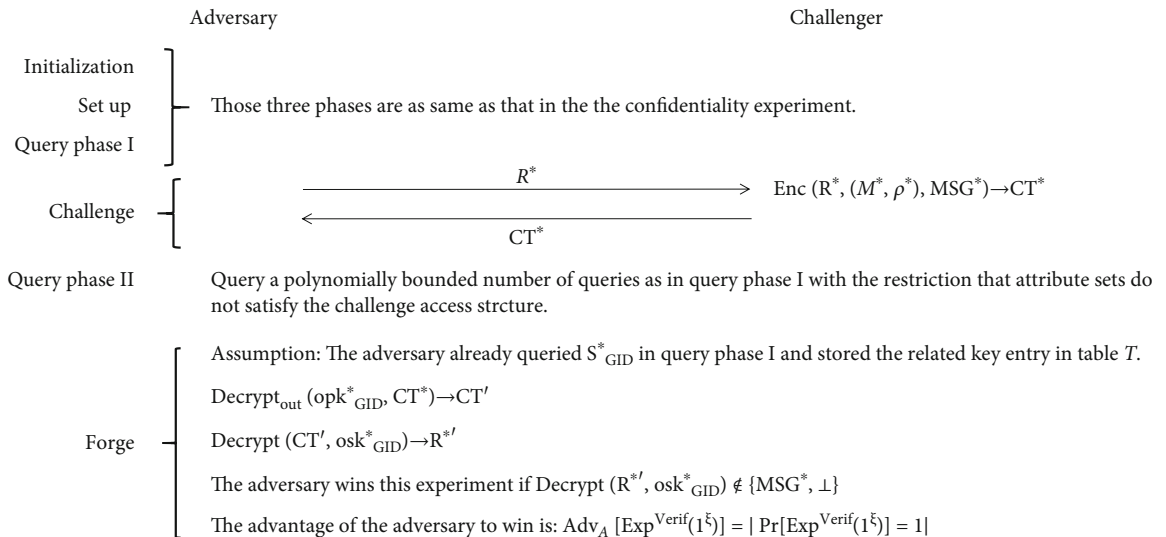


FIGURE 3: Verifiability security model.

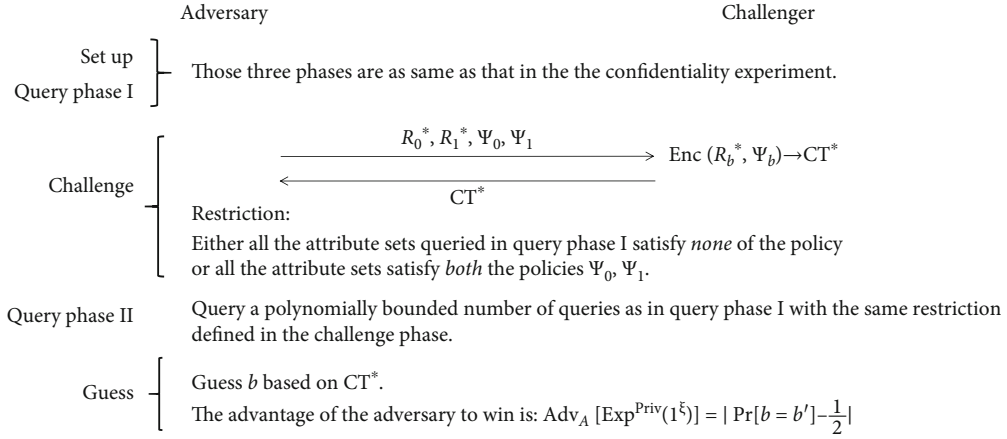


FIGURE 4: Fully hidden security model.

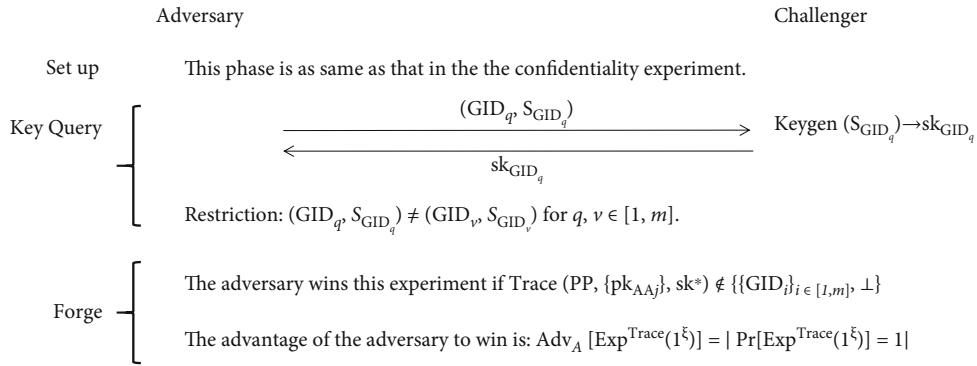


FIGURE 5: Traceability security model.

(1) *System set – up* : this step is performed by the CTA

It defines two multiplicative group  $\mathbb{G}, \mathbb{G}_T$  of prime order  $p$ , and  $g$  is a generator of  $\mathbb{G}$ .

It defines a symmetric bilinear map  $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ .

It defines three collusion resistant hash functions as follows:  $H : \{0, 1\}^* \rightarrow \mathbb{G}, H_1 : \{0, 1\}^* \rightarrow \mathbb{Z}_p^*, H_2 : \{0, 1\}^* \rightarrow \{0, 1\}^k$  where  $k$  is the length of the symmetric key.

It defines a CPA-secure symmetric encryption scheme  $(Enc_{sym}, Dec_{sym})$ .

It outputs the global public parameter PP:

$$PP = \{\mathbb{G}, \mathbb{G}_T, p, e, g, H, H_1, H_2, (Enc_{sym}, Dec_{sym})\} \quad (1)$$

(2) *Authority set – up* : each attribute authority performs this step to get their key pair. We take the  $A_{A_j}$  as an example

It chooses two random numbers  $\alpha_i, \beta_i \in \mathbb{Z}_p^*$  for each attribute  $i \in S_{A, AA_j}$ .

It chooses three random numbers  $h_j, a_j, b_j \in \mathbb{Z}_p^*$ .

It generates its pair of private key  $sk_{AA_j}$  and public key  $pk_{AA_j}$  as follows:

$$\begin{cases} sk_{AA_j} = (\{\alpha_i, \beta_i\}_{i \in S_{AA_j}}, h_j, a_j, b_j), \\ pk_{AA_j} = (\{g^{\alpha_i}, g^{\beta_i}\}_{i \in S_{AA_j}}, g^{h_j}, g^{a_j}, g^{b_j}). \end{cases} \quad (2)$$

**5.1.2. Phase II: Encryption.** We assume that the DO encrypts a message MSG with an self-defined access structure  $\Psi$ , and  $S_\Psi$  is the attribute set which contains all attributes in the access structure  $\Psi$ . This phase contains three steps defined below:

(1) *Fully Hide the access policy*

It chooses a random number  $a \in \mathbb{Z}_p^*$  and then computes  $q_i = e((g^{h_j})^a, H(i))$  where  $i \in S_\Psi$ .

It replaces each attribute in  $S_\Psi$  with the corresponding  $q_i$ .

It converts the access policy to a LSSS access matrix  $(\mathbb{M}_{l \times n}, \rho)$ .

(2) *Encrypt the key seed*

It chooses a random element  $R \in \mathbb{G}_T$  (the key seed) to calculate  $s = H_1(R, \text{MSG})$  and the symmetric key  $K_{\text{sym}} = H_2(R)$ .

It selects a  $p_i \in \mathbb{Z}_p$  for each row  $M_i$  of  $M$  and two random vectors  $\vec{v} = [s, v_1, \dots, v_n] \in \mathbb{Z}_p^n$ ,  $\vec{w} = [0, w_1, \dots, w_n] \in \mathbb{Z}_p^n$ .

It computes  $\lambda_i = M_i \times \vec{v}$  and  $w_i = M_i \times \vec{w}$ .

It outputs the tuple  $CT_{ABE} = (h, (M_{l \times n}, \rho), C_0, \{C_{1,i}, C_{2,i}, C_{3,i}, C_{4,i}, C_{5,i}\}_{i \in [1,l]})$  where  $i$  presents a matrix row corresponding to an attribute.

Details of the ciphertext are presented as follows:

$$CT = \begin{cases} h = g^a, \\ C_0 = \text{Re}(g, g)^s, \\ C_{1,i} = g^{\lambda_i} g^{\alpha_{\rho(i)} p_i}, \\ C_{2,i} = g^{p_i}, \\ C_{3,i} = g^{w_i} g^{\beta_{\rho(i)} p_i}, \\ C_{4,i} = g^{a_i p_i}, \\ C_{5,i} = g^{b_i p_i} \end{cases} \quad (3)$$

### (3) Encrypt the message

Uses  $K_{\text{sym}}$  to encrypt the message  $\text{MSG}$  by the symmetric encryption algorithm  $\text{Enc}_{\text{sym}}$  and denote the result as  $CT_{\text{sym}} = \text{Enc}_{\text{sym}}(K_{\text{sym}}, \text{MSG})$ .

It uploads  $CT = \{CT_{ABE}, CT_{\text{sym}}\}$  to the CS.

### 5.1.3. Phase III: Key Generation

#### (1) Decryption key

Each user owns an unique global identity  $\text{GID} \in \mathbb{Z}_p^*$  and an attribute set  $S_{\text{GID}}$  where each attribute is associated with a designed attribute authority. Let  $S_{AA, \text{GID}}$  be the set of related attribute authorities. According to  $S_{AA, \text{GID}}$ , we divide  $S_{\text{GID}}$  into  $\{S_{\text{GID},j}\}_{j \in S_{AA, \text{GID}}}$ . When the user queries its decryption key, each related AA runs the key generation algorithm. We take the  $AA_j$  as an instance.

It chooses a random number  $r \in \mathbb{Z}_p^* \setminus \{-a_j + \text{GID}/b_j\}$  for each  $i \in S_{\text{GID},j}$ .

It computes and returns the decryption key  $sk_{\text{GID},j} = \{K_{1,i}, K_{2,i}, K_{3,i}\}_{i \in S_{\text{GID}}}$ :

$$\begin{cases} K_{1,i} = g^{\alpha_i/a_j + \text{GID} + b_j r} H(\text{GID})^{\beta_i/a_j + \text{GID} + b_j r}, \\ K_{2,i} = H(i)^{h_j}, \\ K_{3,i} = r. \end{cases} \quad (4)$$

The decryption key of the user  $\text{GID}$  is noted as

$$sk_{\text{GID}} = \left( \{sk_{\text{GID},j}\}_{j \in S_{AA, \text{GID}}}, \text{GID} \right) = \left( \{K_{1,i}, K_{2,i}, K_{3,i}\}_{i \in S_{\text{GID}}}, \text{GID} \right) \quad (5)$$

(2) Outsourced decryption key: the data user runs this algorithm

#### (a) Reconstructs the access policy

It computes  $q'_i = e(h, H(i)^{h_j}) = e(g^a, H(i)^{h_j}), \forall i \in S_{\text{GID}}$ .

It uses  $q'_i$  to replace the attribute  $i$  to get the attribute set  $S'_{\text{GID}}$ .

It gains the access structure  $(M_{l \times n}, \rho)$  from  $CT$ .

It identifies the set of attributes  $L' = \{i : (\rho(i) \cap S'_{\text{GID}})_{i \in [l]}\}$  required for the decryption.

#### (b) Generates the outdec key

Chooses a random number  $z \in \mathbb{Z}_p^*$  to compute the outsourced decryption key  $\{\text{ok}_{\text{GID}}\} = (\{\text{opk}_{\text{GID}}\}, \text{osk}_{\text{GID}})$  as

$$\begin{cases} \text{opk}_{\text{GID}} = (\text{GID}, \{K_{1,i}^{1/z}, K_{3,i}\}_{i \in L'}, g^{1/z}, H(\text{GID})^{1/z}), \\ \text{osk}_{\text{GID}} = z. \end{cases} \quad (6)$$

### 5.1.4. Phase IV: Decryption

(1) *Outsourced decryption* : the CS performs outsourced decryption for the user

It computes the following equation for each matrix row corresponding to an attribute  $i$ :

$$Q = \frac{e(g^{1/z}, C_{1,i}) e(H(\text{GID})^{1/z}, C_{3,i})}{e(K_{1,i}^{1/z}, C_{2,i}^{\text{GID}} C_{4,i} K_{5,i}^{K_{3,i}})} = \left( e(g, g)^{\lambda_i} e(H(\text{GID}), g)^{w_i} \right)^{1/z}. \quad (7)$$

It chooses a set of constants  $\{c_i\}_{i \in [1,l]} \in \mathbb{Z}_p$  such that  $\sum_i c_i M_i = [1, 0, \dots, 0]$ .

It Computes

$$\prod_{i=1}^l Q^{c_i} = \left( e(g, g)^{\sum_{i=1}^l \lambda_i c_i} e(g, H(\text{GID}))^{\sum_{i=1}^l w_i c_i} \right)^{1/z}, \quad (8)$$

where  $l$  is the row number of the access matrix.

It returns  $CT' = \prod_{i=1}^l Q^{c_i} = e(g, g)^{s/z}$  to the user.

(2) *User decryption*: this phase contains the following two steps

(a) Recovers the message  $R$  based on the partially decrypted ciphertext  $CT'$  by computing the following equation

$$R = \frac{C_0}{(CT')^{osk}} = \frac{C_0}{(e(g, g)^{s/z})^z} = \frac{C_0}{e(g, g)^s}. \quad (9)$$

(note that this equation costs one exponentiation only and no pairing performance.)

(b) Computes  $K_{\text{sym}} = H_2(R)$ ,  $\text{MSG} = \text{Dec}_{\text{sym}}(K_{\text{sym}}, C_{\text{sym}})$ , and  $s = H_1(R, \text{MSG})$

Judge if  $CT' = e(g, g)^{s/z}$ . If no, outputs  $\perp$ . Else, the user gains the right MSG.

Correctness of Equation (7):

*Proof.* First for each attribute  $i \in L'$ , the CS uses  $\{\text{opk}_{\text{GID}}\}$  to compute:

$$\begin{aligned} Q &= \frac{e(g^{1/z}, g^{\lambda_i} g^{\alpha_{\rho(i)} p_i}) e(H(\text{GID})^{1/z}, g^{\beta_{\rho(i)} p_i} g^{w_i})}{e(g^{\alpha_{\rho(i)}/z(a_j + \text{GID} + b, r)} H(\text{GID})^{\beta_{\rho(i)}/z(a_j + \text{GID} + b, r)}, (g^{p_i})^{\text{GID}} g^{a_i p_i} g^{b_i p_i r})} \\ &= \frac{e(g, g)^{\lambda_i/z} e(g, g)^{\alpha_{\rho(i)} p_i/z} e(g, H(\text{GID}))^{\beta_{\rho(i)} p_i/z} e(g, H(\text{GID}))^{w_i/z}}{e(g, g)^{\alpha_{\rho(i)} p_i/z} e(g, H(\text{GID}))^{\beta_{\rho(i)} p_i/z}} \\ &= e(g, g)^{\lambda_i/z} e(g, H(\text{GID}))^{w_i/z}. \end{aligned} \quad (10)$$

Then, it chooses a set of constants  $\{c_i\}_{i \in [1, l]} \in \mathbb{Z}_p$  such that  $\sum_i c_i \mathbb{M}_i = [1, 0, \dots, 0]$ . Because  $\lambda_i = \mathbb{M}_i \vec{v}$  and  $w_i = \mathbb{M}_i \vec{w}$ , so

$$\begin{aligned} \sum_{i=1}^l \lambda_i c_i &= \sum_{i=1}^l \mathbb{M}_i \vec{v} c_i = \vec{v} [1, 0, \dots, 0] = s, \\ \sum_{i=1}^l w_i c_i &= \sum_{i=1}^l \mathbb{M}_i \vec{w} c_i = \vec{w} [1, 0, \dots, 0] = 0. \end{aligned} \quad (11)$$

Hence, we can get

$$\begin{aligned} CT' &= \prod_{i=1}^l Q^{c_i} = \prod_{i=1}^l e(g, g)^{c_i \lambda_{\rho(i)}/z} e(g, H(\text{GID}))^{c_i w_i/z} \\ &= e(g, g)^{\sum_{i=1}^l c_i \lambda_{\rho(i)}/z} e(g, H(\text{GID}))^{\sum_{i=1}^l c_i w_i/z} \\ &= e(g, g)^{s/z} e(g, H(\text{GID}))^0 = e(g, g)^{s/z}. \end{aligned} \quad (12)$$

Then, based on  $CT'$ , the user recovers

$$R = \frac{C_0}{(CT')^{osk}} = \frac{\text{Re}(g, g)^s}{(e(g, g)^{s/z})^z} = \frac{\text{Re}(g, g)^s}{e(g, g)^s}. \quad (13)$$

**5.1.5. Phase V: Trace.** The  $\text{Trace}(\text{PP}, \text{sk}_{\text{GID}}, \{pk_{\text{AA}j}\})$  algorithm is performed by all attribute authorities. The input is the private key  $\text{sk}_{\text{GID}} = (\{\text{sk}_{\text{GID},j}\}_{j \in S_{\text{AA}}'}, \text{GID}) = (\{K_{1,i}, K_{2,i}, K_{3,i}\}_{i \in S_{\text{GID}}}, \text{GID})$  of a user.

Firstly, the AA checks the form of the key. If the key does not satisfies the form, this algorithm aborts.

Then, the AA searches its database to find if  $\exists i \in S_{\text{GID}}$ , s.t.

$$\begin{aligned} K_{1,i}, K_{2,i} &\in \mathbb{G}, K_{3,i}, \text{GID} \in \mathbb{Z}_p^*, \\ e(K_{1,i}, g^{a_i} g^{(b_j)^{K_{3,i}}} g^{\text{GID}}) &= e(g, g)^{\alpha_i} e(H(\text{GID}), g^{\beta_i}). \end{aligned} \quad (14)$$

If yes, the global identity  $\text{GID}$  of the guilty user will be output.

**5.2. Application in the EHR System.** In this section, we describe a simple application of our scheme based on the electronic health record (EHR) system. The basic procedures are presented in Figure 6, and the details are described as follows:

- (1) The central trusted authority (the government) performs the system set-up algorithm to generate and publish the global parameters  $\text{PP}$
- (2) A set of management companies act as attribute authorities, and each attribute authority needs to set up first. Then, they publish their public keys while keeping private keys secret
- (3) A hospital encrypts a patient's medical records  $\text{Rd}$  based on a user-defined access structure  $\mathbb{M}$  and sends the ciphertext  $CT$  along with the fully hidden access structure  $n$  to the cloud storing server to store

$$\text{Hospital} \xrightarrow{\text{Encrypt}(\text{Rd}, \mathbb{M}) \rightarrow CT} \text{Cloud}. \quad (15)$$

- (4) Before a data user (a doctor) requests the wanted records from the cloud server, he/she needs to get the decryption key  $\text{sk}_{\text{GID}}$  from the attribute authorities first
- (5) To outsource the decryption work to the cloud server, the doctor generates the outsourced decryption key  $\text{opk}_{\text{GID}}$  based on  $\text{sk}_{\text{GID}}$ . Then, he/she sends  $\text{opk}_{\text{GID}}$  to the cloud server
- (6) The cloud server will partially decrypt for the doctor as long as his/her attribute set satisfies the encryption



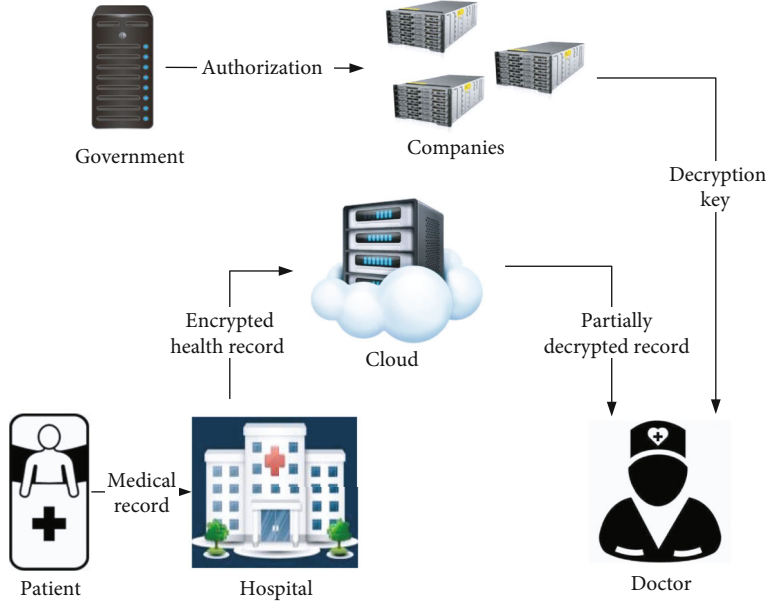


FIGURE 6: Application in an EHR system.

access structure. Then, the cloud sends the partially decrypted ciphertext  $CT'$  back to the doctor

$$\text{Cloud} \xrightarrow{\text{Decrypt}_{\text{out}}(\text{pk}_{\text{GID}}, \text{CT}) \rightarrow \text{CT}'} \text{Doctor}. \quad (16)$$

- (7) Finally, the doctor can fully decrypt and get the medical records. Note that doctors only require one exponentiation in  $\mathbb{G}_T$  to fully decrypt, and one hash operation to verify whether the ciphertext was tampered

$$\text{Decrypt}(CT') \rightarrow \text{Rd}. \quad (17)$$

- (8) If a malicious user decrypt illegally with a valid decryption key, the attribute authorities can perform the trace algorithm to recover the identity of the guilty user who leaks his/her decryption key to a illegal user

## 6. Security Analysis

### 6.1. Indistinguishability

**Theorem 1.** *If Lewko et al.'s scheme [8] is CPA=secure, our multiauthority attribute-based encryption scheme is selectively replayable CCA-secure according to Definition 6 such that  $\text{Adv}_A[\text{Exp}^{\text{Conf}}] < \text{Adv}_A[\text{Exp}^{\text{Lewko}}]$ .*

*Proof.* We define a PPT adversary  $\mathbb{A}$  running the experiment defined in Section 4.3(1) with an entity  $\mathbb{B}$ .  $\mathbb{B}$  running Lewko et al.'s CPA-secure [8] experiment with a challenger  $\mathbb{C}$ . The proof described below is going to show that the advantage of  $\mathbb{A}$  to win the experiment  $\text{Exp}^{\text{Conf}}$  is smaller than the advantage of  $\mathbb{B}$  to win Lewko et al.'s CPA-secure experiment  $\text{Exp}^{\text{Lewko}}$ . The detailed interactions are described as follows:

- (1) Initialization: the adversary  $\mathbb{A}$  submits a challenge access policy  $\Psi^* = (\mathbb{M}^*, \rho^*)$  to the challenge  $\mathbb{C}$  through  $\mathbb{B}$
- (2) Set-Up:  $\mathbb{C}$  runs the  $\text{Setup}(\lambda)$  algorithm to generate the global parameter  $\text{PP}$

It chooses two multiplicative cyclic groups  $\mathbb{G}, \mathbb{G}_T$  of prime order  $p$  with a generator  $g$  of  $\mathbb{G}$ .

It chooses a bilinear map  $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ .

It chooses three collusion-resistant hash functions  $H^* : \{0, 1\}^* \rightarrow \mathbb{G}, H_1^* : \{0, 1\}^* \rightarrow \mathbb{Z}_p^*, H_2^* : \{0, 1\}^* \rightarrow \{0, 1\}^k$ .

It chooses a cpa-secure symmetric encryption scheme  $(\text{Enc}_{\text{sym}}, \text{Dec}_{\text{sym}})$ .

It sends the global parameter  $\text{PP} = \{\mathbb{G}, \mathbb{G}_T, p, e, g, H^*, H_1^*, H_2^*, (\text{Enc}_{\text{sym}}, \text{Dec}_{\text{sym}})\}$  to  $\mathbb{A}$  through  $\mathbb{B}$ .

It runs the  $\text{Setup}_{\text{auth}}$  algorithm to generate the key pairs of the noncorrupted authorities:

It chooses two random numbers  $\alpha_i$  and  $\beta_i \in \mathbb{Z}_p^*$  for each attribute  $i \in S_{A, AA_j}$ .

It chooses three random numbers  $h_j, a_j,$  and  $b_j \in \mathbb{Z}_p^*$  to compute the public key  $\text{pk}_{AA_j} = (\{g^{\alpha_i}, g^{\beta_i}\}_{i \in S_{A, AA_j}}, g^{h_j}, g^{a_j}, g^{b_j})$ .

It sends all attribute authorities' public keys to  $\mathbb{A}$  through  $\mathbb{B}$ .

$\mathbb{A}$  runs the  $\text{Setup}_{\text{auth}}$  algorithm to generate the key pairs of the corrupted authorities in the same way.

- (3) Query phase I:  $\mathbb{B}$  initializes three empty tables  $\mathbb{T}$ ,  $\mathbb{T}_1$ ,  $\mathbb{T}_2$ , an empty set  $\mathbb{D}$ , and an integer  $j = 0$ . Details of queries are described as follows:

- (a) Hash query

$H_1^*$  oracle: if the entry  $(R, \text{MSG}, s)$  already existed in Table  $\mathbb{T}_1$ , return  $s$ . Otherwise, it chooses a random element  $s \in \mathbb{Z}_p^*$  ( $s$  is unique in Table  $\mathbb{T}_1$ ). Then, it records  $(R, \text{MSG}, s)$  in Table  $\mathbb{T}_1$  and returns  $s$ .

$H_2^*$  oracle: if the entry  $(R, K_{\text{sym}})$  already existed in Table  $\mathbb{T}_2$ , return  $K_{\text{sym}}$ . Otherwise, it chooses a random element  $K_{\text{sym}} \in \{0, 1\}^k$ . Then, it records  $(R, K_{\text{sym}})$  in Table  $\mathbb{T}_2$  and returns  $K_{\text{sym}}$ .

- (b) Key query: In the  $q$ -th query,  $\mathbb{A}$  queries the decryption key related with an attribute set  $S_{\text{GID}_q}$  by sending  $S_{\text{GID}_q}$  and  $\text{GID}_q$  to  $\mathbb{B}$ .  $\mathbb{B}$  calls  $\mathbb{C}$  to generate the decryption key and sends it to  $\mathbb{A}$ .  $\mathbb{C}$  chooses a random number  $r \in \mathbb{Z}_p^* \setminus \{-a_j + \text{GID}_q/b_j\}$  to compute the decryption key  $\text{sk}_{\text{GID}_q} = (\{\text{sk}_{\text{GID}_q, i}\}_{i \in S_{\text{AA}, \text{GID}}}, \text{GID}) = (\{K_{1,i}, K_{2,i}, K_{3,i}\}_{i \in S_{\text{GID}}}, \text{GID})$  while setting  $\mathbb{D} = \mathbb{D} \cup S_{\text{GID}_q}$

$$\begin{cases} K_{1,i} = g^{\alpha/a_j + \text{GID}_q + b_j} H^*(\text{GID}_q)^{t_i/a_j + \text{GID}_q + b_j}, \\ K_{2,i} = H^*(i)^{h_j}, \\ K_{3,i} = r. \end{cases} \quad (18)$$

$\mathbb{B}$  chooses a random element  $a \in \mathbb{Z}_p^*$  to compute  $h = g^a$  to simulate the output of the encryption algorithm.  $\mathbb{B}$  calls  $\mathbb{C}$  to run the outsourced decryption key generation algorithm:  $\mathbb{C}$  chooses a random number  $z \in \mathbb{Z}_p^*$  to compute

$$\begin{cases} \text{opk}_{\text{GID}_q} = (\{\{K_{1,i}^{1/z}\}_{i \in L'}\}, g^{1/z}, H^*(\text{GID})^{1/z}), \\ \text{osk}_{\text{GID}_q} = z. \end{cases} \quad (19)$$

Sends  $\text{ok}_{\text{GID}_q} = (\text{opk}_{\text{GID}_q}, \text{osk}_{\text{GID}_q})$  to  $\mathbb{B}$ .  $\mathbb{B}$  stores the entry  $(q, S_{\text{GID}_q}, \text{sk}_{\text{GID}_q}, \text{ok}_{\text{GID}_q})$  in the table  $\mathbb{T}$ . Finally,  $\mathbb{B}$  returns the key to  $\mathbb{A}$ .

- (c) Decryption query: without loss of generality, we assume that all ciphertexts input to this query have been partially decrypted. For instance, we assume that  $CT'$  was correctly decrypted by  $\text{opk}$  of the entry  $(q, S_{\text{GID}_q}, \text{sk}_{\text{GID}_q}, \text{ok}_{\text{GID}_q})$ . Let  $CT'$  be associated with a structure  $(\mathbb{M}, \rho)$  which is not equal with  $(\mathbb{M}^*, \rho^*)$ . Let  $\text{opk}$  be associated with a set of attributes which satisfies  $(\mathbb{M}, \rho)$  and not satisfies  $(\mathbb{M}^*, \rho^*)$

TABLE 3: Notations.

Notation	Meaning
$E, /E_T$	One exponentiation in group $\mathbb{G}/\mathbb{G}_T$
$P_e$	One pairing operation of the pairing function $e$ .
$N_e$	The row number of the encryption LSSS access matrix.
$N_u$	The attribute number of the user attribute set.
$N_d$	The attribute number required in decryption.
$N_a$	The attribute number of the attribute universe set.

Search Table  $\mathbb{T}_1$  to find if there exists an entry  $(R, \text{MSG}, s)$  which satisfies  $(CT')^{\text{osk}_{\text{GID}_q}} = e(g, g)^s$ . If not, abort. Else, obtain entry  $(R, K_{\text{sym}})$  in Table  $\mathbb{T}_2$ . If this entry does not exist, abort. Else, test if  $C_0 = \text{Re}(g, g)^s$  and  $CT_{\text{sym}} = \text{Enc}_{\text{sym}}(K_{\text{sym}}, \text{MSG})$ . If yes, output  $\text{MSG}$ . Else, abort.

- (4) Challenge:  $\mathbb{A}$  chooses two message  $\text{MSG}_1, \text{MSG}_2 \in \{0, 1\}^*$  with same length then sends them to  $\mathbb{B}$ .  $\mathbb{B}$  chooses two message  $R_0, R_1 \in \mathbb{G}_T$  with same length and then sends them to  $\mathbb{C}$ .  $\mathbb{C}$  chooses a random bit  $b \in \{0, 1\}$ , then  $\mathbb{C}$  encrypts  $R_b$  under the access structure  $(\mathbb{M}^*, \rho^*)$  by running Lewko's scheme. Finally,  $\mathbb{C}$  returns  $CT_{b, \text{ABE}}^*$  to  $\mathbb{B}$ .  $\mathbb{B}$  guesses  $b$  with advantage  $\text{Adv}_{\mathbb{A}}[\text{Exp}^{\text{Lewko}}]$ . Then,  $\mathbb{B}$  computes  $K_{\text{sym}}^* = H_2^*(R_b^*)$  and  $CT_{b, \text{sym}}^* = \text{Enc}_{\text{sym}}(K_{\text{sym}}^*, \text{MSG}_b)$ . Finally,  $\mathbb{B}$  returns  $CT_b^* = (CT_{b, \text{ABE}}^*, CT_{b, \text{sym}}^*)$  to  $\mathbb{A}$ .
- (5) Query phase II: the adversary  $\mathbb{A}$  can query a polynomially bounded number of queries as in query phase II after receiving the ciphertext  $CT_b^*$  with restrictions that the queried attribute set cannot satisfy the challenge access structure, and the response of the decryption query cannot be either  $\text{MSG}_0$  or  $\text{MSG}_1$ .
- (6) Guess:  $\mathbb{A}$  tries to guess  $b'$  based on  $CT_b^*$ . Then,  $\mathbb{A}$  sends  $b'$  to  $\mathbb{C}$  through  $\mathbb{B}$ . If  $b' = b$ , we say that  $\mathbb{A}$  wins this experiment.

We can easily get that the advantage of  $\mathbb{A}$  to win the experiment  $\text{Exp}^{\text{conf}}$  is smaller than the advantage of  $\mathbb{B}$  to win the experiment  $\text{Exp}^{\text{Lewko}}$ , because  $\mathbb{A}$  has to be based on the right  $CT_b^*$  provided by  $\mathbb{B}$  to guess  $b$  successfully. In other words,  $\Pr[\text{Exp}_{\mathbb{A}}^{\text{Lewko}}(1^\xi)] > \Pr[\text{Exp}_{\mathbb{A}}^{\text{Conf-Real}}(1^\xi)]$  and our scheme achieve selectively replayable CCA secure.

## 6.2. Verifiability

**Theorem 2.** *If  $H_1$  and  $H_2$  are two collision-resistant hash functions, our scheme is verifiable against malicious servers.*

*Proof.* We define a PPT adversary  $\mathbb{A}$  running the experiment defined in Section 4.3(2) with an entity  $\mathbb{B}$ .  $\mathbb{B}$  tries to break the collision resistance of the two hash functions  $H_1^*$  and  $H_2^*$ .

- (1) Initialization: the adversary  $\mathbb{A}$  submits a challenge access policy  $\Psi^* = (\mathbb{M}^*, \rho^*)$  to the entity  $\mathbb{B}$

TABLE 4: Storage cost comparison.

Scheme	[11]	[13]	[14]	Our scheme
Decryption key length	$2N_u  \mathbb{G} $	$3N_u  \mathbb{G}  + N_u  \mathbb{Z}_p^*  +  \mathbb{Z}_p $	$(2N_u + 3)  \mathbb{G}  + 2 \mathbb{Z}_p $	$2N_u  \mathbb{G}  + N_u  \mathbb{Z}_p $
Outdec key length	$(N_d + 2)  \mathbb{G}  +  \mathbb{Z}_p^* $	—	$(2N_u + 2)  \mathbb{G} $	$(N_d + 2)  \mathbb{G}  +  \mathbb{Z}_p^* $
Ciphertext length	$(3N_e + 1)  \mathbb{G}  + 1 \mathbb{G}_T $	$5N_e  \mathbb{G}  + (N_e + 1) \mathbb{G}_T $	$(3N_e + 2)  \mathbb{G}  + 1 \mathbb{G}_T $	$(5N_e + 1)  \mathbb{G}  + 1 \mathbb{G}_T $

(2) Set-up:  $\mathbb{B}$  runs the Setup algorithm to generate the global parameter except the two hash functions

(3)  $\mathbb{B}$  runs the Setup<sub>auth</sub> algorithm to generate keypairs of attribute authorities.

Query:  $\mathbb{A}$  runs the adversary queries as defined in query phase I and query phase II through  $\mathbb{B}$  to get the related decryption keys and outsourced decryption keys

(4) Challenge:  $\mathbb{A}$  sends the challenge message  $\text{MSG}^*$  to  $\mathbb{B}$ , and  $\mathbb{B}$  answers as follows

It chooses a random message  $R^* \in \mathbb{G}_T$  to run Lewko's encryption scheme to encrypt  $R^*$  under the access policy  $(\mathbb{M}^*, \rho^*)$ .

It computes  $s^* = H_1^*(R^* || \text{MSG}^*)$  and  $K_{\text{sym}}^* = H_2^*(R^*)$ .

It runs the symmetric encrypt algorithm to encrypt  $\text{MSG}^*$  to generate the ciphertext  $\text{CT}^* = (\text{CT}_{\text{ABE}}^*, \text{CT}_{\text{sym}}^*) = (h, C_0, \{C_{1,i}, C_{2,i}, C_{3,i}, C_{4,i}, C_{5,i}\}, \text{CT}_{\text{sym}}^*)$ .

It returns the ciphertext  $\text{CT}^* = (\text{CT}_{\text{ABE}}^*, \text{CT}_{\text{sym}}^*)$  to  $\mathbb{A}$ .

If  $\mathbb{B}$  can recover a message  $\text{MSG} \in \{\text{MSG}^*, \perp\}$ , then we say  $\mathbb{A}$  wins this experiment. Hence there are two cases are considered:

- (1)  $(\text{MSG}, R) \neq (\text{MSG}^*, R^*)$ , which means that  $\mathbb{B}$  finds a collision of the hash function  $H_1^*$
- (2)  $(K_{\text{sym}}, \text{CT}_{\text{sym}}) = (K_{\text{sym}}^*, \text{CT}_{\text{sym}}^*)$  but  $(R^* \neq R)$ , which means that  $\mathbb{B}$  breaks the collision resistance condition of  $H_2^*$  such as  $H_2^*(R) = K_{\text{sym}} = K_{\text{sym}}^* = H_2^*(R^*)$

In other words, since  $H_1$  and  $H_2$  are two collision-resistant hash functions, the outsourced decryption of our scheme is verifiable.

### 6.3. Fully Hiding

**Theorem 3.** *Our scheme is an outsourced ABE with fully hidden policy if the one-way anonymous key agreement protocol [15] is IND-CPA secure.*

*Proof.* The purpose of this proof is that no PPT adversary can recover the access policy without the right decryption key. The setup phase and the query phase 1 are same as the confidentiality experiment.

In the challenge phase, the adversary  $\mathbb{A}$  chooses two challenge messages  $R_0^*, R_1^*$  and two valid access policies  $\Psi_0, \Psi_1$ , and then it sends them to the challenger  $\mathbb{C}$ . Notice,  $\Psi_0$  and  $\Psi_1$  satisfy the following restriction: either all the attribute sets

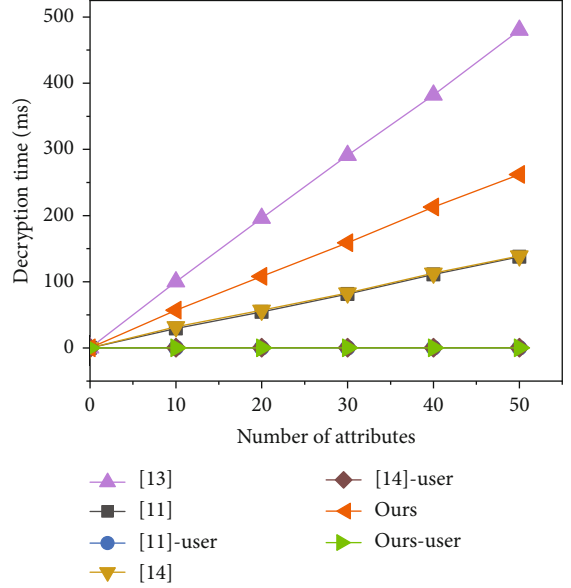


FIGURE 7: Decryption cost.

queried in query phase 1 satisfy none of the policy or all attribute sets satisfy both the policies. Then,  $\mathbb{C}$  computes  $q'(i) = e((g^{h_i})^a, H(i))$  based on the one-way anonymous key agreement protocol where  $a \in \mathbb{Z}_p^*$  is a random number. This step is used to hide the real policy by replacing each attributes in the policy with the corresponding  $q'(i)$ . Then,  $\mathbb{C}$  chooses a random bit  $b \in \{0, 1\}$  and encrypts the message  $R_b^*$  under the access policy  $\Psi_b$ . Finally,  $\mathbb{C}$  sends  $\text{CT}^*$  to  $\mathbb{A}$ . After that,  $\mathbb{A}$  still can query a polynomially bounded number of queries as in query phase I. The none-or-both principle still works in this phase.

In the guess phase,  $\mathbb{A}$  outputs  $b'$ .

When  $\mathbb{A}$  tries to decrypt  $\text{CT}^*$ , it has to recover the access policy first. In our scheme, the decryption key  $K_{2,i} = H(i)^{h_i}$  is necessary for it to compute  $q'(i)$  because we computed the  $q'(i)$  based on the one-way anonymous key agreement protocol before we encrypted the message. It means only the authorized user can get the right access policy. And due to the random value  $a$ , unauthorized user cannot guess attribute  $i$  from  $q'(i)$  which prevents the collusion of the users. Hence, the advantage of the adversary to win the experiment  $\text{Adv}_{\mathbb{A}}[\text{Exp}^{\text{Priv}}(1^\xi)]$  is negligible, and our scheme ensures the privacy preservation of the access policy against adaptive chosen plaintext attack.

6.4. *Traceability.* In this section, we prove that our scheme is fully traceable under the  $q$ -SDH assumption.

**Lemma 1.** *Our scheme achieves fully user traceability based on that the Boneh-Boyen fully signature scheme [31] is strong existential forgery secure against adaptive chosen message attack.*

*Proof.* We define a PPT adversary  $\mathbb{A}$  running the experiment defined in Section 4.3(4) to attack our scheme through an entity  $\mathbb{B}$  by  $\mathbb{B}$  breaking the Boneh-Boyen fully signature scheme with the same advantage under adaptive chosen message attacks. Assuming the advantage of the adversary  $\mathbb{A}$  to break our scheme is  $\epsilon$ , and  $\mathbb{B}$  can access a random oracle  $H$ . Let  $\mathbb{C}$  be the challenger in the B-B scheme,  $Sig_j \in \mathbb{G}$  be the signature of  $AA_j$ , and  $pk_{AA_j}^{sig} = \{\mathbb{G}, p, g, g^{a_j}, g^{b_j}\}$  is the associated public key of  $Sig_j$ .

- (1) Set-up: the challenger  $\mathbb{C}$  runs the *Setup* algorithm to generate the global parameter PP and sends PP to  $\mathbb{B}$ . For each noncorrupted authorities in the set  $S'$ ,  $\mathbb{C}$  sends  $pk_{AA_j}^{sig}$  to  $\mathbb{B}$ . Then,  $\mathbb{B}$  chooses two random numbers  $\alpha_i, \beta_i$  for each attribute in the attribute set of the authority, and then  $\mathbb{B}$  chooses a random number  $h_j$  to generate the public key of the authority  $pk_{AA_j} = ($

$\{g^{\alpha_i}, g^{\beta_i}\}_{i \in S_{AA_j}}, g^{h_j}, g^{a_j}, g^{b_j}$ ). Finally,  $\mathbb{B}$  returns PP and  $\{pk_{AA_j}\}_{j \in S'}$  to  $\mathbb{A}$ . For corrupted authorities,  $\mathbb{A}$  runs the *Setup*<sub>auth</sub> algorithm to generate the key pairs for them

- (2) Key query:  $\mathbb{A}$  runs  $m$  queries. In the  $q$ -th query,  $\mathbb{A}$  sends  $(S_{GID_q}, GID_q)$  to  $\mathbb{B}$ .  $\mathbb{B}$  initiates an empty table  $\mathbb{T}$  and do the following steps
  - (a) Accesses the random oracle  $H(GID_q)$ :  $\mathbb{B}$  searches the entry  $(GID_q, t_{GID_q}, g^{t_{GID_q}})$  in the table  $\mathbb{T}$ , and if it exists,  $\mathbb{B}$  outputs  $g^{t_{GID_q}}$ . Else,  $\mathbb{B}$  chooses a random number  $t_{GID_q}$  while stores  $(GID_q, t_{GID_q}, g^{t_{GID_q}})$  in the table  $\mathbb{T}$ .  $\mathbb{B}$  outputs  $g^{t_{GID_q}}$
  - (b) Generates the decryption key  $sk_{GID_q, j}$ :  $\mathbb{C}$  chooses a random number  $r \in \mathbb{Z}_p^* \setminus \{-a_j + GID_q/b_j\}$  for each attribute  $i \in S_{GID_q, j}$  and returns the signature  $(r, \sigma = g^{1/a_j + GID_q + b_j r})$ . Then,  $\mathbb{B}$  computes the components of  $sk_{GID_q, j}$

$$\begin{cases} K_{1,i} = \sigma^{(\alpha_i + \beta_i t_{GID_q})} = g^{\alpha_i + \beta_i t_{GID_q} / a_j + GID_q + b_j r} = g^{\alpha_i / a_j + GID_q + b_j r} g^{t_{GID_q} \beta_i / a_j + GID_q + b_j r} = g^{\alpha_i / a_j + GID_q + b_j r} (GID_q)^{\beta_i / a_j + GID_q + b_j r}, \\ K_{2,i} = H(i)^{h_j}, \\ K_{3,i} = r. \end{cases} \quad (20)$$

Then,  $\mathbb{B}$  sets  $\mathbb{D} = \mathbb{D} \cup S_{GID_q}$ . Finally  $\mathbb{B}$  returns the following result to  $\mathbb{A}$ :

$$sk_{GID_q} = \left( \left\{ sk_{GID_q, j} \right\}_{j \in S_{AA_j}}, GID_q \right) = \left( \left\{ K_{1,i}, K_{2,i}, K_{3,i} \right\}_{i \in S_{GID_q}}, GID_q \right). \quad (21)$$

- (3) Key forgery:  $\mathbb{A}$  sends a  $sk^*$  to  $\mathbb{B}$ . The advantage of the adversary to win is defined as

$$\Pr [\text{Trace}(PP, \{pk_{AA_j}\}, sk^*) \in \{\perp, GID_1, \dots, GID_m\}] = \epsilon, \quad (22)$$

where  $(GID_1, \dots, GID_m)$  is  $mGID$  queried in the last phase. If  $\text{Trace}(PP, \{pk_{AA_j}\}, sk^*) \in \{\perp, GID_1, \dots, GID_m\}$ , it means  $sk^* = (\{K_{1,i}, K_{2,i}, K_{3,i}\}_{i \in S_{GID}}, GID)$  passed the form check and

$GID \in \{\perp, GID_1, \dots, GID_m\}$ . Hence,  $\exists i \in S$ , s.t.

$$\begin{aligned} K_{1,i}, K_{2,i} \in \mathbb{G}, K_{3,i}, GID \in \mathbb{Z}_p^*, \\ e \left( K_{1,i}, g^{a_j} g^{(b_j)^{K_{3,i}}} g^{GID} \right) = e(g, g)^{\alpha_i} e(H(GID), g^{t_i}). \end{aligned} \quad (23)$$

Without loss of generality, we assume the adversary  $\mathbb{A}$  accessed the random oracle  $H(GID)$  before it outputs the  $k^*$ .  $\mathbb{B}$  obtains the entry  $(GID, t_{GID}, g^{t_{GID}})$  from the table  $\mathbb{T}$ . According to  $e(K_{1,i}, g^{a_j} g^{(b_j)^{K_{3,i}}} g^{GID}) = e(g, g)^{\alpha_i} e(H(GID), g^{t_i})$ , we can get  $K_{1,i} = g^{\alpha_i + t_{GID} \beta_i / a_j + b_j K_{3,i} + GID}$ . Then,  $\mathbb{B}$  computes the signature  $\sigma_j = (K_{1,i})^{1/\alpha_i + t_{GID} \beta_i}$ . Because  $GID, K_{3,i} \in \mathbb{Z}_p^*$ , hence  $(K_{3,i}, \sigma_j)$  is a valid signature on message  $GID$  in the B-B signature scheme. Because  $GID \in \{GID_1, \dots, GID_m\}$ , it means  $\mathbb{B}$  never queried the signature of  $GID$  before, and the advantage of  $\mathbb{B}$  to break the B-B scheme is equal with the advantage of the adversary  $\mathbb{A}$  to break our scheme, which is  $\epsilon$ .

TABLE 5: Computational cost comparison.

Scheme	[11]	[13]	[14]	Our scheme
Key generation	$3N_u E$	$5N_u E$	$(4N_u + 4)E$	$3N_u E$
Encryption	$(N_u + 5N_e + 1)E + 1E_T + N_u P_e$	$(2N_e + 1)E_T + 6N_e E$	$(5N_e + 2)E + 1E_T$	$(N_u + 7N_e + 1)E + 1E_T + N_u P_e$
Outdecryption	$N_d E_T + 3N_d P_e$	—	$N_d E_T + (3N_d + 1)P_e$	$3N_d E_T + 3N_d P_e$
User decryption	$1E_T$	$4N_d E_T + 3N_d P_e$	$3E_T$	$1E_T$

According to the Boneh-Boyen signature scheme, we can also get the following lemma.

**Lemma 2.** *If the  $q$ -SDH assumption holds in the group  $\mathbb{G}$ , the full signature scheme of Boneh and Boyen is strong existential forgery secure against adaptive chosen message attacks.*

**Theorem 4.** *If the  $q$ -SDH assumption holds in the group  $\mathbb{G}$ , our scheme achieves fully user traceability.*

*Proof.* It follows directly from the above Lemma 1 and Lemma 2.

## 7. Performance Analysis

The notations used in our performance analysis are summarized in Table 3.

The comparison of storage cost and computational cost between our scheme and some other ABE schemes is illustrated in Tables 4 and 5 separately. Notice that all results do not contain the costs of the symmetric cryptography including hash operations.

From Table 4, we can see that the decryption key lengths of scheme [11] and ours are related to the number of attributes used in decryption as both scheme outsource the most decryption work to the cloud server, while the decryption key length of scheme [14] is related to the number of attributes in user attribute sets. Speaking of the length of the ciphertext, of all four schemes are associated with the row number of the encryption LSSS access matrix.

As we can see from Table 4, scheme [13] needs  $5N_u$  exponentiations in group  $\mathbb{G}$  to generate the user decryption key. It needs  $2N_e + 1$  exponentiations in group  $\mathbb{G}_T$  and  $6N_e$  exponentiations in group  $\mathbb{G}$  in the encryption phase. Specially,  $4N_d$  exponentiations in group  $\mathbb{G}_T$  and  $3N_d$  pairings are costed by a user who needs to decrypt in scheme [13], which is too heavy for resource-limited IoT devices. Scheme [11] is an ABE scheme with outsourced decryption which needs  $3N_u$  exponentiations in group  $\mathbb{G}$  in the key generation phase. It requires  $N_u + 5N_e + 1$  exponentiations in group  $\mathbb{G}$ , one exponentiation in group  $\mathbb{G}_T$ , and  $N_u$  pairings to encrypt. As the most pairing operations are done by the cloud server, users only cost one exponentiation in group  $\mathbb{G}_T$  to decrypt in [11].

Li et al. proposed a traceable ABE scheme which needs  $4N_u + 4$  exponentiations in group  $\mathbb{G}$  to generate the private key [14]. In encryption phase, users spends  $5N_e + 2$  exponentiations in group  $\mathbb{G}_T$  and one exponentiation in group  $\mathbb{G}$ , while the cloud server performs  $N_d$  exponentiations in group  $\mathbb{G}_T$  as well as  $3N_d + 1$  pairings to predecrypt in [14]. As a

result, users only cost three exponentiations in group  $\mathbb{G}_T$  to fully decrypt.

Our scheme needs  $3N_u$  exponentiations in group  $\mathbb{G}$  in the key generation phase. To achieve fully policy hidden which is deeply valuable in some healthy data application, our scheme requires  $N_u + 7N_e + 1$  exponentiations in group  $\mathbb{G}$ , one exponentiation in group  $\mathbb{G}_T$ , and  $N_u$  pairings to encrypt. Meanwhile, our scheme realizes verifiable outsourced decryption. Our scheme outsources  $3N_d$  exponentiations in group  $\mathbb{G}_T$  and  $3N_d$  pairings to the cloud server. Thus, IoT devices in our scheme only require one exponentiation in group  $\mathbb{G}_T$  to decrypt, which dramatically reduces the computational overhead of resource-limited devices.

Figure 7 illustrates the time overhead of decryption. The simulation is performed in a Ubuntu 16.4 desktop system with 3.0-GHz Intel Core (TM) i5-7400 CPU and 2-GB RAM, and all experiments are done by using the Charm (version 0.50) [37], a rapid prototyping framework for cryptographic schemes based with Python.

Compared with the outsourced multiauthority ABE scheme [11] with no traceability, our traceable MAABE scheme is with little extra computational cost. However, the user decryption cost of [11] and our scheme is same owing to the outsourced decryption. While comparing with the traceable single-authority ABE scheme [14], our multi-authority scheme can handle more attributes and is more suitable for a large number of devices of IoT systems. In addition, another traceable MAABE [13] is not applicable for resource-limited IoT devices due to its heavy decryption cost.

More importantly, our scheme costs barely one hash operation to achieve the verification of decryption results. About another practical function is achieved by our scheme, traceability, and the cost of our scheme is  $N_a(2E + H + 3P)$ . Although it looks like that this result is linear to the size of the attribute universe set, the real computational cost of this algorithm for each AA is linear to the size of its own attribute set as we assumed that attribute sets controlled by different attribute authorities are disjoint in our scheme.

## 8. Conclusion

In this paper, we propose a multiauthority ABE scheme supporting verifiable outsourced decryption and white-box traceability. Our scheme outsources most decryption works to the honest-but-curious resource-rich cloud server; thus, our scheme meets the special needs of resource-limited IoT devices. Moreover, our scheme protects the privacy of both the encryptor and the decryptor by the fully hiding policy technology. At the same time, another issue influences the application of ABE—the key leakage problem—which is



solved by the user traceability algorithm. In a word, our scheme realizes several practical functions while achieving replayable chosen-ciphertext attack security.

In the future, we plan to improve the scheme with fixed key size and ciphertext size to further reduce equipment overheads. Moreover, we can also consider how to solve another difficulty of the practical application of the ABE—attribute revocation and user revocation. How to dynamically withdraw attributes or users without affecting other authorized users is the focus of our future works.

## Data Availability

All data used to support the findings of this study are available from the corresponding author upon request.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This work was supported in part by the National Key Research and Development Program of China under Grant 2019YFB2102600; in part by the National Natural Science Foundation of China under Grants 62072065, 61832012, 61672321, 61771289, and 61373027; in part by the Fundamental Research Funds for the Central Universities under Grant 2019CDQYR006; in part by the Chongqing Research Program of Basic Research and Frontier Technology under Grant cstc2018jcyjAX0334; in part by the Key Project of Technology Innovation and Application Development of Chongqing under Grant CSTC2019jscx-mbdx0151; and in part by the Overseas Returnees Innovation and Entrepreneurship Support Program of Chongqing under Grants cx2018015 and cx2020004.

## References

- [1] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Workshop on the theory and application of cryptographic techniques*, pp. 47–53, Springer, 1984.
- [2] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Annual international cryptology conference*, pp. 213–229, Springer, 2001.
- [3] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 457–473, Springer, 2005.
- [4] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in *International Workshop on Public Key Cryptography*, pp. 53–70, Springer, 2011.
- [5] S. Pattar, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik, "Searching for the iot resources: fundamentals, requirements, comprehensive review, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2101–2132, 2018.
- [6] M. Chase, "Multi-authority attribute based encryption," in *Theory of Cryptography Conference*, pp. 515–534, Springer, 2007.
- [7] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *Proceedings of the 16th ACM conference on Computer and communications security - CCS '09*, pp. 121–130, Chicago Illinois USA, 2009.
- [8] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Annual international conference on the theory and applications of cryptographic techniques*, pp. 568–588, Springer, Tallinn, Estonia, 2011.
- [9] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of abe ciphertexts," in *Proc. 20th USENIX Security Symposium, USENIX Association*, vol. 2011, pp. 1–16, San Francisco, CA, 2011.
- [10] J. Li, F. Sha, Y. Zhang, X. Huang, and J. Shen, "Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length," *Security and Communication Networks*, vol. 2017, Article ID 3596205, 11 pages, 2017.
- [11] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "Phoabe: securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted iot," *Computer Networks*, vol. 133, pp. 141–156, 2018.
- [12] Z. Liu, S. Duan, P. Zhou, and B. Wang, "Traceable-then-revocable ciphertext-policy attribute-based encryption scheme," *Future Generation Computer Systems*, vol. 93, pp. 903–913, 2019.
- [13] K. Zhang, H. Li, J. Ma, and X. Liu, "Efficient large-universe multi-authority ciphertext-policy attribute-based encryption with white-box traceability," *Science China Information Sciences*, vol. 61, no. 3, article 032102, 2018.
- [14] Q. Li, H. Zhu, Z. Ying, and T. Zhang, "Traceable ciphertext-policy attribute-based encryption with verifiable outsourced decryption in eHealth cloud," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 1701675, 12 pages, 2018.
- [15] H. Zhong, W. Zhu, Y. Xu, and J. Cui, "Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage," *Soft Computing*, vol. 22, no. 1, pp. 243–251, 2018.
- [16] S. Belguith, N. Kaaniche, A. Jemai, M. Laurent, and R. Attia, "Pabac: a privacy preserving attribute based framework for fine grained access control in clouds," in *13th IEEE International Conference on Security and Cryptography (Secrypt)*, pp. 133–146, Portugal, 2016.
- [17] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2018.
- [18] V. Božović, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption with honest-but-curious central authority," *International Journal of Computer Mathematics*, vol. 89, no. 3, pp. 268–283, 2012.
- [19] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.
- [20] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: a fuzzy attribute-based signcryption scheme," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 37–46, 2013.

- [21] X. Zheng, Z. Cai, J. Yu, C. Wang, and Y. Li, "Follow but no track: privacy preserved profile publishing in cyber-physical social systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1868–1878, 2017.
- [22] Y. Pu, C. Hu, S. Deng, and A. Alrawais, "R<sup>2</sup>PEDS: a recoverable and revocable privacy-preserving edge data sharing scheme," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8077–8089, 2020.
- [23] Z. Cai and Z. He, "Trading private range counting over big iot data," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 144–153, Dallas, TX, USA, July 2019.
- [24] X. Xu, J. Zhou, X. Wang, and Y. Zhang, "Multi-authority proxy re-encryption based on cpabe for cloud storage systems," *Journal of Systems Engineering and Electronics*, vol. 27, no. 1, pp. 211–223, 2016.
- [25] Y. Yang, H. Zhu, H. Lu, J. Weng, Y. Zhang, and K.-K. R. Choo, "Cloud based data sharing with fine-grained proxy re-encryption," *Pervasive and Mobile Computing*, vol. 28, pp. 122–134, 2016.
- [26] X. Zheng, Z. Cai, and Y. Li, "Data linkage in smart internet of things systems: a consideration from a privacy perspective," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 55–61, 2018.
- [27] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp. 1343–1354, 2013.
- [28] N. Deng, S. Deng, C. Hu, and K. Lei, "An efficient revocable attribute-based signcryption scheme with outsourced design-encryption in cloud computing," in *International Conference on Wireless Algorithms, Systems, and Applications*, pp. 84–97, Springer, 2019.
- [29] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in *International conference on applied cryptography and network security*, pp. 111–129, Springer, 2008.
- [30] M. J. Hinek, S. Jiang, R. S. Naini, and S. F. Shahandashti, "Attribute-based encryption without key cloning," *International Journal of Applied Cryptography*, vol. 2, no. 3, pp. 250–270, 2012.
- [31] D. Boneh and X. Boyen, "Short signatures without random oracles," in *International conference on the theory and applications of cryptographic techniques*, pp. 56–73, Springer, 2004.
- [32] Zhen Liu, Zhenfu Cao, and D. S. Wong, "White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 76–88, 2013.
- [33] Z. Liu, Z. Cao, and D. S. Wong, "Traceable cp-abe: how to trace decryption devices found in the wild," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 55–68, 2015.
- [34] G. Yu, Y. Wang, Z. Cao, J. Lin, and X. Wang, "Traceable and undeniable ciphertext-policy attribute-based encryption for cloud storage service," *International Journal of Distributed Sensor Networks*, vol. 15, no. 4, 2019.
- [35] H. Qiao, J. Ren, Z. Wang, H. Ba, and H. Zhou, "Compulsory traceable ciphertext-policy attribute-based encryption against privilege abuse in fog computing," *Future Generation Computer Systems*, vol. 88, pp. 107–116, 2018.
- [36] R. Canetti, H. Krawczyk, and J. B. Nielsen, "Relaxing chosen-ciphertext security," in *Annual International Cryptology Conference*, pp. 565–582, Springer, 2003.
- [37] J. A. Akinyele, C. Garman, I. Miers et al., "Charm: a framework for rapidly prototyping cryptosystems," *Journal of Cryptographic Engineering*, vol. 3, no. 2, pp. 111–128, 2013.

## Research Article

# Participant Recruitment Method Aiming at Service Quality in Mobile Crowd Sensing

Weijin Jiang,<sup>1,2</sup> Junpeng Chen ,<sup>1,2</sup> Xiaoliang Liu,<sup>1,2</sup> Yuehua Liu,<sup>1,2</sup> and Sijian Lv<sup>1,2</sup>

<sup>1</sup>Key Laboratory of Hunan Province for New Retail Virtual Reality Technology, Changsha 410205, China

<sup>2</sup>College of Computer and Information Engineering, Hunan University of Technology and Business, Changsha 410205, China

Correspondence should be addressed to Junpeng Chen; [jjpchen@163.com](mailto:jjpchen@163.com)

Received 11 December 2020; Revised 16 February 2021; Accepted 9 March 2021; Published 19 April 2021

Academic Editor: Yingjie Wang

Copyright © 2021 Weijin Jiang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the rapid popularization and application of smart sensing devices, mobile crowd sensing (MCS) has made rapid development. MCS mobilizes personnel with various sensing devices to collect data. Task distribution as the key point and difficulty in the field of MCS has attracted wide attention from scholars. However, the current research on participant selection methods whose main goal is data quality is not deep enough. Different from most of these previous studies, this paper studies the participant selection scheme on the multitask condition in MCS. According to the tasks completed by the participants in the past, the accumulated reputation and willingness of participants are used to construct a quality of service model (QoS). On the basis of maximizing QoS, two heuristic greedy algorithms are used to solve participation; two options are proposed: task-centric and user-centric. The distance constraint factor, integrity constraint factor, and reputation constraint factor are introduced into our algorithms. The purpose is to select the most suitable set of participants on the premise of ensuring the QoS, as far as possible to improve the platform's final revenue and the benefits of participants. We used a real data set and generated a simulation data set to evaluate the feasibility and effectiveness of the two algorithms. Detailedly compared our algorithms with the existing algorithms in terms of the number of participants selected, moving distance, and data quality. During the experiment, we established a step data pricing model to quantitatively compare the quality of data uploaded by participants. Experimental results show that two algorithms proposed in this paper have achieved better results in task quality than existing algorithms.

## 1. Introduction

The rapid development of smart sensing technology and the widespread popularity of mobile smart devices have made it possible for the holder of each mobile device to become a sensing unit [1] which has led to the rapid development of mobile crowd sensing (MCS) [2, 3]. The use of mobile devices to build an interactive and participatory sensor network allows ordinary users to participate in the data collection process, which makes the data collection technology under the big data environment highly developed. Compared with traditional static sensing technology, MCS utilizes existing sensing equipment and communication infrastructures, saving the expense of building additional sensing equipment [4]. At the same time, MCS has the advantages of high mobility and a wide range of potential participants, especially for sudden and unpredictable events, and MCS provides unprece-

dent time and space coverage conditions [5]. Nowadays, MCS has been widely used in public safety [6], environmental monitoring [7], smart transportation [8, 9], etc., which brings a lot of convenience to our daily life while also improving our quality of life. Compared with traditional wireless perception technology, MCS pays more attention to and emphasizes the participation process of participants in the collection process and the decisive role of perception data [10].

The main theoretical research of MCS includes three major aspects: participant selection [11], task distribution [12], and incentive mechanism [13–15]. The key of the research is how to set up an excellent incentive mechanism to recruit suitable users for perception tasks, so as to meet the time requirements, quality requirements, and cost requirements of the tasks, so that the data platform can obtain considerable benefits [16].

The problem of participant selection refers to how to effectively select suitable participants from a large user group to perform various perception tasks under certain constraints [17]. On the one hand, the data platforms hope to use less expenditure to obtain the desired data in order to maximize the benefits of them; on the other hand, the participants also hope to make as much profit as possible in the perception task that is to increase each the number of tasks undertaken by participants. There are gaps in the data that different participants can collect, and the returns they demand from the platform are also different [18, 19]. How to achieve a game equilibrium between platforms and users is an important direction of current academic research. In addition to the above two main goals, the number of participants in each task, the number of tasks assigned by each participant, the quality of the data submitted by participants, and the total distance a participant needs to move to complete tasks are all in the selection process, which need to be considered [20]. Participant selection, as the core key issue in the field of MCS, is the focus and difficulty of current research. The current related research mainly stays in single-objective optimization, such as platform-centered seeking to maximize profits and user-centered to maximize user benefits [21]. Single-objective optimization often produces various problems. For example, maximizing the benefits of the data platform will damage the benefits of participants, thereby reducing the willingness of users to participate, and ultimately will affect the benefits of the platform [22]. In reality, it is necessary to comprehensively consider various impact conditions in order to ensure the benefits of the data platform and participants. Therefore, this paper comprehensively considers a variety of factors and conducts an in-depth study on participant selection methods under multitask conditions.

The main contributions of this article include the following:

- (1) First, sort out and explain the research on participant selection in the theory of MCS. Among them, the MultiTasker method proposed by Liu et al. provides constructive ideas for the two selection methods proposed in this paper
- (2) Research on the multitask distribution model of MCS. Based on the historical task completion of participants, we use the reputation and willingness of participants to establish a service quality model and propose a participant selection plan based on service quality
- (3) Aiming at the task-centered and user-centered participant selection problems, the heuristic greedy algorithm is used to solve the problem, and a participant selection algorithm is proposed, respectively, and the platform is realized under the conditions of meeting the service quality constraints and distance constraints the requirements for minimum expenditure and maximum user benefits
- (4) Verify the feasibility and effectiveness of the selection scheme through simulation experiments on real data

and simulated data, construct a data value evaluation index system, and find the most suitable distance constraint value. Compare it with existing algorithms in terms of the number of participants, the number of tasks, and the data quality

## 2. Related Work

Now, a train of scholars have conducted extensive research and exploration on the selection of participants in the MCS system.

Some scholars' research mainly focuses on designing excellent incentive mechanisms to encourage participants to perform perceptual tasks. Jin et al. [23] proposed a new type of MCS system framework, which integrates data aggregation, incentives, and disturbance mechanisms. Its incentive mechanism selects users who are more likely to provide reliable data and compensates for their perceived cost; its data aggregation mechanism combines the reliability of users to generate high-precision aggregation results; its data perturbation mechanism weakens users' privacy. Leaking concerns improve participant satisfaction and the desired accuracy of the final disturbance result. Hu et al. [24] focused on the location-based MCS system and proposed a demand-based dynamic incentive mechanism. The mechanism can dynamically change the reward of each task as needed to balance the popularity between tasks. Propose a solution based on optimal backtracking for opportunistic scenarios to help each user choose a task, while maximizing their profits, and better achieve the balance between participants and tasks. Xu et al. [25] proposed two models, MCT-M and MCT-S, for the purpose of minimizing social costs. These two solutions use the real relationship of social networks to group participants, so that each collaborative task can be completed by a group of compatible users. Experiments show that the proposed model can further reduce social costs while reducing grouping time.

At the same time, some researchers pay attention to the research on the selection mechanism of excellent participants. Guo et al. [26] mainly studied the problem of participant selection in the task types oriented to diversity. Starting from the microscopic and macroscopic visual task types, respectively, they designed the UtiPay visual group perception framework, which greatly improved the quality of group intelligence perception data. Zhou et al. [27] defined the coverage model of "t-Sweep k-Coverage" and proposed a selection method based on linear programming and a selection method based on greedy strategy. Through solving on real data sets, they verified the feasibility and effectiveness of the two selection methods. However, this method only solves the situation when the participant's moving time, location, and other attributes are known and does not predict the future location of the user's historical movement law. Estrada et al. [28] proposed a framework for selecting participants in order, which comprehensively considers the reputation and payment model of participants and maximizes the quality of service under certain time constraints. However, this method does not collect the actual movement speed of the participant and randomly generates the movement speed of



the participant, and it also does not consider the movement trajectory of the user. Pu et al. [29] proposed another sequence selection scheme, which models the nature of tasks, user capabilities, and real-time performance to predict the quality of services provided by participants. The plan considers the importance of keywords to maximize the possibility of participants accepting and completing tasks in a timely manner but does not consider the reputation of participants and the expenses caused by moving distance. Azzam et al. [30] proposed a group-based selection scheme, which considers maximizing coverage, sampling frequency, and battery life and greatly improves data quality. However, using this model to select participants requires a lot of running time, and the model does not consider the cost of the task platform and the movement trajectory of participants. Yang et al. [31] proposed a multiarmed slot machine user selection model with a budget mechanism, which solves the cost problem of effectively learning to select each user without prior knowledge and reduces the selection to a large extent. The accumulated regrets are considered in this process; but the time correlation of user environment information has not been studied in depth. Wang et al. [32] divided users into two groups, formulated different pricing plans, proposed a semi-Markov model to determine the user's interest points distribution, and proposed a prediction-based participant preference Method to minimize the cost of uploading data. Jiang et al. [16] proposed an optimal participant decision model based on voting mechanism. In the participant selection stage, considering the platform benefits, they designed a participant decision model based on the reverse auction model, which is similar to the traditional reverse auction model. In contrast, this method increases the parameter of the number of effective perception tasks and effectively reduces the redundancy of participants. However, this method does not fully consider the geographic location information of participants. For large-scale surveillance systems, Li et al. [33] introduced the caching mechanism to mobile group intelligence perception for the first time. They proposed a dynamic participant selection problem with heterogeneous perception tasks and designed offline and online algorithms to solve this problem. Simulations on real data sets verify the effectiveness and efficiency of the proposed algorithm. Liu [34] et al. proposed three algorithms: T-Random, T-Most, and PT-Most, for multitask participant selection from task-centric and user-centric. The number of participants, the number of tasks assigned by each user, and the moving distance were compared through experiments, and the most appropriate participant selection strategy under different indicators was selected. However, this method only uses the number of users, tasks, and movement distance as the main optimization indicators and does not consider the service quality of participants.

In summary, most of the current research methods characterize the selection problem as a target optimization problem on certain constraints. In this process, it considers the reputation of participants, geographic location, moving distance, and incentive mechanism and converts multiobjective constraints into single-objective constraints. However, there are few studies on using participant historical information

to estimate the task quality of participants. Some methods ignore the platform's need for task quality when considering the number of participants or moving distances. Other methods take into account the task quality requirements but ignore the actual moving speed or willingness of participants. In reality, the different speeds of participants and willingness have a great influence on the task completion time and task quality. This paper takes into account the historical tasks of participants and establishes a service quality model. In the task-centered and user-centered selection algorithms, many factors such as travel distance, reputation, and task completion degree are comprehensively considered to find the best option under the best service quality. Finally, we use real data sets and simulated data sets to carry out simulation experiments on the two proposed algorithms and analyze and study the participant task set and running time in terms of distance weakening.

### 3. Multitask Participant Selection Model Based on QoS

The MCS system consists of three parts: task release, user selection, and data collection. For various needs, it is often necessary to collect relevant information at a certain time in certain regions and in real life. Collecting data by themselves often consumes a lot of time and financial resources. Nowadays, the common solution is that the data requester uploads the task requirements to a certain task distribution platform; then the cloud server receives the request information and distributes the task to some practitioners for completion. Participants receive tasks and perform data perception according to the task requirements, then upload the data to the cloud. Cloud cleans the data and packages it to the requester. In this process, it is undoubtedly crucial to select the right participants for the perception task, and the quality of participants directly determines the quality of the collected data. Aiming at task-centered and user-centered, under the premise of maximizing service quality, this paper proposes two multitask distribution participant selection methods, from the two aspects of maximizing the benefits of the data platform and participants optimization.

The task platform tends to issue multiple tasks at one time to form a task set  $T = \{t_1, t_2, t_3, \dots, t_n\}$ . At the same time, the data platform will have certain restrictions on the task completion time. Late data is often worthless; this paper agree that the completion time of each task set  $T$  should not exceed  $h$  hours. There are also certain differences in the urgency and importance of tasks. In order to ensure the completeness of the collected data as much as possible and consider the emergencies of the participants and other factors, we consider that each task requires multiple participants to complete, and the number of people  $s_i$  required to complete each task  $t_i$  is different. For ease analysis, the completion time of each task is assumed to be 5 minutes. Suppose there are  $U = \{u_1, u_2, u_3, \dots, u_m\}$  participants in the task platform, and the moving speed of each participant is different,  $V = \{v_1, v_2, v_3, \dots, v_m\}$ . The set of tasks that each participant needs to complete is represented by  $TU_i = \{t_{i1}, t_{i2}, t_{i3}, \dots\}$ . The sum



of the time taken by the participants to complete tasks and spent on the trip is lower than required by the platform. The constraint conditions are defined as follows:  $D(TU_i)$  is the total distance the participant needs to move to complete the task set:

$$TU_i \times 5 + \frac{D(TU_i)}{v_i} \leq h \times 60, \quad 1 \leq i \leq m. \quad (1)$$

This paper integrates the willingness to participate and the reputation of the participants in completing tasks in the past, constructing the service quality model of the participants.

The quality of data uploaded by participants is positively related to their willingness. For example, the higher the willingness of a participant, the more actively participant will collect data and the higher the quality the data uploaded; if a participant adopts a negative attitude to collect data, the quality will also be low. However, it is not enough to only consider the impact of participants' willingness on data quality; the impact of participants' objective perception on data quality is also crucial. We have established evaluation indicators for participation willingness and data quality. In order to reflect the willingness to participate  $w_i$  and data quality  $D_i$  are equally important, we restrict them to the range of [0,1], namely,

$$\begin{aligned} w_i &= \begin{cases} \min(w_i, 1), \\ \max(0, w_i), \end{cases} \\ D_i &= \begin{cases} \min(D_i, 1), \\ \max(0, D_i). \end{cases} \end{aligned} \quad (2)$$

Currently, there are studies that use distance and other conditions to define the willingness of participants. Different participants' willingness to participate in a task is often different and difficult to consider comprehensively. Therefore, this paper defines participant willingness from another perspective. In normal circumstances, the longer it takes a participant to receive the task from the data platform to the confirmation of acceptance of a task, the lower the participant's willingness to participate in the perception task.

The time from when the task is distributed to a participant to when the participant accepts the task is called hesitation time. And willingness is defined as a function related to hesitation time. Inspired by social principles [35], the longer the participants hesitate, the less value they contribute to the platform. We take the average hesitation time of all participants as the critical value. If a participant's hesitation time is equal to it, his willingness to participate is neutral, and his willingness value is 0.5.

Based on the above discussion, participation willingness and hesitation time are modeled as the following functions:

$$w_i = 1 - \max \left[ 0, \min \left( \frac{1}{2} \log_t t_i, 1 \right) \right], \quad (3)$$

where  $w_i'$  represents the willingness of the participant,  $t_i$  is the hesitation time, and  $\bar{t}$  represents the average hesitation time. It can be seen from the above formula that the longer the participants hesitate, the lower their willingness to participate is.

Participants' untrustworthiness can be obtained from the historical data of participating in the perception task. No record of untrustworthiness indicates that participants have a higher sense of responsibility for participation; the quality of the collected data will be higher.

For the sake of simplicity, we use an improved reputation model [36] to describe the reputation of participants, and the calculation formula as follows:

$$R = \frac{T + 1}{T + F + 2} \times \xi \quad (0 \leq R < 1, T > 0, F > 0). \quad (4)$$

The closer the value of  $R$  is to 1, the higher the reputation value of participants is.  $T$  and  $F$  are the records of "true" and "false" in the participant's historical task.  $\xi$  is the weighting factor of the participants' malicious events; the calculation formula as follows:

$$\begin{cases} \xi = \lambda^k, & 0 \leq k < K, \\ \xi = 0, & k \geq K. \end{cases} \quad (5)$$

In this formula,  $k$  is the malicious event of some perceived participants, and  $K$  is the malicious event threshold set by the data platform. Once the threshold is exceeded, the reputation score of the participant will be set to 0. Considering that the platform's tolerance for malicious events is extraordinarily low, participants who uploaded the wrong information three times can be considered malicious participants, and  $K = 3$  by default during the experiment.  $\lambda$  is the attenuation factor within the threshold range, and the default value of  $\lambda$  is set to 0.8. The reputation of participants can be infinitely close but not equal to 1. It can be seen from (4) and (5) that the reputation of a participant who performed the perception task for the first time is 0.5. With the number of perception tasks increasing, there is a large gap between the reputations of participants with no wrong records and those with wrong records. At the same time, the credibility of participants who submit correct data each time should be different. Participants who have 10 correct records must be more credible than those who have only one correct record. When selecting participants, participants with bad reputations are often eliminated. Participant reputation constraints  $\delta$  are established; if  $R \in (0, \delta)$ , we do not consider choosing this participant for perception tasks.

Combining the aforementioned reputation model and participation willingness model, we establish the participant's quality of service (QoS), which is calculated as follows:

$$QoS = w \times R. \quad (6)$$

The configuration or brand of the mobile devices carried by participants is different; even the sensing data collected by the devices in the same location may be different. The quality of sensing device may have a certain impact on the data

Input: task set  $T$ , user set  $U$ , integrity constraint set  $C$ , distance constraint  $\theta$ , reputation constraint  $\delta$ .  
Output: the participant set  $P$  and the completed task set  $TU$ .

1. Calculate the reputation  $R$  of all candidates and the data integrity indicator  $D$
2. Delete participants with substandard reputation
3. Select the task with the most people in the task set to be completed as the initial node  $t_{ij}(j=1)$
4. Calculate the  $Qos$  of the participants who meet the condition  $D \geq \varepsilon_j$  within the bound distance  $\theta$  from the initial task  $t_{ij}$
5. Select the participant  $p_i(i \geq 1)$  with the highest  $Qos$  in  $\theta$  range
6. Select the task  $t_{i(j+1)}(j \geq 1)$  that meet  $\varepsilon_{(j+1)} \leq D$  and closest to the task  $t_{ij}$  as the new central task node
7. Repeat 4~6, and stop the loop when the time for the participant  $p_i$  to complete these tasks exceeds the time constraint
8. Output task set  $TU_i = \{t_{i1}, t_{i2}, t_{i3}, \dots\}$  of  $p_i$
9. Repeat 3~8 until all tasks are completed
10. Output participant set  $P = \{p_1, p_2, p_3, \dots\}$  and completed task set  $TU = TU_1 \cup TU_2 \cup \dots \cup TU_i$
11. End

ALGORITHM 1

quality. The complete performance of the data characterizes the perception of participants. Quantitative research on the perception of participants' equipment and professional conditions obviously requires consideration of a variety of positive and negative related factors; the degree of difference between the data submitted by participants and the expected data on the platform can characterize the perception of the participant.

Evaluate the historical submitted data of participants, calculate the gap between it and the expected value of the platform, and establish data integrity function to characterize data quality  $D_i$ . The calculation formula is as follows:

$$D_i = \begin{cases} 0.8, & N = 0, \\ \frac{1}{N} \sum_{t=1}^N P_t, & N \geq 1. \end{cases} \quad (7)$$

$P_t$  is the completeness of the data uploaded by a participant at historical time  $t$ ,  $P_t \in (0, 1)$ ,  $N$  is the number of historical tasks completed by the participant, and the larger the value of  $D$ , the more complete the information uploaded by the participant high. For the participant who performs the perception task for the first time, platforms are always willing to give him more opportunities to complete the task, and the tolerance for novices is often higher, so we expect the complete performance of the participant to submit the task to 0.8. Similarly, we establish the integrity constraint index  $\varepsilon$ . When  $D \in (0, \varepsilon)$ , the task completion quality of the participant cannot meet the current task completion requirements, so this participant will not be considered for the perception task.

The platform's tolerance for data quality is often higher than untrustworthy participants. Some tasks are only a rough perception that can meet the needs of the platform; that is, the requirements for the quality of participation in each task may be different. When the platform publishes the task set  $T = \{t_1, t_2, t_3, \dots, t_n\}$ , it often gives the corresponding minimum integrity data set  $C = \{\varepsilon_1, \varepsilon_2, \varepsilon_3, \dots, \varepsilon_n\}$ . As long as the completeness of the tasks submitted by participants is higher than this standard, the needs of the platform can be met.

The optimization goal of the participant selection method proposed in this paper is to minimize the movement

distance of participants under the condition of ensuring service quality to maximize the benefits of the data platform.

#### 4. Participant Selection Method

Algorithm 1 proposed in this paper is improved on the basis of the T-Most algorithm. It is task-centered to select participants and maximizes the service quality of participants as the main optimization goal. At the same time, it also takes into account the minimum number of participants; each participant should complete multiple tasks in the specified time and the smallest possible moving distance, while meeting the data quality requirements of the data platform.

The specific process of participant selection can be considered as follows: select the task which needs the largest number of people among the tasks to be completed as the initial task, and select the participant with the highest service quality within a certain distance from the initial task to complete the task. Next, select the task that is closest to the initial task point and that the participant is eligible to complete as the second task to be completed. When the second task is completed, take this task as the initial node, and select the most recent task and the participant is eligible to complete as the third task to be completed. Repeat this, and follow the above process until the task set completed by this participant in  $h$  hours is selected. Eliminate the participant in the above process, and reduce the number of people required for each task in the task set that they have participated in by one. According to the above method, continue to select participants and the corresponding task set until all tasks are completed.

Algorithm 1 is task-centered for participant selection, and its main goal is to maximize the  $Qos$  of participants, thereby improving the benefits of data platform. This paper proposes a participant-centric selection scheme based on the PT-Most algorithm. Different from Algorithm 1, the main optimization goal of Algorithm 2 is to maximize the number of tasks completed by participants and to maximize the benefits of participants on the premise of meeting the data quality requirements of the platform.

The specific process of participant selection is considered as follows: randomly select participants in the user set as candidate, and select the nearest task that satisfies the integrity

Input: task set  $T$ , user set  $U$ , integrity constraint set  $C$ , distance constraint  $\theta$ , reputation constraint  $\delta$ .

Output: the participant set  $P$  and the completed task set  $TU$ .

1. Calculate the reputation  $R$  of all candidate participants and the data integrity indicator  $D$
2. Delete participants with substandard reputation
3. Randomly select a user in the participant set as the task candidate  $p_{ji}$
4. Select the task  $t_{ik}$  ( $k=1$ ) that satisfies the condition  $\varepsilon_k \leq D_i$  closest to the user  $p_{ji}$  within the constraint condition as the initial task
5. Select the closest task  $t_{i(k+1)}$  that satisfies  $\varepsilon_{k+1} \leq D_i$  under the distance constraint from task  $t_{ik}$  as the next task
6. Repeat 5~6, and stop the loop when the time for the participant  $p_{ji}$  to complete these tasks exceeds the time constraint
7. Output task set  $TU_{ji} = \{t_{i1}, t_{i2}, t_{i3}, \dots\}$  of candidate  $p_{ji}$
8. Execute 3~8 in a loop to determine the task collection of each candidate  $p_{ji}$  within the time constraint  $TU_{ji}$
9. Choose the participant  $p_j$  with the largest task set to complete the task set  $TU_j$
10. Repeat 3~10 until the task set of each participant who meets the constraints is determined
11. Output participant set  $P = \{p_1, p_2, p_3, \dots\}$  and completed task set  $TU = TU_1 \cup TU_2 \cup \dots \cup TU_i$
12. End

ALGORITHM 2

constraint within the range of this candidate  $\theta$  as the initial task. Next, select the task that is closest to the initial task and the candidate is eligible to complete as the next task. This is repeated until the task set for each participant within the agreed time is selected. Choose the candidate with the most tasks as the first participant. Eliminate the participants in the above process, and reduce the number of people required for each task in the task set by 1. According to the above method, continue to select the participants and the corresponding task set until all tasks are completed.

Algorithm 1 is a task-centric algorithm. The time complexity of the algorithm is directly related to the number of tasks. The time complexity of Algorithm 1 is  $n!$ . Algorithm 2 is a user-centered selection algorithm. As the number of tasks increases, the number of participants  $x$  required increases. The value of  $x$  will affect the amount of calculation of Algorithm 2. The time complexity of Algorithm 2 is  $m!/(m-x)!$ , where  $m$  is a participant whose credibility meets the standard.

## 5. Experimental Evaluation

### 5.1. Data Set and Experimental Settings

**5.1.1. Data Set.** This paper selects a real data set and a simulated data set to evaluate the participants' preferred schemes in multitasking conditions.

- (1) Real data set: this paper uses the crowdsourced task allocation data set of the Chinese Society of Industrial and Applied Mathematics. The data set contains 835 tasks and 1877 participants in the four cities of Guangzhou, Shenzhen, Foshan, and Dongguan. On the basis of this data set, we randomly assign a task complete index  $\varepsilon$  for each task to be constrained, and at the same time, assign a certain speed value to each participant randomly to represent their true moving speed; the value is 50-1000 m/min. The data set also provides the participant's reputation score  $R$ ; we map it to  $[0,1]$ . Table 1 summarizes the parameter settings for this data set.

TABLE 1: Real data set parameter settings.

Parameter	Description	Parameter value
$m$	Number of perception tasks	835
$n$	Optional participants	1877
$R$	Participant reputation	$[0,1]$
$\varepsilon$	Minimum task integrity requirement	$[0,1]$
$v$	Participant moving speed	50-1000 m/min

- (2) Simulation data set: this paper follows the existing data generation method to generate a simulation data set. Evenly distribute the perception task and the location of the participants in a rectangular plane of 20 km  $\times$  20 km. In addition, set a reputation parameter  $R$  within the range of  $[0,1]$  for each participant. In the process of the experiment, we consider task sets and participant sets of different sizes, from  $\{100,200,500,800\}$  and  $\{50,100,150,200\}$ ; select  $m$  perception tasks and  $n$  participants to combine. And specify the same other parameters as the real data set for the simulated data set. Table 2 summarizes the parameter settings of the simulation data set.

**5.1.2. Experimental Setup.** Since the real data set used in this paper has given the task location and the participant's current location, the generated simulation data set is also randomly distributed on the participant and task location; we will not take other considerations of location information. However, in real life, participants and tasks are often not connected in a straight line. Considering the buildings and traffic routes is more in line with the real situation. Choosing a suitable path obviously requires a special study. Since the content of this paper is the preferred plan of the participants, for the convenience of the experiment, we use the Euclidean distance between two points to represent the distance that needs to be moved.

TABLE 2: Simulation data set parameter settings.

Parameter	Description	Parameter value
$m$	Number of perception tasks	{100,200,500,800}
$n$	Optional participants	{50,100,200,300}
$R$	Participant reputation	[0,1]
$\varepsilon$	Minimum task integrity requirement	[0,1]
$v$	Participant moving speed	50-1000 m/min

In the subsequent experiments, in order to facilitate the comparison of algorithm performance, we default that each task requires 5 users to complete without special instructions. At the same time, set the completion time of each task to 5 minutes, and the completion time of each task set to 2 hours.

This paper considers experimental design from two aspects. The first is to study the parameters of the algorithm and compare the experimental results to select the most suitable distance constraint  $\theta$ . At the same time, in the case of changes of the perception task and the number of participants, the performance of the algorithm is considered; the second is to consider the quality of the collected data and evaluate the effect of the algorithm.

## 5.2. Experimental Results

**5.2.1. Selection of Suitable Distance Constraint  $\theta$ .** This experiment is conducted on the real data set and the simulated data set. For the real data set, we determine the appropriate  $\theta$  through experimental comparison; for the simulated data set, on the basis of changing the number of perception tasks and the number of participants available for selection, we conducted multiple experiments to verify the effect of  $\theta$  changes in different task densities and participant densities on the platform's revenue and then chose the appropriate  $\theta$  restrictions.

The larger the range of  $\theta$ , the higher the QoS of the selected participant will undoubtedly be. However, when pursuing higher QoS, the time required for the participant to complete the task will be higher, which increases the cost of the platform. We define participant's revenue as task revenue and travel revenue and establish a pricing mechanism for the participant's revenue time. The longer the participant takes to reach a certain task, the higher the participant's travel revenue will be, and the platform's variable expenses will be larger. For simplicity, we establish a linear time expenditure function to characterize the variable expenditure of the platform. Its function can be set as follows:

$$P(u) = kt. \quad (8)$$

$P(u)$  is the variable expenditure of the platform,  $t$  is the time required for the participant to reach the next task point, and  $k$  is the movement cost per unit time. For simplicity, set the value of  $k$  to 1.

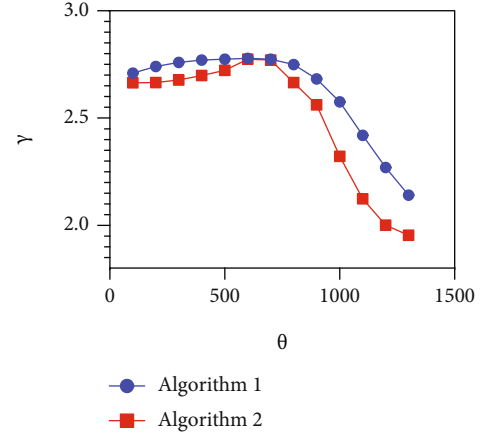


FIGURE 1: The influence of the change of  $\theta$  value on the real data set  $\gamma$ .

At the same time, pricing is based on the data collected by the participants. The higher the service quality of the participants, the greater the revenue of the data platform. We establish a step-type pricing model. The pricing model is as follows:

$$G(u) = \begin{cases} 10 \text{ QoS} : 0 \leq \text{QoS} < 0.2, \\ 2 + 10(\text{QoS} - 0.2) : 0.2 \leq \text{QoS} < 0.5, \\ 7 + 10(\text{QoS} - 0.5) : 0.5 \leq \text{QoS} < 0.8, \\ 10 + 10(\text{QoS} - 0.8) : 0.8 \leq \text{QoS} < 1. \end{cases} \quad (9)$$

Among them,  $G(u)$  is the income that the platform can finally obtain with the improvement of QoS.

And set the objective function  $\gamma$  to represent the final return of the platform as the distance changes and consider the impact of changes in  $\theta$  on the platform's return. The  $\gamma$  function is expressed as follows:

$$\gamma = G(u) - P(u). \quad (10)$$

Figure 1 is the result of the experiment on the real data set. It can be clearly seen that with the relaxation of the

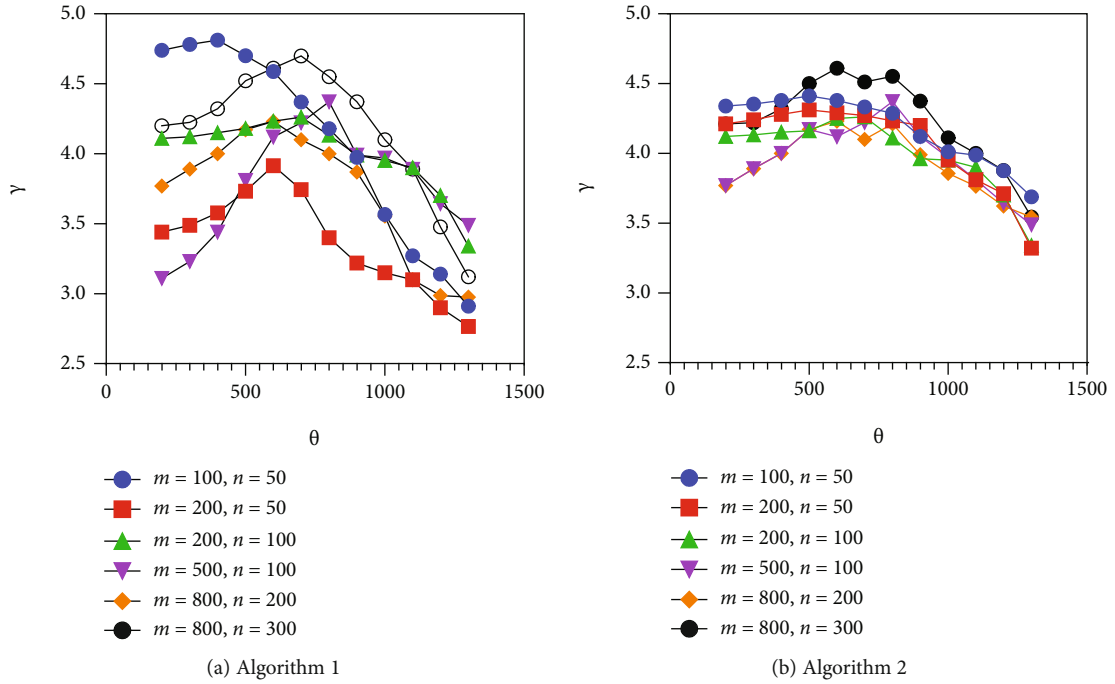


FIGURE 2: The influence of the change of  $\theta$  value on the simulated data set  $\gamma$ .

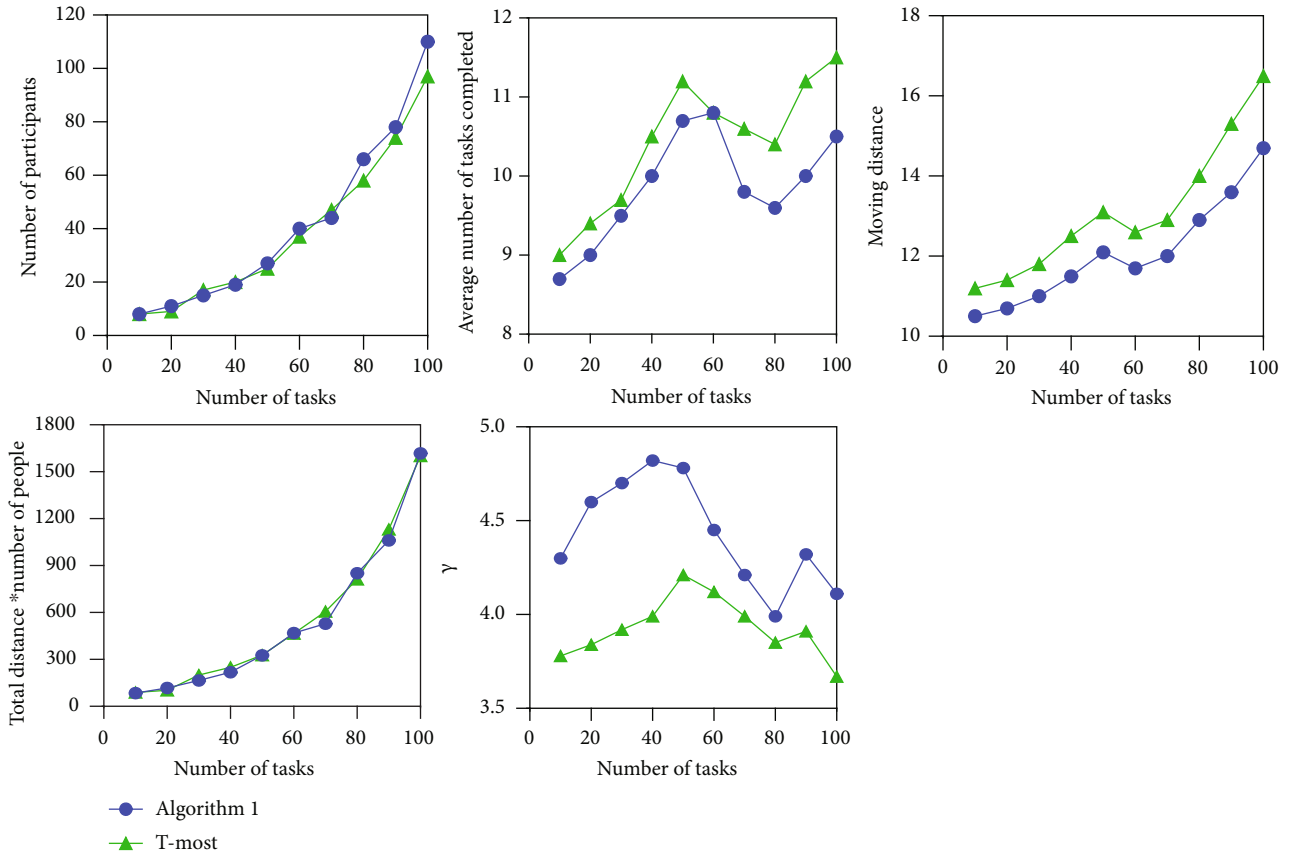


FIGURE 3: The impact of changes in the number of tasks on algorithm performance.



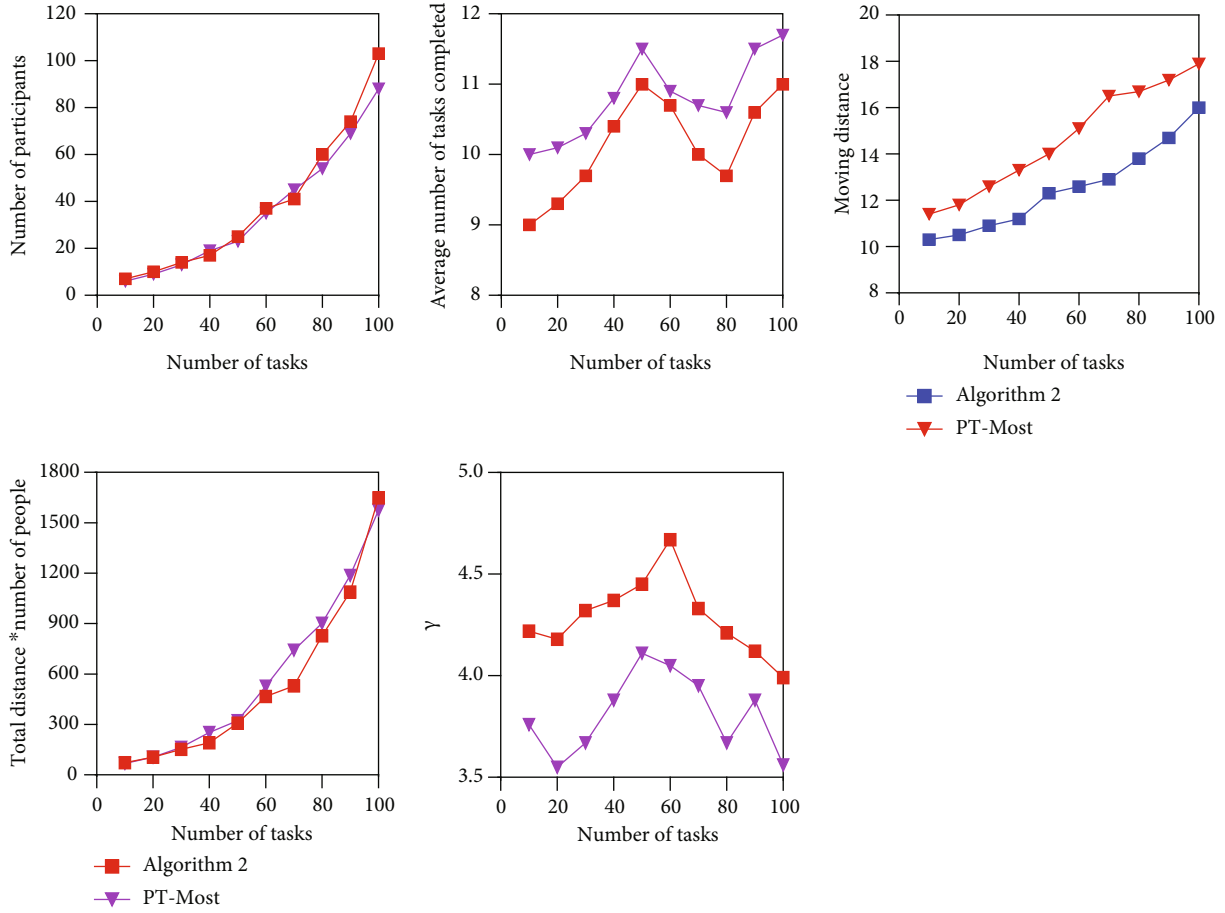


FIGURE 4: The impact of changes in the number of tasks on algorithm performance.

constraints, the final revenue of the platform will first increase and then decrease and, when the constraint distance is greater than 900 m, the revenue of the platform will significantly decrease; this should be consistent with the actual situation. Too short a distance constraint is difficult to select participants with better service quality, which will make the platform’s revenue less than the optimal level; and the value of  $\theta$  is selected too large; although participants with better QoS can be selected, the distance the users needs to move will increase, which will undoubtedly increase the additional expenses of the platform.

Figure 2 is the experimental result of the dynamic combination of the number of tasks and the number of participants on the simulated data set. It can be seen that as the number of tasks distributed and the number of participants changes, the distance when  $\gamma$  reaches the maximum value also changes greatly. Too high or too low  $\theta$  will make the  $\gamma$  value lower. Therefore, it is not easy to select the most appropriate value of  $\theta$  for different data, but it can be seen from Figure 2 that in view of the changes in the number of tasks and participants, most data will achieve better results in the condition of  $\theta \in [500,800]$ . In subsequent experiments, if there are no special instructions, we default  $\theta = 600$  as the distance constraint value.

**5.2.2. The Impact of Changes in the Number of Tasks on the Algorithm.** The number of tasks issued by the platform is not constant. This experiment considers changing the number of tasks distributed each time when other factors are determined to make the selection of participants. Figure 3 shows the results of a comparison experiment between Algorithm 1 and T-Most algorithm. As the number of tasks increases, the gap between the number of participants selected by Algorithm 1 and the T-Most algorithm is not too large. Even in some certain tasks, Algorithm 1 will select fewer users. Regarding the number of tasks assigned to users on average, there is not much difference between Algorithm 1 and T-Most. In terms of moving distance, because Algorithm 1 weakens the distance constraint, the moving distance of participants in the T-Most is less than that in Algorithm 1, but in the index of “total distance  $\times$  number of people,” in the two algorithms, the performance effect is not much different. The optimization goal of the T-Most is to minimize the distance and reduce the cost. Algorithm 1 is not so strict in the distance requirement but pays more attention to the service quality of participants. So on the platform’s final profit evaluation index  $\gamma$ , Algorithm 1 achieves significantly better results than T-Most, which is

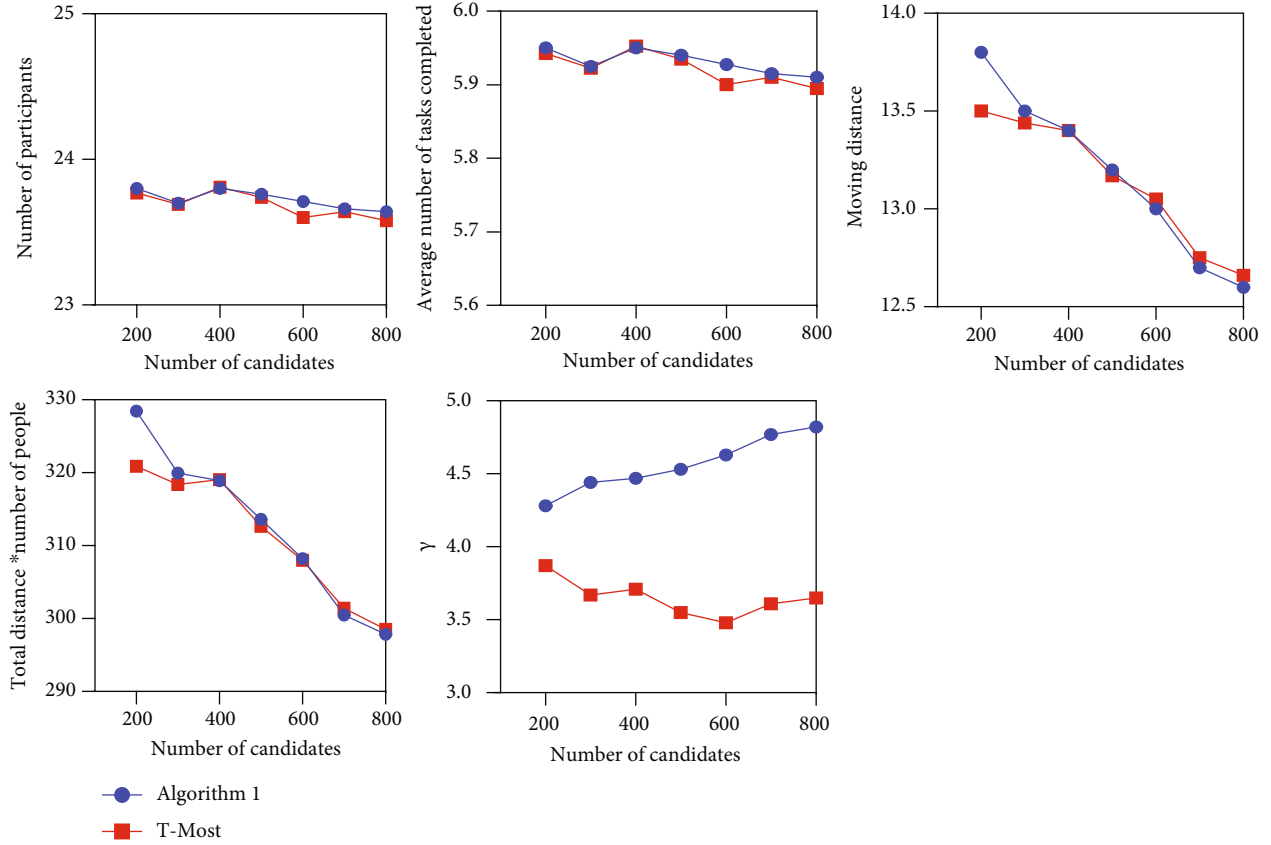


FIGURE 5: The impact of changes in the number of candidates on algorithm performance.

consistent with what we envisioned when proposing the algorithm.

Figure 4 shows the results of a comparison experiment between Algorithm 2 and PT-Most. Like the results in Figure 3, when the gap between other indicators is not obvious, the effect of our proposed algorithm 2 on the evaluation index  $\gamma$  is obviously better than that of PT-Most.

**5.2.3. The Impact of Changes in the Number of Candidates on the Algorithm.** In the process of participant selection, in addition to the number of tasks to be completed that has a great influence on the selection, the number of participants to be selected will also have an impact on the selection effect to a large extent. The more candidates there are, the closer the selected participant will be to the task, and the quality of service for participants will be further improved. This experiment changes the number of candidate participants in the task area when the task to be completed is constant. The evaluation indicators are the same as the previous experiment. It can be seen from Figures 5 and 6 that as the number of candidates in the area increases, the number of participants selected by the four algorithms and the average number of tasks completed by each participant did not change much, and there was not much difference in quantitative indicators. However, as the number of candidates increases, the total distance that participants need to move and distance  $\times$

number of people indicators will drop rapidly. The experimental results are in line with our expectations. As the number of candidates increases, the closer the selected participant will be to the task, the corresponding movement distance will decrease. In terms of task completion quality, it is obvious that the two algorithms mentioned in this paper are better than T-Most and PT-Most. As the number of candidates increases, the performance of the two algorithms in this paper will get better and better on the  $\gamma$  index, while T-Most and PT-Most have no obvious changes.

**5.2.4. Perceive Time Changes.** The specified completion time of task is also a major factor affecting the performance of the algorithm. This experiment changes the limited time to 1 h, 2 h, and 3 h for experimental comparison and analysis of various situations when the number of tasks remains unchanged. It can be seen from Figure 7 that with the relaxation of the time limit, the number of tasks performed will continue to decrease and the number of tasks that each user needs to complete increases accordingly. The moving distance increases slightly, and the index of distance  $\times$  number of people also shows a downward trend. Compared with the comparison algorithm, the two algorithms in this paper have no obvious difference in the above four indicators. In most cases, the algorithms in this paper have similar effects to the comparison algorithm. On the  $\gamma$  index, the algorithm

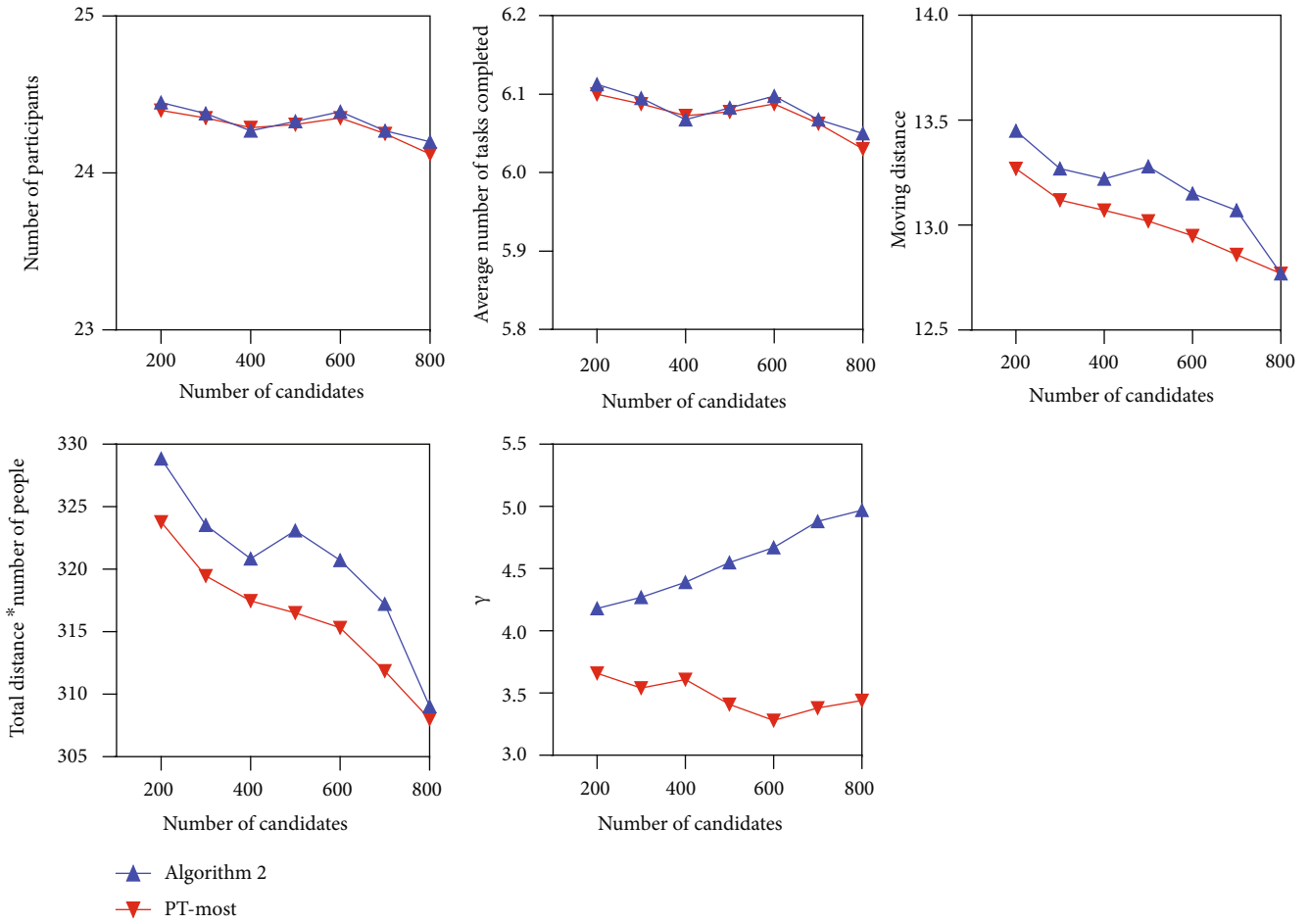


FIGURE 6: The impact of changes in the number of candidates on algorithm performance.

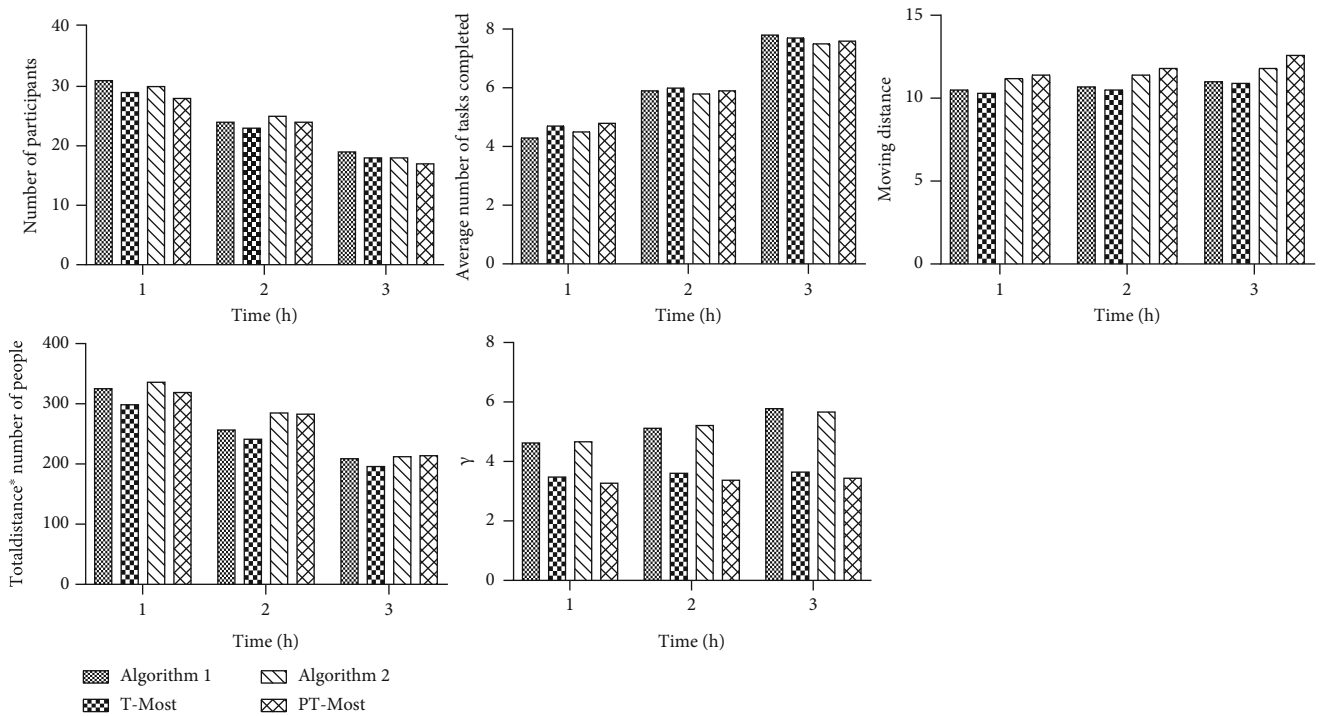


FIGURE 7: The impact of perceptual time changes on the algorithm.

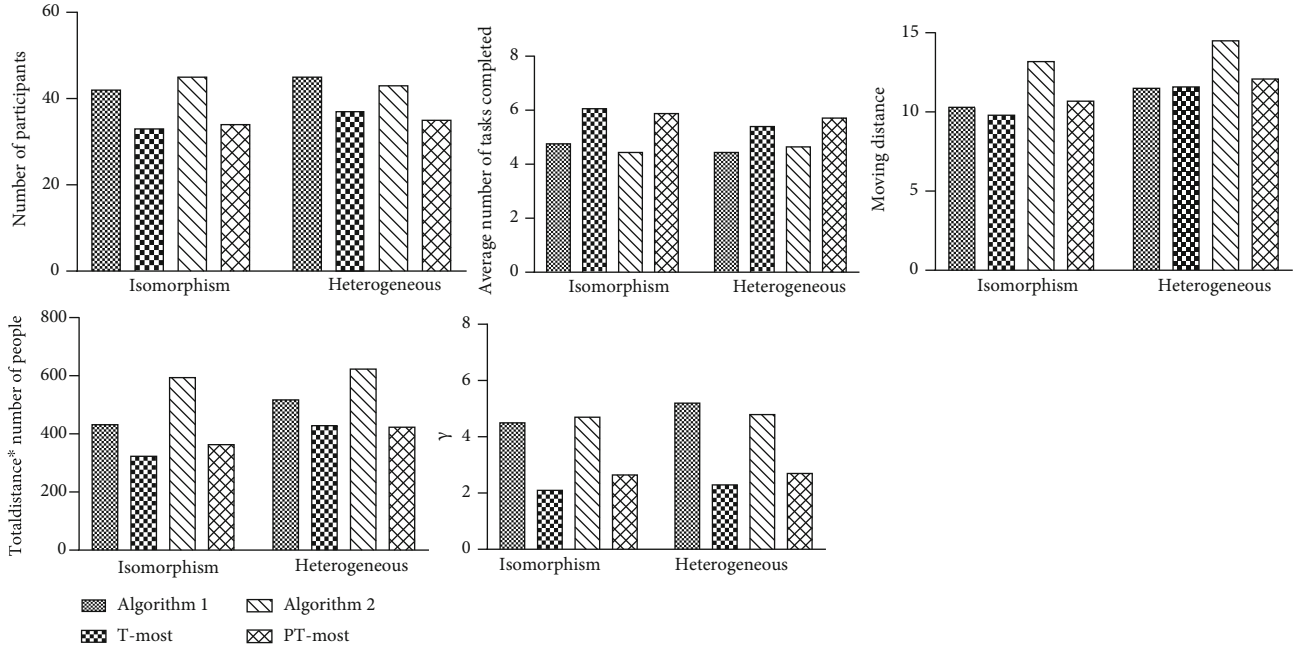


FIGURE 8: The influence of homogeneous and heterogeneous conditions on algorithms.

proposed in this paper is significantly better than the two comparison algorithms, and with the relaxation of the time limit, the  $\gamma$  index of our algorithms has a gradual upward trend.

### 5.2.5. Change the Number of People Required for Each Task.

The above experiments are conducted under the premise that each task requires 5 participants to complete. But in real life, due to the difficulty level of each task, the different requirements of the data requester for data quality, and the difference in the budget for each task, the number of participants required for each task is not the same. Therefore, this experiment will study the changes of the five comparative indicators in the above experiment under the condition that the task requires the same and different participants.

In order to facilitate the experiment, we set the number of tasks to be completed to 20. Under homogeneous conditions, each task requires 10 participants to complete. Under heterogeneous conditions, the number of people required to set tasks is 5, 10, and 15 and accounted for 25%, 50%, and 25% of the total number of tasks; that is, 5 tasks require 5 participants to complete, 10 tasks require 10 participants to complete, and 5 tasks require 15 participants to complete. We generate two 3 km  $\times$  3 km rectangular areas to simulate the real environment and make the participants and tasks evenly distributed on the rectangular plane. In the two scenarios, except for the differences in the participants required for the task, the other parameter settings are roughly the same.

It can be seen from Figure 8 that there is a big difference when the participants required by the task are different and when the participants required by the task are completely consistent. Algorithms 1 and 2 have certain weaknesses in the first four comparison indicators, which is consistent with

our expected situation. However, comparing Algorithms 1 and 2 longitudinally, we find that in terms of the number of participants and the average number of tasks completed, Algorithm 1 has achieved better results under the condition of task isomorphism. Under the condition of heterogeneous tasks, Algorithm 2 performs better. In terms of moving distance, Algorithm 2 has moved a longer distance compared to Algorithm 1 under both conditions, because the main goal of Algorithm 2 is to maximize the completion of tasks for each participant, this result is also in line with expectations. On the index of distance  $\times$  people, Algorithm 1 is superior to Algorithm 2. On the  $\gamma$  factor, the two algorithms proposed in this paper are undoubtedly superior to the existing algorithms.

## 6. Conclusion

This paper studies the participant selection method in the multitask situation in MCS. Based on the participant's historical task completion, the reputation and willingness of participants are used to establish a service quality model, aiming at task-centered and participant-oriented for the center; we establish a preferred plan for participants based on service quality. Under the condition of satisfying service quality constraints and distance constraints, the requirements of minimizing platform expenses and maximizing user benefits can be achieved. We establish a data quality pricing function and quantitatively evaluate the data uploaded by participants. In terms of experimental evaluation, we have compared multiple index factors with the T-Most and PT-Most. The experimental results show that the two algorithms proposed in this paper have no obvious gap with the comparison algorithm in terms of participant selection evaluation indicators. However, in terms of data quality,

our algorithms are significantly better than the control algorithm. Our participant selection program based on QoS can effectively select better participants, thereby greatly increasing platform revenue.

In the follow-up research, we plan to study the heterogeneity of users and the law of historical movement to further improve the quality of service.

## Data Availability

The data used to support the findings of this study have not been made available because our organization has confidentiality measures.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This work has been supported by the National Natural Science Foundation of China (61472136 and 61772196), the Natural Science Foundation of Hunan Province (2020JJ4249), the Social Science Foundation of Hunan Province (2016ZDB006), the Key Project Social Science Achievement Review Committee of Hunan Province (XSP19ZD1005), the Degree and Graduate Education Reform Research Project of Hunan Province (2020JGYB234), the and Scientific Research Project of Hunan Provincial Department of Education (20A131).

## References

- [1] X. Liu, M. S. Obaidat, C. Lin, T. Wang, and A. Liu, "Movement-based solutions to energy limitation in wireless sensor networks: state of the art and future trends," *IEEE Network*, vol. 34, pp. 1–6, 2020.
- [2] Y. Liu, "Crowd sensing computing," *Communications of the ccf*, vol. 8, pp. 38–41, 2012.
- [3] Y. Ruiyun, W. Pengfei, B. Zhihong, and W. Xingwei, "Participatory sensing: people-centric smart sensing and computing," *Journal of computer research and Development*, vol. 54, no. 3, pp. 457–473, 2017.
- [4] T. Huang, J. Liu, S. Wang, C. Zhang, and R. J. Liu, "Survey of the future network technology and trend," *Journal on Communications*, vol. 42, no. 2, pp. 1–23, 2021.
- [5] T. Wang, H. Luo, X. Zeng, Z. Yu, A. Liu, and A. K. Sangaiah, "Mobility based trust evaluation for heterogeneous electric vehicles network in smart cities," *IEEE Transactions on Intelligent Transportation Systems*, vol. 99, pp. 1–10, 2020.
- [6] Y. Liu, T. Feng, M. Peng et al., "COMP: online control mechanism for profit maximization in privacy-preserving crowdsensing," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 7, pp. 1614–1628, 2020.
- [7] X. Zhu, Y. Luo, A. Liu, W. Tang, and M. Z. A. Bhuiyan, "A deep learning-based mobile crowdsensing scheme by predicting vehicle mobility," *IEEE Transactions on Intelligent Transportation Systems*, vol. 99, pp. 1–12, 2020.
- [8] H. Xiong, D. Zhang, L. Wang, and G. Chen, "CrowdRecruiter: selecting participants for Piggyback Crowdsensing under probabilistic coverage constraint," in *Acm International Joint Conference on Pervasive & Ubiquitous Computing*, pp. 703–714, September 2014.
- [9] R. K. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: current state and future challenges," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 32–39, 2011.
- [10] J. Huang, L. Kong, H. N. Dai et al., "Blockchain based mobile crowd sensing in industrial systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6553–6563, 2020.
- [11] F. Restuccia, N. Ghosh, S. Bhattacharjee, S. K. Das, and T. Melodia, "Quality of information in mobile crowdsensing," *ACM Transactions on Sensor Networks (TOSN)*, vol. 13, no. 4, pp. 1–43, 2017.
- [12] J. An, Z. Peng, X. Gui, and L.-L. Xiang, "Research on task distribution mechanism based on public transit system in crowd sensing," *Chinese Journal of Computers*, vol. 42, no. 2, pp. 65–78, 2019.
- [13] W. J. Jiang and X. L. Liu, "Research on anti-greedy incentive mechanism for mobile user recruitment in crowd sensing," *Control and Decision*, vol. 36, pp. 1–10, 2021.
- [14] Y. Wu, J. R. Zeng, H. Peng, H. Chen, and C. P. Li, "Survey on incentive mechanisms for crowd sensing," *Journal of Software*, vol. 27, no. 8, pp. 2025–2047, 2016.
- [15] H. Jin, L. Su, and K. Nahrstedt, "CENTURION: incentivizing multi-requester mobile crowd sensing," in *IEEE INFOCOM 2017-IEEE conference on Computer Communications*, pp. 1–9, Atlanta, GA, USA, May 2017.
- [16] N. Jiang, D. Xu, J. Zhou, H. Yan, T. Wan, and J. Zheng, "Toward optimal participant decisions with voting-based incentive model for crowd sensing," *Information Sciences*, vol. 512, pp. 1–17, 2020.
- [17] Y. Wen, J. Shi, Q. Zhang et al., "Quality-driven auction-based incentive mechanism for mobile crowd sensing," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 9, pp. 4203–4214, 2015.
- [18] Z. Sheng, C. Mahapatra, C. Zhu, and V. C. M. Leung, "Recent advances in industrial wireless sensor networks toward efficient management in IoT," *IEEE access*, vol. 3, pp. 622–637, 2015.
- [19] Y. Sei and A. Ohsuga, "Differentially private mobile crowd sensing considering sensing errors," *Sensors*, vol. 20, no. 10, p. 2785, 2020.
- [20] B. Tian, Y. Yuan, H. Zhou, and Z. Yang, "Pavement management utilizing mobile crowd sensing," *Advances in Civil Engineering*, vol. 2020, 16 pages, 2020.
- [21] J.-S. Lee and B. Hoh, "Sell your experiences: a market mechanism based incentive for participatory sensing," in *2010 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 60–68, Mannheim, Germany, April 2010.
- [22] M. Xiao, J. Wu, L. Huang, Y. Wang, and C. Liu, "Multi-task assignment for crowdsensing in mobile social networks," in *2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 2227–2235, Hong Kong, China, April 2015.
- [23] H. Jin, L. Su, H. Xiao, and K. Nahrstedt, "Incentive mechanism for privacy-aware data aggregation in mobile crowd sensing systems," *IEEE/ACM Transactions on Networking*, vol. 26, no. 5, pp. 2019–2032, 2018.
- [24] J. Hu, Z. Wang, J. Wei et al., "Towards demand-driven dynamic incentive for mobile crowdsensing systems," *IEEE*



- Transactions on Wireless Communications*, vol. 19, no. 7, pp. 4907–4918, 2020.
- [25] J. Xu, Z. Rao, L. Xu, D. Yang, and T. Li, “Incentive mechanism for multiple cooperative tasks with compatible users in mobile crowd sensing via online communities,” *IEEE Transactions on Mobile Computing*, vol. 19, no. 7, pp. 1618–1633, 2019.
- [26] B. Guo, H. Chen, Q. Han, Z. Yu, D. Zhang, and Y. Wang, “Worker-contributed data utility measurement for visual crowdsensing systems,” *IEEE Transactions on Mobile Computing*, vol. 16, no. 8, pp. 2379–2391, 2016.
- [27] J. Zhou, Z. Y. Yu, W. Z. Guo, L. K. Guo, and W. P. Zhu, “Participant selection algorithm for t-sweep k-coverage crowd sensing tasks,” *Computer Science*, vol. 45, no. 2, pp. 157–164, 2018.
- [28] R. Estrada, R. Mizouni, H. Otrok, A. Ouali, and J. Bentahar, “A crowd-sensing framework for allocation of time-constrained and location-based tasks,” *IEEE Transactions on Services Computing*, vol. 13, no. 5, pp. 769–785, 2017.
- [29] L. Pu, X. Chen, J. Xu, and X. Fu, “Crowd foraging: A QoS-oriented self-organized mobile crowdsourcing framework over opportunistic networks,” *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 4, pp. 848–862, 2017.
- [30] R. Azzam, R. Mizouni, H. Otrok, S. Singh, and A. Ouali, “A stability-based group recruitment system for continuous mobile crowd sensing,” *Computer Communications*, vol. 119, pp. 1–14, 2018.
- [31] S. Yang, F. Wu, and G. Chen, “On designing most informative user selection methods for mobile crowdsensing,” *Chinese Journal of Computers*, vol. 43, no. 3, pp. 409–422, 2020.
- [32] E. Wang, Y. Yang, J. Wu, W. Liu, and X. Wang, “An efficient prediction-based user recruitment for mobile crowdsensing,” *IEEE Transactions on Mobile Computing*, vol. 17, no. 1, pp. 16–28, 2017.
- [33] H. Li, T. Li, W. Wang, and Y. Wang, “Dynamic participant selection for large-scale mobile crowd sensing,” *IEEE Transactions on Mobile Computing*, vol. 18, no. 12, pp. 2842–2844, 2018.
- [34] Y. Liu, B. Guo, W. Wu, Z. Yu, and D. Zhang, “Multitask-oriented participant selection in mobile crowd sensing,” *Chinese Journal of Computers*, vol. 40, no. 8, pp. 1872–1887, 2017.
- [35] D. J. Hardisty, K. C. Appelt, and E. U. Weber, “Good or bad, we want it now: fixed-cost present bias for gains and losses explains magnitude asymmetries in intertemporal choice,” *Journal of Behavioral Decision Making*, vol. 26, no. 4, pp. 348–361, 2013.
- [36] C. Miao, H. Yu, Z. Shen, and C. Leung, “Balancing quality and budget considerations in mobile crowdsourcing,” *Decision Support Systems*, vol. 90, pp. 56–64, 2016.

## Research Article

# Anti-Attack Scheme for Edge Devices Based on Deep Reinforcement Learning

Rui Zhang <sup>1</sup>, Hui Xia <sup>1</sup>, Chao Liu <sup>1</sup>, Ruo-bing Jiang <sup>1</sup> and Xiang-guo Cheng <sup>2</sup>

<sup>1</sup>The College of Information Science and Engineering, Ocean University of China, Qingdao 1266100, China

<sup>2</sup>The College of Computer Science and Technology, Qingdao University, Qingdao 1266100, China

Correspondence should be addressed to Hui Xia; [xiahui@ouc.edu.cn](mailto:xiahui@ouc.edu.cn) and Xiang-guo Cheng; [chengxg@qdu.edu.cn](mailto:chengxg@qdu.edu.cn)

Received 9 December 2020; Revised 9 March 2021; Accepted 29 March 2021; Published 15 April 2021

Academic Editor: Yaguang Lin

Copyright © 2021 Rui Zhang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Internet of Things realizes the leap from traditional industry to intelligent industry. However, it makes edge devices more vulnerable to attackers during processing perceptual data in real time. To solve the above problem, we use the zero-sum game to build the interactions between attackers and edge devices and propose an antiattack scheme based on deep reinforcement learning. Firstly, we make the  $k$  NN-DTW algorithm to find a sample that is similar to the current sample and use the weighted moving mean method to calculate the mean and the variance of the samples. Secondly, to solve the overestimation problem, we develop an optimal strategy algorithm to find the optimal strategy of the edge devices. Experimental results prove that the new scheme improves the payoff of attacked edge devices and decreases the payoff of attackers, thus forcing the attackers to give up the attack.

## 1. Introduction

Internet of Things (IoT) [1, 2] integrates various sensors or controllers with sensing and monitoring capabilities as well as advanced technologies (e.g., mobile communication technology and intelligent analysis technology) into all aspects of industrial production, realizing the leap from traditional industry to intellect industry. It has been widely used in logistics [3, 4], transportation [5], energy [6], and so on. During the application process of IoT, mass perception data is produced in end devices, which requires the edge devices to have higher real time, security [7, 8], and privacy [9, 10]. However, edge devices are usually located in a nearby user or on a routing path to the cloud, making them more vulnerable to attackers. For example, machine learning models on edge devices during the training period are vulnerable to well-designed adversarial examples [11, 12]. UPGUARD, an American cybersecurity firm, found that hundreds of millions of Facebook user records stored on Amazon's cloud computing servers could be easily accessed by anyone. Tens of thousands of private Zoom videos are uploaded to the public web page that anyone can watch online.

The above threats can cause network penetration, personal data theft, and the epidemic spread of intelligent computer viruses. Therefore, preventing attacks and ensuring data security are the key to improve the efficient application of this system.

Currently, resisting malicious attackers mostly adopts traditional skills in IoT, such as encryption method and identity management technology. The encryption method is the most common traditional skill [13, 14]. However, due to the limited resources of edge devices in IoT, making the lightweight encryption program becomes one of the biggest challenges. Identity management technologies are the first line of resisting malicious attackers. However, the existing identity management technology cannot achieve identity authentication between multi-layer architectures. In recent years, a few emerging safety precaution technologies are widely used in IoT [15–17], such as trusted execution environments and machine learning technologies. However, most machine learning technologies, which are based on the assumption that training data remains constant during training, are incompatible with the environment where the data changes dynamically in real-time in IoT [18, 19].

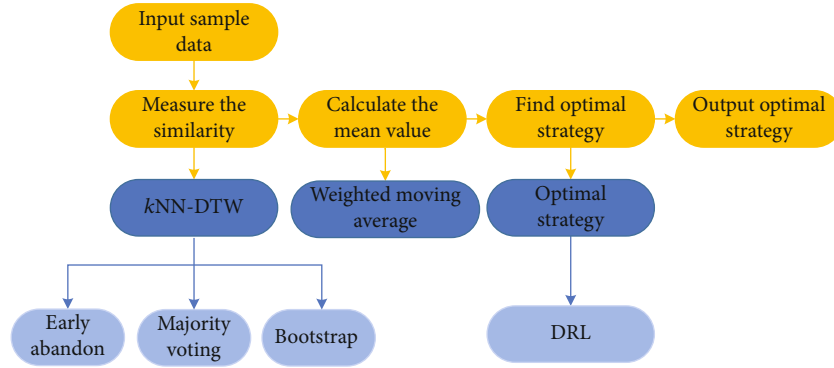


FIGURE 1: The structure diagram of the proposed scheme.

Inspired by the above schemes, from the point of view of attacker payoffs, we build the interactions between edge devices and attackers as the zero-sum game and propose an antiattack scheme for edge devices based on deep reinforcement learning. The structure diagram of the proposed scheme is shown in Figure 1. The major contributions are as follows:

- (1) To find the optimal strategy of edge devices, we propose the  $k$  NN-DTW algorithm to find a similar sample to the current sample and then use the weighted moving mean method to calculate the mean and the variance of the samples;
- (2) To weaken the influence of time series' irregularity, we emphasize the influence of the latest data on forecast value and then set weight for samples by the law that the object is big when near and small when far;
- (3) To overcome the overestimation problem of the optimal strategy, we design an optimal strategy algorithm to find the edge device's optimal strategy by maximizing their accumulated payoff and then achieve the purpose of defending against attackers.

The structure of this paper is as follows: in Section 2, we define problems that we seek to solve in this article. In Section 3, we discuss the antiattack scheme for edge devices. In Section 4, we verify the effectiveness of the antiattack scheme for edge devices. Section 5 contains conclusions and future research.

## 2. Related Work

This section introduces the latest development and research of antiattack schemes from two aspects: traditional security protection schemes and emerging security protection schemes in IoT.

**2.1. Traditional Safety Precaution Technologies.** Homomorphic encryption, differential privacy, and identity authentication are three traditional protection technologies. Homomorphic encryption can process sensitive data without decryption to protect data privacy. Lu et al. [20] encrypted structured data by using homomorphic Paillier crypto-

graphic system technology. Tan et al. [21] used the technique of finite field theory and proposed a private comparison algorithm based on full homomorphic encryption for encrypted integers. Differential privacy technology is used to ensure the privacy of any single item in the data set under the statistical query. Wang [22] proposed a data-driven spectrum trading solution that could maximize the income of PUS and retain SU's privacy differences. However, the computing resources on the edge devices are quite limited and cannot support the huge computing power consumed by using encryption schemes. Identity management technologies can set access authority by identity management and access control to prevent illegal user intrusion. Alizadeh et al. [23] summarized authentication technology in mobile cloud computing. Malik et al. [24] proposed an identity authentication and expeditious revocation framework based on the blockchain, which can quickly update the status of revoked vehicles in the shared blockchain. Zhang et al. [25] proposed a smart contract framework comprised of several access control contracts, a judge contract, and a registered contract, which gave a trusted access control strategy. However, using an access control strategy for precautions makes it hard to clear different users' roles and their rights in IoT.

**2.2. Emerging Safety Precaution Technologies.** The improvement of traditional security schemes can be used to enhance the security of edge devices in the IoT [26]. With the rise of artificial intelligence, some emerging security prevention technologies, such as trusted execution environment and machine learning technology, are gradually used to improve the security of edge devices in the IoT. The trusted execution environment [27] can be used to ensure the security of the running environment of the software. Running an application in a trusted execution environment can guarantee the security of data even if edge devices are compromised. Trusted execution environment, such as trustzone, intel management engine, and ARM trustzone, are quite popular. Han et al. [28] built a complete framework that supports visibility into encrypted traffic and can be used in secure and functional networks. However, trusted execution environment usually has its loophole, such as Qualcomm loopholes, and trustonic loopholes. Ghaffarian and Shahriari [29] proposed a neural vulnerability analysis method based on custom intermediate graph representation of the program for

software vulnerability analysis. Scandariatio et al. [30] explored machine learning-based text mining to predict security loopholes in a software source code. However, most machine learning methods assume that statistical data remain unchanged during the training process, but the data in the IoT changes dynamically in real time.

### 3. Problem Definition

In this article, we build the interactions between edge devices and attackers as a zero-sum game [31]. Namely, the payoff of attackers equals the loss of edge devices. In each round of interaction, the attacker attacks the sample from edge devices to gain illegal payoff, and the edge device plays his strategy to defend against attackers. Previous studies usually determine the optimal strategy of edge devices by calculating the Nash equilibrium in the handcrafted abstraction of the domain [32]. Currently, some researchers introduce the recursion technique to the neural network to determine players' optimal strategy by predicting human action in a strategic environment. From [33], the payoff function of edge devices can be defined as

$$U(a, \mu, C) = \log(a^T \mu) - \frac{1}{2 * (a^T \mu)^2} a^T C a, \quad (1)$$

where  $a$  is the strategy vector of edge devices, that is,  $a = \{a_1, a_2, \dots, a_n\}^T$ ;  $\mu, \mu = \{\mu_1, \mu_2, \dots, \mu_n\}^T$  is sample mean payoff; and  $C$  is the covariance matrix of sample payoff. As can be seen from Equation (1), if we know the sample mean payoff and the covariance matrix, we can determine the optimal strategy of edge devices by maximizing the payoff function. That is,

$$a^{opt} \in \arg \max_a U(a, \mu, C). \quad (2)$$

However, the sample mean payoff and the covariance matrix are unknown. But, we can take advantage of the similarity between the historical sample and current sample to predict the sample mean payoff and the covariance matrix and then determine the optimal strategy of the edge device.

When we determine the optimal strategy of the edge device, we should try to resolve the following three problems: (1) during the process of measuring similarity between samples, we need to avoid using improper measuring methods which might cause the disappearance of optimal solution; (2) during the process of calculating the sample mean payoff and covariance matrix, we need to weaken the influence of time series' irregularity; (3) during the process of finding the optimal strategy of edge devices, we need to break the correlation between training samples and solve the problem of overestimation.

### 4. Antiattack Scheme for Edge Devices

This section introduces the following three problems that we seek to solve: how to find the sample that are similar to the current sample, how to calculate the mean value and the

covariance matrix, and how to calculate the optimal strategy of edge devices to resist attackers.

*4.1. Measuring Similarity of Sample.* To find a sample similar to the current sample, we propose the  $k$  NN-DTW algorithm to determine the category of the current sample and then find the similar sample with the current sample. The  $k$  NN-DTW algorithm is a combination of the  $k$ -nearest neighbor algorithm and the dynamic time warping method (DTW); the  $k$  NN algorithm classifies the current sample and the DTW method finds the similar sample in the same category samples with the current sample.

In the  $k$  NN algorithm, the choice of  $k$  has a significant impact on the classification results. We use the bootstrap method to find the optimal value of  $k$ . Assuming the value of  $k$  and the probability of time series being correctly classified  $\rho$  satisfy the following regression model:

$$\rho_i = h(k_i, \beta) + \varepsilon, i = 1, 2, \dots, n, \quad (3)$$

where  $h(\cdot)$  is the mapping from  $k$  to  $\rho$ ,  $\beta$  is a coefficient vector, and  $\{\varepsilon_i\}$  is a numerical vector, i.e.,  $F(x)$ . We use the least square method to estimate  $\beta$ , i.e.,  $\hat{\beta} = g(\rho_1, \dots, \rho_n)$ , make the regression residual empirical distribution function to estimate  $F(x)$ , and apply the bootstrap method to estimate the covariance matrix  $\text{Var}(\hat{\beta})$  of  $\beta$ . If the estimation error of each coefficient (the square root of the diagonal element in  $\text{Var}(\hat{\beta})$ ) meets the threshold  $\varepsilon_0$ , the value of  $k$  can be determined by maximizing  $\rho$ .

After the category of the current sample is determined by  $k$  NN, we use DTW to measure the distance between the current sample and the historical sample. DTW method locally scales two samples on the time axis to make the morphology of the two sets, so that the DTW method can measure the distance between time samples that have different lengths. Comparing with *Euclidean distance*, the DTW method is more elastic and supports local time shifts and in the length of time series, but the time and special complexity of this method is  $O(nm)$ , where  $n$  and  $m$  are the lengths of two time series, respectively. To decrease the space and time complexity of the DTW method, we apply early abandoning method to optimize the computations of the DTW method. The detailed process is as follows:

Step 1. Given two time series  $X$  and  $Y$ ,

$$\begin{aligned} X &= (x_1, x_2, \dots, x_n), \\ Y &= (y_1, y_2, \dots, y_m), \end{aligned} \quad (4)$$

where  $n$  is the length of time series  $X$ , and  $m$  is the length of time series  $Y$

Step 2. Define the warping path as  $P = p_1, p_2, \dots, p_K$ , where  $\max(n, m) < K < m + n + 1$ ,  $p_k = (i, j)$  is the  $k$ th element in warping path  $P$ ,  $i$  is the  $i$ th cell of time series  $X$ , and  $j$  is the  $j$ th cell of time series  $Y$ , the  $i$  and  $j$  of  $p_k = (i, j)$  are monotonically increasing,

$$p_k = (i, j), p_{k+1} = (i', j'), i \leq i' \leq i + 1, j \leq j' \leq j + 1. \quad (5)$$

Specially, when calculating warping path, it must ensure that every coordinate in the time series  $X$  and  $Y$  is involved. That is, the calculation starts from  $p_1 = (1, 1)$  and ends at  $p_k = (n, m)$

Step 3. Find the warping path between two time series with the shortest cumulative distance,

$$P = \arg \min_{p_k \in P} \sum_{k=1}^K p_k. \quad (6)$$

To obtain the warping path with the shortest cumulative distance, Eq. (6) can be solved iteratively by using the dynamic programming method

$$D(i, j) = \text{Dist}(i, j) + \min \{D(i-1, j), D(i, j-1), D(i-1, j-1)\} \quad (7)$$

Step 4. Set the distance threshold  $\varepsilon$ ,  $\varepsilon > 0$ , if the distance  $D(i, j) > \varepsilon$  in cell  $(i, j)$ , the calculation of the distance between two time series on the path will be terminated

Step 5. Determine the distance between two time series  $D(n, m)$

**4.2. Calculating the Mean Value and the Covariance Matrix.** To weaken the influence of time series' irregularity, we emphasize the influence of the latest data on forecast value and set weight for samples by the law that the object is big when near and small when far. Namely, the sample elements that are close to the prediction period will be given a relatively big weight. We use the weighted moving average method to calculate sample's mean value. That is,

$$\mu_t = \frac{y_t w_t + y_{t-1} w_{t-1} + \dots + y_1 w_1}{w_t + w_{t-1} + \dots + w_1}, \quad (8)$$

where  $w_t$  refers to the weight of sample data  $y_t$ ; it follows the rule that weight decreases as the distance increases, i.e.,  $w_t > w_{t-1} > \dots > w_1$ . Accordingly, the covariance matrix  $C$  can be calculated as

$$C = E[(X - \mu_X)(Y - \mu_Y)]. \quad (9)$$

**4.3. Preventing Malicious Attacks.** After finding the similar sample, we first take the mean payoff and covariance matrix of the similar sample as the mean payoff and covariance matrix of the current sample, respectively. And then, to weaken the influence of time series irregularity, we emphasize the influence of the latest data on forecast value and set weight for samples by the law that the object is big when near and small when far. Finally, we find the solution to the optimal strategy of edge devices by maximizing the payoff function. The detailed process is shown in Algorithm 1.

However, the above method is prone to overestimation. To solve the above problem, we design Algorithm 2 to find the optimal strategy of the edge devices by maximizing their accumulated payoff.

Reinforcement learning is aimed at maximizing the reward for the long term to find the payoff maximum of

```

Input: Similarity sample set  $W$ ;
Output: Optimal strategy  $a^{\max}$ ;
1: for  $n = 2: N$  do
2:   Calculate similarity with DTW;
3:   if similarity < 1 then
4:     Continue;
5:   else:
6:      $U_p = \max_a U(a, \mu, C)$ ;
7:   end for
8: return  $a^{\max}$ 

```

ALGORITHM 1: Optimal strategy.

the agent. Thus, players of the game are transformed into separate agents. We use *Deep Q Network* to find the agent's optimal strategy. In this algorithm, the state set  $S$  of agent is defined as  $S = \{s_1, s_2\}$ , where  $s_1$  means that the current data is normal (not attacked) and  $s_2$  means that the current data is abnormal (already attacked); the above states can be described by the *Markov decision process*. The action set  $A$  is defined as  $A = \{a_1, a_2\}$ , where  $a_1$  means that the *agent* accepts the current data set,  $a_2$  means that the *agent* rejects the current data set, and action reward  $R$  is defined as

$$R = \begin{cases} 1, & a = a_1, s = s_1 \text{ or } a = a_2, s = s_2, \\ -1, & \text{others.} \end{cases} \quad (10)$$

The agent interacts with its fellow agents and stores its experience of strategy transitions  $(s_j, a_j, r_j, s_{j+1})$  in replay memory  $R$ . To break the correlation between training samples, during the process of training, we select samples randomly from replay memory  $R$  to train model for finding the optimal strategy of the agent. The detailed process is shown Algorithm 2, where  $\hat{Q}$  is the payoff when the agent adopts the optimal strategy.

## 5. Stimulation Results

We use the Anaconda-integrated development tool to validate the proposal. First, we analyze the feasibility of weakening the influence of time series irregularity to prove the reasonableness of setting sample data's weight according to the rule of the object being big when near and small when far. Second, we compare the *DTW* method with seven classical distance methods like *correlation distance*, *Jaccard distance*, and cosine distance to verify the reasonableness of *k NN-DTW*. Finally, we apply optimal strategy to the rock-paper-scissors game [34] to verify the practicability of optimal strategy by comparing the winner (choose winner's strategy) and opponent (choose opponent's strategy) strategies.

**5.1. Feasibility Analysis of Weakening the Influence of Time Series Irregularity.** Tables 1–3 analyze the influence of weighting weights on each parameter in the target payoff function according to the law that the object is big when near and small when far. To better describe the complete process,



```

01: Initialize replay memory  $R$ ;
02: Initialize anticipatory parameters  $\eta$ ;
03: Initialize target function  $Q$  with weight  $\vartheta$ ;
04: forepisode = 1, Mdo
05: Set policy  $\sigma \leftarrow \begin{cases} a^{opt}, \eta \\ \beta, 1 - \eta \end{cases}$ ;
06: Receive initial observation state  $s_1$  and reward  $r_1$ ;
07: fort = 1, Tdo
08: Select action at from policy  $\sigma$ ;
09: Execute action at and observe reward  $r_{t+1}$  and observe new state  $s_{t+1}$ ;
10: Store transition  $(s_t, a_t, r_{t+1}, s_{t+1})$  in  $R$ ;
11: Sample random minibatch of transition  $(s_j, a_j, r_j, s_{j+1})$  from  $R$ 
12: if terminates at step  $t + 1$  then
13:    $Q_t = r_t$ ;
14: else
15:    $Q_t = r_t + r \max_{a_{t+1}} Q(\eta a_t + (1 - \eta)\beta | s_t)$ ;
16: end if
17: Perform a gradient descent step on  $(\bar{Q} - Q_t)^2$  with respect to network parameters;
19: Periodically update the target networks  $Q$ ;
20: end for
21: end for

```

ALGORITHM 2: Optimal strategy.

TABLE 1: Sample dataset.

Number	Data 1	Data 2	Data 3	Data 4	Weight
1	22.44	21.95	21.96	15.82	0.099066
2	23.01	21.94	22.67	16.69	0.08585
3	23.1	22.4	22.4	16.43	0.082904
4	23.2	21.7	21.88	15.84	0.07981
5	21.51	20.85	21.44	15.66	0.078681
6	22.08	21.3	21.45	16.2	0.073956
7	21.86	21.15	21.79	15.97	0.07361
8	21.39	20.77	21.11	16.65	0.07244
9	21.43	20.85	21.23	16.45	0.067382
10	21.48	20.96	21.25	15.89	0.051061
11	21.19	20.8	21.1	16.56	0.046455
12	22	21.24	22	16.54	0.045742
13	22.47	21.5	21.64	16.28	0.03978
14	21.6	20.74	20.81	16.44	0.03306
15	20.48	19.51	19.88	16.11	0.028871
16	20.19	19.75	19.8	15.9	0.019483
17	20.06	18.16	18.59	15.1	0.010127
18	18.77	18.06	18.31	14.51	0.004814
19	18.35	17.6	18.2	14.06	0.003591
20	18.41	17.73	17.99	13.88	0.003319

we set each sample dataset only has 20 data and make the weight for each sample, as shown in Table 1. Table 2 shows the prediction error between the weighted mean and mean under the same strategy profile (1, 1, 1, 0), where 1 means that the edge device accepts the data, and 0 means that the edge device rejects the data.

TABLE 2: Player's mean payoff comparison.

Value	Data 1	Data 2	Data 3	Data 5
Mean payoff	21.251	20.448	20.775	15.849
Weight mean payoff	21.9937	21.219	21.5435	16.1693
Error	0.742695	0.771	0.7685	0.3203
Action	1	1	1	0

Table 3 shows the effects of weakening the influence of time series irregularity on the parameters of the objective function (e.g.,  $C$ ). According to the table, setting the weight of the data according to the rule of the object is big when near and small when far has a greater influence on  $C$  and a weaker influence on  $\log(a^T \mu)$ . Therefore, the proposed method can weaken the irregularity of the time series.

*5.2. Verification of the Reasonableness of  $k$  NN-DTW.* To verify the reasonableness of combining  $DTW$  method and  $k$  NN algorithm, Figure 2 shows the  $DTW$  method with seven classical distance methods like *correlation distance*, *Jaccard distance*, and *cosine distance*. From Figure 2, we can see that the *cosine distance* and *Chebyshev distance* are the worst. For example, when the ratio of the same elements in the range from 20% to 33%, the results of the *Cosine distance* are all 0.79 while the ratio of the same elements in the range from 6% to 67%; the results of the *Cosine distance* are all 0.66. Therefore, *cosine distance* and *Chebyshev distance* are not suitable for measuring the distance between the samples in this paper. Although other methods also produce the same results, the number of the same results is less than that of *cosine distance* and *Chebyshev distance*. For example, the results of the  $DTW$  method are the same if and only if the ratio of the same elements is 80% or 87%. And the results

TABLE 3: The influence of time series irregularity.

Parameter	$a^T \mu$	$C$	$a^T Ca$	$\log(a^T \mu)$
No-weight	62.47	$\begin{bmatrix} 2.15 & 2.10 & 2.07 & 0.99 \\ 2.10 & 2.18 & 2.14 & 1.03 \\ 2.07 & 2.14 & 2.15 & 1.03 \\ 0.99 & 1.03 & 1.03 & 0.69 \end{bmatrix}$	19.09	1.80
Weight	64.76	$\begin{bmatrix} 0.49 & 0.48 & 0.48 & 0.35 \\ 0.48 & 0.46 & 0.47 & 0.34 \\ 0.48 & 0.47 & 0.48 & 0.35 \\ 0.35 & 0.34 & 0.35 & 0.25 \end{bmatrix}$	4.29	1.81

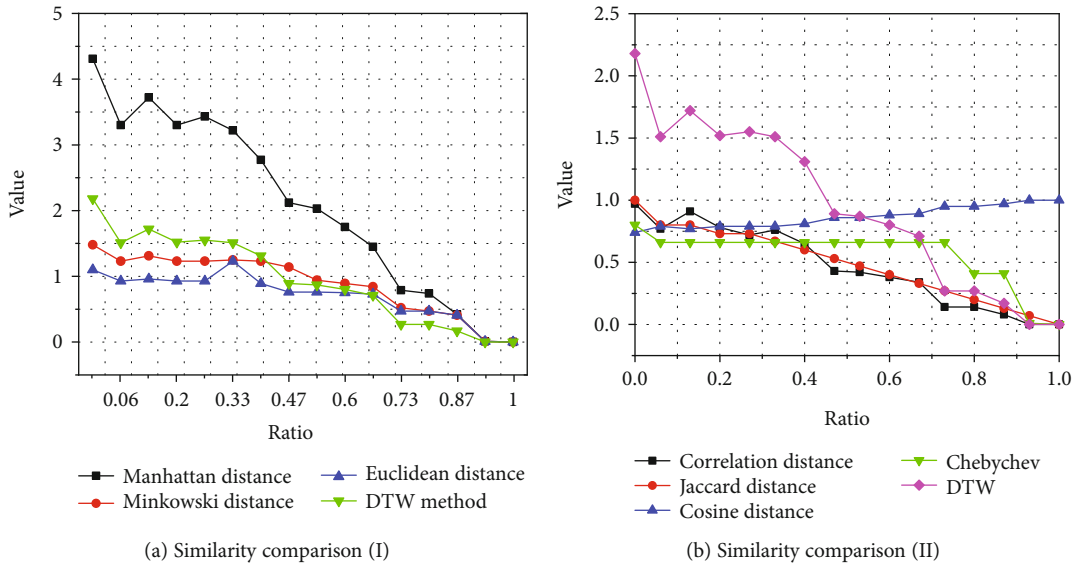


FIGURE 2: Similarity comparison.

TABLE 4: Payoff matrix.

Player1/2	Rock	Scissors	Paper
Rock	0, 0	2, -2	-2, 2
Scissors	-2, 2	0, 0	2, -2
Paper	2, -2	-2, 2	0, 0

of *Euclidean distance* are the same if and only if the ratio of the same elements is 47% or 53%.

By comparing Figures 2(a) and 2(b), it can be seen that *DTW* method works best, followed by *Jaccard distance*. For example, when the number of the same elements is 80%, 87%, and 93%, the results of *Jaccard distance* are 0.2, 0.13, and 0.07; the results of *Euclidean distance* are 0.52, 0.41, and 0.01; the results of *Manhattan distance* are 0.74, 0.42, and 0.01; and the results of *DTW* method are 0.27, 0.17, and 0.0004, respectively. From the above results, we can draw a conclusion that *Euclidean distance* and *Manhattan distance* have a similar impact on measuring the distance between

samples, while the results measured by these two methods varied greatly when the data in the two samples varied from 87% to 93%. While the *Jaccard distance* and *DTW* method have a similar impact measuring the distance between samples, the results measured by these two methods varied slightly when the data in the two samples varied from 87% to 93%. The *DTW* method is more suitable for measuring the distance between samples; this is because the *DTW* method can measure the distance between samples of different lengths. Therefore, we combine the *DTW* method with the *k NN* algorithm to measure the distance between samples.

**5.3. Application of Antiattack Scheme.** First, we need to define the rock-paper-scissors game's payoff matrix, as shown in Table 4. The rock-paper-scissors game is a typical example of zero-sum game. In the game, two players have the same strategy set, which is (rock, paper, scissors). If two players play the same strategy, then both of them get 0 for a draw; otherwise, the winner gets 2 and the loser gets -2.

Figure 3 shows the changing trend of payoff that player 1 and player 2 play optimal strategy, winner strategy, and opponent strategy in the initial states  $S_0 = \{\text{scissors, rock}\}$

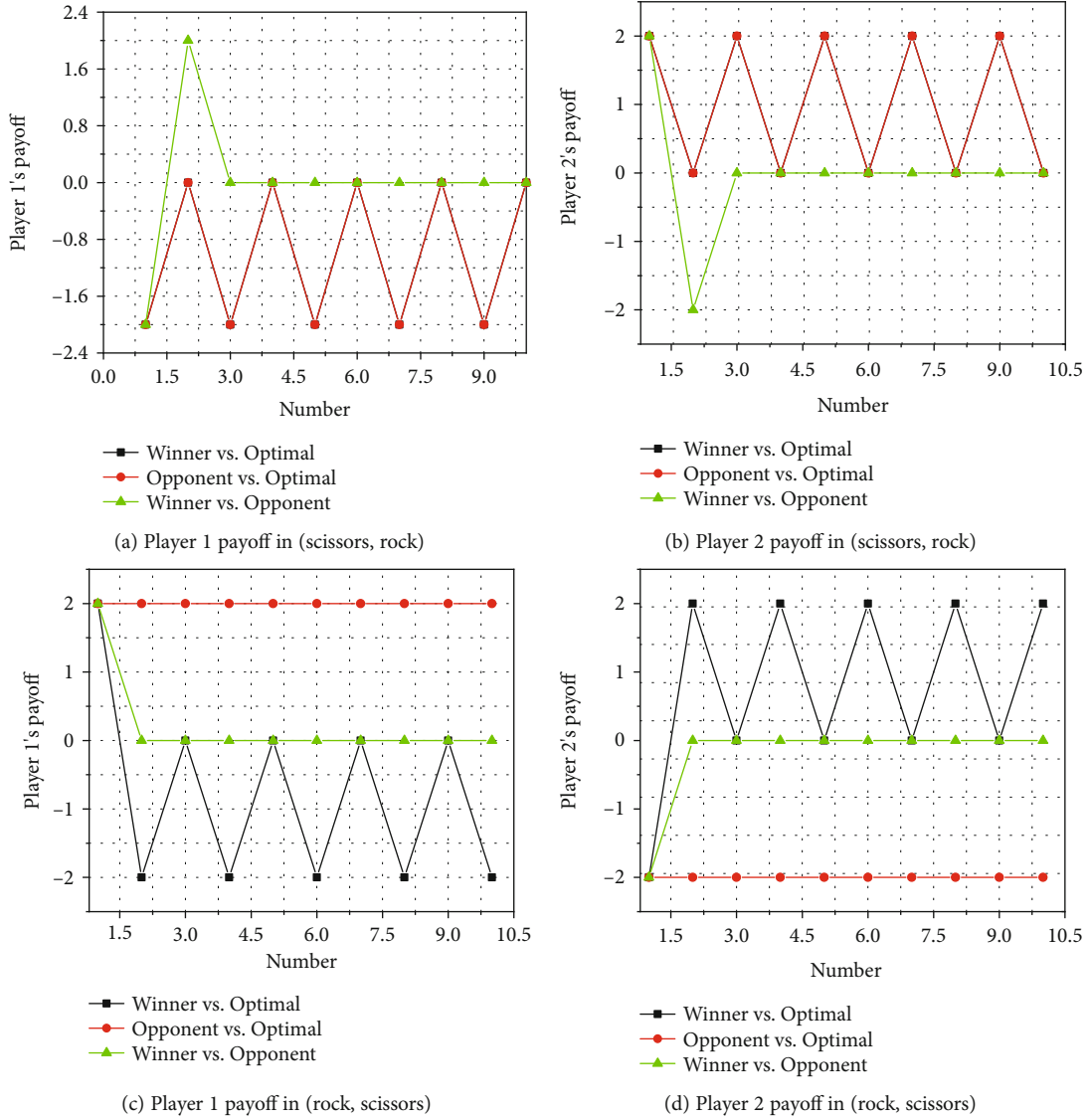


FIGURE 3: Payoff comparison.

TABLE 5: Total payoff comparison.

Players	Winner	Opponent	Optimal
Total	-16	8	8

and  $S_1 = \{\text{rock, scissors}\}$ . In the figure, winner vs. optimal means that player 1 plays winner strategy and player 2 players optimal strategy in the game. Similarly, we can know the meaning of opponent vs. optimal and winner vs. opponent. Figures 3(a)–3(d) show the payoff of player 1 and player 2 in  $S_0$  and  $S_1$  states, respectively. From Figure 3(a), we can see that due to player 1 adjusts scissors strategy to rock strategy when starting the second round of the game, the payoff of player 1 is -2 in the first round, and the payoff of player 1 is 2 in the second round. It is worth noting that the payoff trend of player 1 and player 2 is the same in winner vs. optimal and opponent vs. optimal because the strategies adjusted by winner strategy and opponent are the same in

the initial state  $S_0$ . According to Figures 3(a)–3(d), we can draw a conclusion that the optimal strategy is optimal in state  $S_0$ , while in state  $S_1$ , optimal strategy is superior to winner strategy and inferior to opponent. As can be seen Table 5, the overall payoff of players is same in opponent strategy and optimal strategy. To sum up, optimal strategy scheme can help to determine the player’s strategy and maximize the player’s payoff.

## 6. Conclusion

In *IoT*, defending against attacks by determining the optimal strategy of the edge device for ensuring data security is the key to improve its effectiveness. In this article, we propose an antiattack scheme for edge devices based on deep reinforcement learning to solve this issue. And the core of this scheme is the optimal strategy algorithm. Detailed simulation experiment verified the effectiveness of this new scheme.

In future studies, we will focus on creating a new methodology to determine the similarity between data samples and use machine learning approaches to solve more data security problems.

## Data Availability

All data generated or analyzed during this study are included in this article.

## Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

## Acknowledgments

This research is supported by the National Natural Science Foundation of China (NSFC) under Grant No. 61872205, the Shandong Provincial Natural Science Foundation under Grant No. ZR2019MF018, and the Source Innovation Program of Qingdao under Grant No. 18-2-2-56-jch.

## References

- [1] N. Lin, X. P. Wang, Y. H. Zhang, X. Hu, and J. Ruan, "Fertigation management for sustainable precision agriculture based on Internet of Things," *Journal of Cleaner Production*, vol. 277, article 124119, 2020.
- [2] S. Chen, Y. Tao, D. Yu, F. Li, and B. Gong, "Privacy-preserving collaborative learning for multiarmed bandits in IoT," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3276–3286, 2021.
- [3] W. Liu, S. Wang, D. Dong, and J. Wang, "Evaluation of the intelligent logistics eco-index: evidence from China," *Journal of Cleaner Production*, vol. 274, article 123127, 2020.
- [4] F. Basso, J. Leonardo, and M. Ronnqvist, "Coalition formation in collaborative production and transportation with competing firms," *European Journal of Operational Research*, vol. 289, no. 2, pp. 569–581, 2021.
- [5] Y. Yan, Q. Li, W. Huang, and W. Chen, "Operation optimization and control method based on optimal energy and hydrogen consumption for the fuel cell/supercapacitor hybrid tram," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 2, pp. 1342–1352, 2021.
- [6] S. R. Pokhrel, H. L. Vu, and A. L. Cricenti, "Adaptive admission control for IoT applications in home WiFi networks," *IEEE Transactions on Mobile Computing*, vol. 19, no. 12, pp. 2731–2742, 2019.
- [7] Y. Liang, Z. Cai, J. Yu, Q. Han, and Y. Li, "Deep learning based inference of private information using embedded sensors in smart devices," *IEEE Network*, vol. 32, no. 4, pp. 8–14, 2018.
- [8] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.
- [9] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: a survey," in *Wireless Algorithms, Systems, and Applications. WASA 2015*, K. Xu and H. Zhu, Eds., vol. 9204 of Lecture Notes in Computer Science, pp. 685–695, Springer, Cham, 2015.
- [10] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2018.
- [11] T. Tsiligkaridis, "Information Aware max-norm Dirichlet networks for predictive uncertainty estimation," *Neural Networks*, vol. 135, pp. 105–114, 2021.
- [12] B. Henz, E. Gastal, and M. Oliveira, "Synthesizing camera noise using generative adversarial networks," *IEEE Transactions on Visualization and Computer Graphics*, vol. 27, no. 3, pp. 2123–2135, 2021.
- [13] H. Wang, J. Ning, X. Huang, G. Wei, G. S. Poh, and X. Liu, "Secure fine-grained encrypted keyword search for e-healthcare cloud," *IEEE Transactions on Dependable and Secure Computing*, 2019.
- [14] H. Cheng, H. Wang, X. Liu, Y. Fang, M. Wang, and X. Zhang, "Person re-identification over encrypted outsourced surveillance videos," *IEEE Transactions on Dependable and Secure Computing*, 2019.
- [15] H. Xia, L. Li, X. Cheng, X. Cheng, and T. Qiu, "Modeling and analysis botnet propagation in social internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7470–7481, 2020.
- [16] Z. Cai and T. Shi, "Distributed query processing in the edge assisted IoT data monitoring system," *IEEE Internet of Things Journal*, 2020.
- [17] S. Chen, Y. Tao, D. Yu, F. Li, and B. Gong, "Distributed learning dynamics of multi-armed bandits for edge intelligence," *Journal of Systems Architecture*, vol. 114, article 101919, 2021.
- [18] F. Li, D. Yu, H. Yang, J. Yu, and K. Holger, "Multi-armed-bandit-based spectrum scheduling algorithms in wireless networks: a survey," *IEEE Wireless Communications Magazine*, vol. 27, no. 1, pp. 24–30, 2020.
- [19] T. Zhu, T. Shi, J. Li, Z. Cai, and X. Zhou, "Task scheduling in deadline-aware mobile edge computing systems," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4854–4866, 2019.
- [20] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: an efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.
- [21] B. Tan, H. Lee, H. Wang, S. Q. Ren, and A. M. M. Khin, "Efficient private comparison queries over encrypted databases using fully homomorphic encryption with finite fields," *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2020.
- [22] J. Wang, "Data-driven spectrum trading with secondary users' differential privacy preservation," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 1, pp. 438–447, 2019.
- [23] M. Alizadeh, S. Abolfazli, M. Zamani, S. Baharun, and K. Sakurai, "Authentication in mobile cloud computing: A survey," *Journal of Network and Computer Applications*, vol. 61, pp. 59–80, 2016.
- [24] N. Malik, P. Nanda, and A. Arora, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pp. 674–679, New York, NY, USA, 2019.
- [25] Y. Zhang, S. Kasahara, and Y. Shen, "Smart contract-based access control for the internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, 2019.
- [26] Q.-S. Hua, Y. Shi, Z. Cai, X. Cheng, and H. Chen, "Faster parallel core maintenance algorithms in dynamic graphs," *IEEE*

- Transactions on Parallel and Distributed Systems*, vol. 31, pp. 1287–1300, 2020.
- [27] X. Ruan, “Platform Embedded Security Technology Revealed,” in *Safeguarding the Future of Computing with Intel Embedded Security and Management Engine*, p. 272, Apress, 2014.
- [28] J. Han, S. Kim, D. Cho, B. Choi, J. Ha, and D. A. Han, “A secure middlebox framework for enabling visibility over multiple encryption protocols,” *IEEE/ACM Transactions on Networking*, vol. 28, no. 6, pp. 2727–2740, 2020.
- [29] S. Ghaffarian and H. Shahriari, “Neural software vulnerability analysis using rich intermediate graph representations of programs,” *Information Sciences*, vol. 553, pp. 189–207, 2021.
- [30] R. Scandariatio, J. Walden, and A. Hovsesepyan, “Predicting vulnerable software components via text mining,” *IEEE Transactions on Software Engineering*, vol. 40, no. 10, pp. 993–1006, 2014.
- [31] H. Xia, R. Zhang, X. Cheng, T. Qiu, and D. O. Wu, “Two-stage game design of payoff decision-making scheme for crowdsourcing dilemmas,” *IEEE/ACM Transactions on Networking*, vol. 28, no. 6, pp. 2741–2754, 2020.
- [32] H. Xia, F. Xiao, S. Zhang, C.-q. Hu, and X.-z. Cheng, “Trustworthiness inference framework in the social internet of things: a context-aware approach,” *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, pp. 838–846, 2019.
- [33] Y. Guo, X. Fu, Y. Shi, and M. Liu, “Robust log-optimal strategy with reinforcement learning,” 2018, <https://arxiv.org/abs/1805.00205>.
- [34] Z. Cai, X. Zheng, and J. Yu, “A differential-private framework for urban traffic flows estimation via taxi companies,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6492–6499, 2019.



## Research Article

# A Hybrid Alarm Association Method Based on AP Clustering and Causality

Xiao-ling Tao <sup>1,2</sup>, Lan Shi <sup>1</sup>, Feng Zhao <sup>3</sup>, Shen Lu <sup>1</sup> and Yang Peng <sup>1</sup>

<sup>1</sup>Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin 541004, China

<sup>2</sup>Guangxi Cooperative Innovation Centre of Cloud Computing and Big Data, Guilin University of Electronic Technology, Guilin 541004, China

<sup>3</sup>School of Information and Communication, Guilin University of Electronic Technology, Guilin 541004, China

Correspondence should be addressed to Feng Zhao; zhaofeng@guet.edu.cn

Received 6 January 2021; Revised 21 February 2021; Accepted 15 March 2021; Published 30 March 2021

Academic Editor: Zhuojun Duan

Copyright © 2021 Xiao-ling Tao et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Internet of Things (IoT) brought great convenience to people's daily lives. Meanwhile, the IoT devices are facing severe attacks from hackers and malicious attackers. Hackers and malicious attackers use various methods to invade the Internet of Things system, causing the Internet of Things to face a large number of targeted, concealed, and penetrating potential threats, which makes the privacy problem of the Internet of Things suffers serious challenges. But the existing methods and technologies cannot fully identify the attacker's attack process and protect the privacy of the Internet of Things. Alarm correlation method can construct a complete attack scenario and identify the attacker's intention by alarming the alarm data which provides an effective protection for user privacy. However, the existing alarm correlation methods still have the disadvantages of low correlation accuracy, poor correlation efficiency, and strong dependence on the knowledge base. To address these issues, we propose an alarm correlation method based on Affinity Propagation (AP) clustering algorithm and causal relationship. Our method considers that the alarm data triggered by the same attack process has high similarity characteristics, adopts the AP algorithm to improve the correlation efficiency, and at the same time constructs a complete attack process based on the causal correlation idea. The new alarm correlation method has a high correlation effect and builds a complete attack process to help managers identify attack intentions and prevent attacks.

## 1. Introduction

Smart city and intelligent transportation system improved the people's lifestyle. The Internet of Things (IoT) applications brought great convenience to people's lives [1]. IoT is seen as the third wave and revolution in the development of the global information industry after the advent of computers and the Internet. By the huge market scale and broad industry application prospect, IoT has become the current hot research field. With the continuous change of technology and the advent of 5G networks, the scale and complexity of the Internet of Things continue to increase, and the complex network architecture of heterogeneous integration and interconnection of the Internet of Things is facing increasingly prominent security and efficiency issues [2], and data privacy

has also become one of the most important issues in the Internet of Things [3]. The security issue of the Internet of Things has increasingly become a hot issue that people are concerned about today. According to the white paper on the development of China's network security in 2019 [4], in 2018, the size of China's IoT security market reached 8.82 billion, with a growth rate of 34.7%, which was significantly higher than the industry average growth rate. In recent years, viruses, Trojans, vulnerabilities, spyware, and other attacks and threats against the Internet of things emerge in an endless stream. For example, in 2019, security researchers discovered that popular connected or smart home devices sold by large retailers such as Wal-Mart and Best Buy generally have serious security vulnerabilities and privacy issues. Amazon's Ring also has privacy and security issues, as well

as a series of problems such as the terrifying Mirai botnet continues to maintain a high-speed growth, data upload leakage in intelligent cyber-physical systems [5], and privacy protection of data sharing in the industrial Internet of Things [6]. Various advanced multistep attacks are also appearing more and more frequently. Due to their penetration, pertinence, and concealment, they pose a serious threat to the Internet of Things [7]. In addition to this, the types of attacks on the network are becoming more abundant [8], such as worm attacks, vulnerability attacks, denial of service (DoS) attacks, and phishing attacks. Such a series of intrusions have brought severe challenges to the security and privacy protection of the Internet of Things [9].

In the complex network system, correlation analysis of alarm data is of great importance. It is one of the most effective methods for constructing attack scenarios, allowing managers to intuitively analyse attack trends. The principle of the alarm correlation technology is to dig out the internal connection between the attack events through the correlation analysis and processing of the alarm data [10] and further correlate the alarm information to realize the reconstruction of the attack scenario to help the network manager grasp the entire attack process. Identify the attacker's attack intention, which can effectively prevent network attacks and protect the privacy of the Internet of Things.

There are a series of research in the field of alarm correlation, such as causality-based correlation method [11, 12], data mining method [13, 14], and attribute similarity-based correlation method [15, 16]. However, there are still some problems that need to be solved. First of all, the popularization and diversification of the Internet of Things make the network environment more complicated, and the attacks on the network are also complex and changeable [17]. The existing methods cannot build a more comprehensive attack scene against complex intrusion behaviours. Secondly, because of the high false-positive rate of intrusion detection system, the key attack steps are missing. And the existing methods have strong dependence on the knowledge base, thus affecting the accuracy of correlation results, resulting in low correlation accuracy and poor correlation efficiency. Therefore, how to coordinate the relation between correlation accuracy and correlation efficiency to achieve more ideal effect of alarm correlation is an urgent problem.

*1.1. Contributions.* An efficient alarm correlation method is an effective way to reconstruct attack scenarios for helping network administrators to identify attackers' attack intentions and protect network privacy. Therefore, we propose a hybrid method based on Affinity Propagation (AP) clustering algorithm and causality to correlate alarm data. The main contributions of this paper are summarized as follows:

We improve the similarity calculation method in AP algorithm and use the attribute similarity calculation method to replace the traditional similarity measurement method in AP clustering. According to the different properties of alarm data, we define different similarity calculation functions to calculate their similarity. Combined with the weight of each attribute, we calculate the overall similarity of the alarm. Then, use the AP algorithm to cluster the massive alarm data

and classify the alarm data with higher similarity into the same attack scenario. AP clustering algorithm does not rely on prior knowledge to automatically classify attack scenes, which can greatly improve the correlation efficiency of alarm data.

After dividing the attack scenarios, we sort the alarm data in the same attack scenario in the order of attack time and then associate the alarm data of the same attack event in the same attack scenario according to the principle of causality between the attack sequences. Finally, build a complete attack process.

*1.2. Organization.* The remainder of this paper is organized as follows. The related work is introduced in Section 2. We review the conception of AP clustering algorithm and attribute similarity calculation in Section 3. Our scheme is given in Section 4. Section 5 analyses the effectiveness of our proposed method on the honey pot dataset. We conclude this paper in Section 6.

## 2. Related Work

Most of the attacks launched by attackers on the network are composed of multiple interrelated attack actions, these attacks involve multiple intrusions [18]. Alarm correlation is a technology that extracts effective attribute information from a large amount of original alarm data, connects the alarms induced in the same attack step based on certain rules, and reconstructs the attack process, which can effectively identify attack intentions and reduce repeated alarms. In recent years, the correlation analysis of alarm data has always been a research hotspot in the field of network security [19]. So far, many researchers have done a lot of research on alarm data from the perspectives of causality, data mining, and attribute similarity.

The correlation method based on causality is the most common correlation method. It does not require the support of an expert knowledge base and performs related analysis on the alarm data according to the premise and possible consequences of the attack type [20]. Literature [21] proposed an alert correlation framework (RTECA), the type of framework extracts causality based on Bayesian networks in offline mode and constructs an attack graph. Aiming at the problem that the existing association methods fail to identify many distributed attacks, a real-time alarm correlation method based on attack planning graph (APG) is proposed in reference [22]. This method establishes an attack graph model according to attack types and causality. In order to obtain effective network intrusion alarm information and reveal the intention of attackers, the literature [23] proposed a method to construct attack scenarios based on single-value causality graphs, which constructs attack scenes based on causal graph and can correctly reflect the real hacker intrusion process. The above methods have a strong dependence on prior knowledge. Once an intermediate link in the attack step is missing, a complete attack scene cannot be constructed.

Association method based on data mining is a research hotspot in recent years, it does not need expert knowledge and prior knowledge. It can automatically mine data through

statistical methods to find attack scenarios. Both literature [24] and literature [25] extract complex attack scenarios by mining frequent attack sequences, which can effectively mine attack scenarios and discover more valuable attack patterns. Aiming at the problem that causal knowledge is difficult to obtain automatically in alarm correlation analysis, in reference [26], the transition probability matrix between different attack types is automatically mined based on Markov property, thereby constructs causal knowledge of each attack scenario. In literature [27], a plot mining algorithm is used to discover possible combinations of alarms, and then, a supervised decision tree (DT) learning method is used to detect multistep attack scenarios. The literature [28] proposes an alarm correlation framework based on Markov chain, the framework combines statistics and mining techniques to correlate alerts. Although the abovementioned correlation method does not require a large amount of knowledge base and prior knowledge, there are still defects in the statistical analysis process of large amount of calculation and low accuracy.

The alarm correlation method based on attribute similarity is to judge whether there is correlation between alarms by comparing the alarm similarity and the set threshold. The literature [29] uses the similarity of alarms to determine the causal relationship between alarms and reconstructs the attack scene through the evidence in alarms. This method can quickly and incrementally reconstruct known and unknown attack schemes without expert intervention. Literature [30] determines the causal relationship between attack events by calculating the similarity between attacks, thereby constructing attack paths. Mining association rules from the perspective of alarm timing, literature [31] proposes an alarm correlation method based on block similarity that converts the alarm data sequence into a time node sequence and improves the maximum correlation coefficient method to enhance the correlation accuracy. The alarm association method based on attribute similarity has the advantages of simple algorithm and strong real-time performance, but there is no standard for attribute similarity. The final association result is greatly affected by the parameters such as similarity weight coefficient, and the association result cannot show the relationship between attacks very well.

### 3. Preliminaries

In this section, we review the conception of AP clustering algorithm and attribute similarity calculation.

**3.1. AP Clustering Algorithm.** The AP clustering algorithm is a graph-based clustering algorithm, it was first proposed by Frey and Dueck [32] in Science Journal in 2007. The algorithm regards all samples in the dataset as possible cluster centres and transmits information through iterations between data points. In the process of iteration, the iteration information for each point continues to be updated until  $m$  specific cluster centres are produced to achieve the corresponding classification. The basic idea is as follows:

The AP algorithm takes the similarity matrix  $S$  formed by similarity among data  $N$  points as input for clustering analy-

sis. It uses  $s(i, j)$  to represent similarity between node  $i$  and node  $j$  and introduces the concept of reference  $P$  to represent reference degree of data points as clustering centre. The reference degree of point  $i$  is expressed as  $P(i)$  or  $s(i, i)$ , and the larger the value, the more likely point  $i$  is to be the cluster centre. Because the AP algorithm considers that each data point is likely to be the cluster centre, so all  $P$  take the same value, and the final number of clusters is greatly affected by the value of the reference degree. Generally, the median or minimum value of the input similarity value is used as the value of  $P$ . At the same time, by setting the damping factor ( $\lambda$ ), it avoids data shock during the clustering process and achieves a better convergence effect. Its value range is  $[0,1]$ .

The AP algorithm also introduces the two concepts of responsibility and availability and realizes the transfer and update of data points by iteratively updating the responsibility matrix and the availability matrix and then obtains the final cluster centre point. The formula used in AP clustering algorithm is given below.

The update formula of responsibility matrix  $R$  is as follows:

$$r_{t+1}(i, k) = \begin{cases} s(i, k) - \max_{j \neq k} \{a_t(i, j) + r_t(i, j)\}, & i \neq k, \\ s(i, k) - \max_{j \neq k} \{s(i, j)\}, & i = k. \end{cases} \quad (1)$$

The update formula of availability matrix  $A$  is as follows:

$$a_{t+1}(i, k) = \begin{cases} \min \left\{ 0, r_{t+1}(k, k) + \sum_{j \neq i, k} \max\{r_{t+1}(j, k), 0\} \right\}, & i \neq k, \\ \sum_{j \neq k} \max\{r_{t+1}(j, k), 0\}, & i = k. \end{cases} \quad (2)$$

At the same time, in order to avoid the problem of data oscillation in the process of matrix update, AP algorithm attenuates the above two formulas by setting damping coefficient, and the update formula is as follows:

$$R_{t+1}(i, k) = \lambda * r_t(i, k) + (1 - \lambda) * r_{t+1}(i, k). \quad (3)$$

$r_{t+1}(i, k)$  represents the responsibility of point  $i$  and point  $k$  after the  $t + 1$ th update, and  $R_{t+1}(i, k)$  represents the degree of responsibility after attenuation.

$$A_{t+1}(i, k) = \lambda * a_t(i, k) + (1 - \lambda) * a_{t+1}(i, k). \quad (4)$$

$a_{t+1}(i, k)$  represents the availability degree after the  $t + 1$ th times update, and  $A_{t+1}(i, k)$  represents the availability after attenuation.

The flow of AP algorithm is as follows:

*Step 1.* Set the initialized responsibility and availability matrix as 0 matrix and set parameters damping factor and maximum iteration times  $\text{MaxIterNum}$ .

*Step 2.* Input the data to calculate the similarity matrix  $S$  and then calculate the median value of the similarity matrix and assign it to the parameter preference.

*Step 3.* Use formula (1) to update the responsibility matrix.

*Step 4.* Use formula (2) to update the availability matrix.

*Step 5.* Attenuate formula (1) and formula (2) according to the attenuation coefficient.

*Step 6.* Check whether the clustering result meets the termination condition, if it is satisfied, the algorithm ends and the result is output; otherwise, it returns to step 3 for the next iteration.

*Step 7.* When the algorithm is finished, output the final cluster centre and the dataset of the classified categories.

**3.2. Attribute Similarity Calculation.** Within a certain time-threshold, the alarm data belonging to the same attack scenario must have certain relations in IP address, port, and alarm type. Therefore, when clustering, we use the attribute selection method in literature [33] for reference and conduct correlation analysis from the four attributes of attack type, IP, port, and time.

**3.2.1. Similarity of Attack Types.** For the alarm type attribute, if the two alarm data  $\text{alert}_i$  and  $\text{alert}_j$  have the same alarm type, set their similarity to 1; otherwise, it is 0. The calculation formula is as follows:

$$\text{sim}_{\text{type}} = \begin{cases} 0, & \text{alter}_i.\text{type} \neq \text{alter}_j.\text{type}, \\ 1, & \text{alter}_i.\text{type} = \text{alter}_j.\text{type}. \end{cases} \quad (5)$$

**3.2.2. IP Address Similarity.** The IP address in the alarm log is expressed in decimal form. Therefore, it is necessary to convert the IP address into a binary form first and then calculate the similarity by comparing the same consecutive prefix digits [34]. The calculation formula is as follows:

$$\text{sim}_{\text{ip}} = \frac{r}{32}, \quad (6)$$

where  $r$  represents the two alarm data  $\text{alert}_i$  and  $\text{alert}_j$  from high to low, the IP address is the same number of consecutive digits.

**3.2.3. Port Similarity.** The port number is a Boolean attribute. If two alarm ports are identical, the similarity is considered as 1; otherwise, it is 0. The calculation formula is as follows:

$$\text{sim}_{\text{port}} = \begin{cases} 0, & \text{alter}_i.\text{port} \neq \text{alter}_j.\text{port}, \\ 1, & \text{alter}_i.\text{port} = \text{alter}_j.\text{port}. \end{cases} \quad (7)$$

**3.2.4. Time Similarity.** For the calculation of time similarity, we first compare the date attributes and then use the sigmoid function to calculate the time similarity for alarms with the

same date attributes. Otherwise, the similarity is 0. The calculation formula is as follows:

$$\text{sim}_{\text{timestamp}} = \begin{cases} 0, & \text{alter}_i.\text{date} \neq \text{alter}_j.\text{date}, \\ \frac{1}{1 + e^t}, & \text{alter}_i.\text{date} = \text{alter}_j.\text{date}. \end{cases} \quad (8)$$

That  $t = |t_i - t_j|/60$ .

After calculating the similarity of four attributes of attack type, IP, port, and time, the overall similarity between alarm data is obtained by taking the weighted average. The formula for calculating the overall similarity between two alarms is as follows:

$$\text{sim}(\text{alter}_i, \text{alter}_j) = \sum_{l=1}^6 \text{sim}_l * \omega_l, \quad (9)$$

where  $\text{sim}_l$  indicates the similarity of each attribute, the  $\omega_l$  represents the weight corresponding to each attribute, and the subscript of 6 indicates that the formula is weighted by six attributes, which are attack type, timestamp, source IP address, source port number, destination IP address, and destination port number. The weight of each attribute is determined by principal component analysis based on the idea of reference [35].

## 4. Our Scheme

In this section, we propose the hybrid alarm correlation method based on AP clustering algorithm and causality, it mainly includes three phases: (1) alarm data preprocessing, (2) attack scene division based on AP clustering, and (3) constructing attack process graph based on causality. Our method is based on the idea that the alarm data with high similarity after preprocessing are aggregated into the same cluster by using AP clustering algorithm, so as to realize the division of attack scenarios. Then, the alarm data in the same attack scenario are further correlated and analysed by using causal correlation method to restore the attack process. Our method can restore attack process without setting attack knowledge base, and it well shows the logical relationship among alarm information, eliminates redundant data, improves the correlation accuracy, and realizes multistep attack restoration. The overall flow of the algorithm is shown in Figure 1.

**4.1. Alarm Preprocessing.** Different intrusion detection systems generate different formats of alarm data according to the abnormal conditions of the network environment. These data cannot be directly used for correlation analysis, so attribute filtering and normalization processing of alarm logs in different formats are the bases of subsequent work. We use Intrusion Detection Information Exchange Format (IDMEF) [36] to extract eight attributes from the original log and standardize the format of the original alarm data and define the alarm data as a seven-tuple. The meaning of each attribute is shown in Table 1.



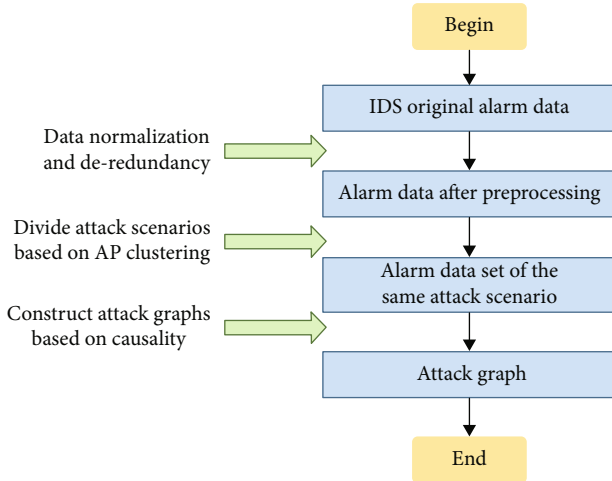


FIGURE 1: Flow chart of alarm correlation method.

TABLE 1: Alarm data attribute.

Attribute	Meaning
Signature	Characteristic string
Type	Alarm category
Date	Alarm date
Timestamp	Alarm timestamp
Src_ip	Source IP
Src_port	Source port
Des_ip	Destination IP
Des_port	Destination port

Due to the large number of repeated and redundant alarms in the alarm data, it is difficult for us to obtain valuable alarm information from the massive alarm data [37]. In order to solve this problem, we deduplicate and merge the original alarm data. We set a time threshold, and under the condition of not exceeding this time threshold, in addition to the signature attribute, we merge the alarm data with high similarity of other attributes to remove duplicates and add alert\_id attribute to the deduplicated data to prepare for the follow-up work.

**4.2. Attack Scene Division Based on AP Clustering.** In the process of alarm correlation analysis, we use AP clustering algorithm to divide attack scenarios. The AP algorithm divides the massive and disordered alarm logs into a collection of attack scenarios with small intraclass spacing and large interclass spacing without prior knowledge, and it does not need to set the clustering number in advance, nor does it need to randomly select the initial clustering centre. It overcomes the defect of the traditional clustering algorithm that is sensitive to the initial conditions. What is more, compared with the K-means clustering algorithm, its fitting degree is much higher than that of the K-means algorithm, and the squared error of the results is also smaller.

The standard AP clustering algorithm uses Euclidean distance as the similarity calculation criterion, but the type of

the alarm log generated by the intrusion detection system is string type, and there is a certain connection between the attributes of the alarm data, and the relative importance of each attribute field is not the same. It is difficult to calculate its similarity by using the distance calculation formula, and it will also destroy the connection between the alarms. Therefore, we improve the similarity matrix calculation method of AP clustering algorithm. According to the attribute similarity calculation method given in Section 3, we calculate the attribute similarity and then use the AP clustering algorithm to aggregate the alarms with higher attribute similarity. In order to make it easier to understand our attack scenario division method, we give an algorithm flow to illustrate the construction of our method, as shown in Algorithm 1.

As described in Algorithm 1, Alert is an alarm dataset, and Scene is an attack scene set based on AP clustering partition. Firstly, the similarity matrix is obtained based on the above attribute similarity calculation method, and initialize the attraction matrix and the attribution matrix. Then, according to the requirements of the AP method, the similarity is taken as a negative value. Finally, the alarm data with high similarity is clustered into the same attack scenario according to the AP method.

**4.3. Constructing Attack Process Graph Based on Causality.** Every attack has its premise and corresponding consequences. That is, the previous attack is the precondition of the next attack, and the next attack is the consequence of the previous attack. For example, in a multistep attack, before launching an attack on the target, the intruder first scans and detects the target, finds the vulnerabilities in the target, and then starts the attack based on the vulnerabilities. Each of these attack steps can be regarded as a prerequisite for the next attack step, and the next attack step can be regarded as the consequence of the previous attack. Therefore, a complete attack sequence can be obtained by connecting the premise and result of alarm according to causality, which is based on causality. The method of dividing attack scenes was introduced, and the attack scenes were divided. Based on the previous work, this part will analyse the alarm data of the same attack scene by causal association method [38] and then construct an attack graph. The flow chart is shown in Figure 2.

In the multistep attack, the attack with correlation occurred in a short period of time and the alarm data with causality existed in the order of time, and the attack premise and the attack result have corresponding relations in IP and port attributes, that is, the destination IP address and destination port number of the attack premise must be the same as the source IP address and source port number of the attack result. The specific implementation process of association is as follows:

*Step 1.* Read the alarm dataset after the cluster processing sequentially and conduct correlation analysis of the data in each attack scene in turn.

*Step 2.* According to the idea of causality, sort the alarm data in each attack scenario in chronological order.



```

Input: Alarm dataset Alert =  $\{a_1, a_2, \dots, a_n\}$ .
Output: Attack scenario set Scene =  $\{\text{scene}_1, \text{scene}_2, \dots, \text{scene}_n\}$ .
1 Calculate the similarity matrix  $\rightarrow$  Similarity =  $[\text{sim}_{11}, \text{sim}_{12}, \dots, \text{sim}_{nn}]$ .
2 Calculate the responsibility matrix  $\rightarrow R = [r_{11}, r_{12}, \dots, r_{nn}]$ .
3 Calculate the availability matrix  $\rightarrow A = [a_{11}, a_{12}, \dots, a_{nn}]$ .
4 Update  $R$  matrix and  $A$  matrix iteratively
5   if Convergence(cluster)
6     output cluster
7   else
8     return 4
9   end if
10 return Scene =  $\{\text{scene}_1, \text{scene}_2, \dots, \text{scene}_n\}$ .

```

ALGORITHM 1: Attack scenario division based on AP clustering.

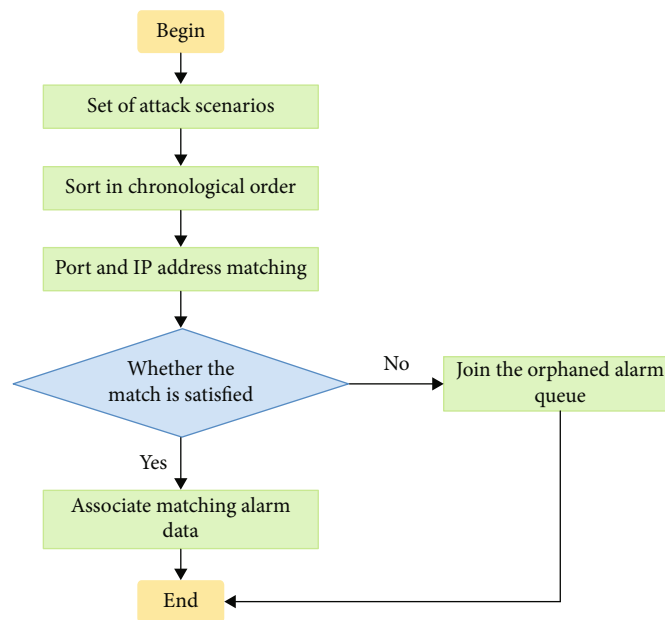


FIGURE 2: Flow chart of alarm association based on causal relationship.

*Step 3.* Match the first piece of data  $\text{alert}_1$  in the set with other data one by one according to the step size of 1. Within a certain time threshold, if the corresponding relationship between IP and port attributes is satisfied, that is, if the target IP address of the first data is the same as the source IP address of an alarm data, and the source port number and destination port number are the same, then, the two pieces of alert data are associated. If no qualified data is found after searching, it will be listed  $\text{alert}_1$  as an isolated alarm.

*Step 4.* Sequentially execute the operations in step 3 on the remaining alarm data until all alarms are analysed.

*Step 5.* After completing the above steps to obtain the associated alarm, use Graph-viz to draw the attack graph.

## 5. Performance Evaluation

*5.1. Experimental Environment.* We use the Python 3.6 programming with PyCharm Community 2017.3 version in

Windows 10. Use the Scikit-learn library to simply and efficiently process alarm data files. After the alarm association, we use the Graph-viz drawing tool to visually display the attack scene in the form of an attack graph.

*5.2. Experimental Dataset.* We use the honeypot dataset to verify the effectiveness of our proposed method in alarm correlation and the ability to construct attack scenarios. The honeypot dataset is obtained by simulating real network system and then using network decoy technology to lure intruders to launch attacks and capture the attack data [39]. Honeypot is essentially a kind of intelligence gathering system to trap attackers. All the actions of accessing honeypot system are the attacks of intruders. Through the correlation analysis of the honeypot data, all the activity information of the intruder in the system can be restored, which is convenient for the security management personnel to analyse the attacker's data and take corresponding measures to improve the protection capability of the real network system. These types of information include operating systems, brute force

network attacks, host vulnerabilities, and port scanning. In one aspect, the types of attacks included are shown in Table 2.

5.3. *Experimental Results and Analysis.* In this section, we divide the verification experiment into two parts: construction of attack graphs and correlation efficiency analysis.

5.3.1. *Build Attack Graphs.* After the attack scenarios are divided by the AP clustering algorithm, the alarm data in each attack scenario is used to find out the correlation between the alarms according to the causal relationship. If the following relationships are satisfied, it indicates that there is a connection between the two alarms. If the following relationship is satisfied, it is an isolated alarm.

- (1) Within a certain period of time, the occurrence time of alert<sub>i</sub> precedes the occurrence time of alert<sub>j</sub>
- (2) alert<sub>i</sub>'s destination IP is the same as alert<sub>j</sub>'s source IP address
- (3) alert<sub>i</sub>'s destination port number is the same as alert<sub>j</sub>'s source port number

After obtaining the associated alarm data based on the idea of causal association, we use the drawing software Graph-viz to construct an attack graph on these alarm data. Below we have selected several representative attack graphs for analysis.

As shown in Figure 3, we restored a distributed attack. The attack figure describes the process of a target host being attacked by multiple hackers. Multiple intruders perform SYN scan or FIN scan on the target host within the same time period, obtain active port information through the returned message, and then capture the host and obtain advanced permissions. Finally, using the host as a springboard, launch different types of distributed attacks on different hosts in the network.

As shown in Figure 4, it depicts an attack source launching the same type of attack on multiple target hosts at the same time. In these target hosts, a pair of pairwise combination is used to launch a centralized attack on the same host, and then a single step attack is implemented.

As shown in Figure 5, we restore a distributed port attack process. The attack source launches distributed attacks on the same port of different target hosts, controls these puppet machines through remote login, and uses the current host as the host to search for the target port to initiate local or remote attacks. Finally, use buffer overflow attacks to destroy the target host.

5.3.2. *Correlation Efficiency Analysis.* The correlation ratio and false alarm rate are reasonable indicators to verify the validity of alarm correlation. The false alarm rate refers to the ratio of false alarms that are not generated by real attacks to the total number of alarms. The correlation ratio refers to the ratio of the number of alarms generated by real attacks and the number of correctly associated alarms to

TABLE 2: Types of honeypot data attacks.

Attack type	Quantity
Portmap-request-mountd	111
Web-cgi	10
Ping zeros	51
SYN FIN scan	47
DNS-version-query	116
DNS-zone-transfer	3989
Large-icmp	286
Ping Microsoft Windows	14
RPC-rpcinfo-query	24
Spp_portscan	838
SourcePortTraffic-53-tcp	26
Ping Nmap 2.36BETA	459
Socks-probe	2627
Telnet-login-incorrect	397
PING-ICMP time exceeded	12
IDS118-MISC-traceroute ICMP	2360
PING-ICMP destination unreachable	709
IDS212-MISC	1487
NAMED Iquery probe	146
RPC-portmap-request-status	67
MISC-Source Port Traffic 53 TCP	60
SMTP-expn-root	786
Portmap-request-mountd	111

the total number of alarms. The calculation formulas are as follows:

$$\text{FAR} = \frac{\text{NIA}}{\text{TNA}} \times 100\%, \quad (10)$$

where FAR represents the false alarm rate, NIA represents the number of false alarms in isolated alarms, that is, the number of false alarms that did not participate in the correlation, and TNA represents the total number of alarms.

$$\text{CR} = \frac{\text{NPA}}{\text{TNA}} \times 100\%, \quad (11)$$

where CR represents the correlation ratio, NPA represents the number of alarms correctly participating in the association, and TNA represents the total number of alarms.

This paper selects two different alarm correlation analysis methods proposed in literature [40] and literature [41] to compare with the method proposed in this paper. Among them, literature [40] and literature [41] use a single alarm correlation method. It can be seen from Table 3 that our multi-type mixed alarm correlation method is the method with the best correlation effect, and the correlation ratio reaches 96.7%, which is higher than the single correlation method. In addition, associating alarm data in attack scenarios based on AP clustering can find out more internal logical connections between alarms and reduce isolated alarms. The false

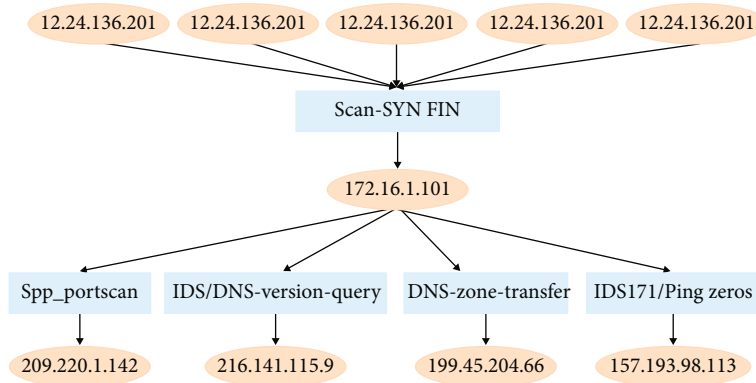


FIGURE 3: Attack figure 1.

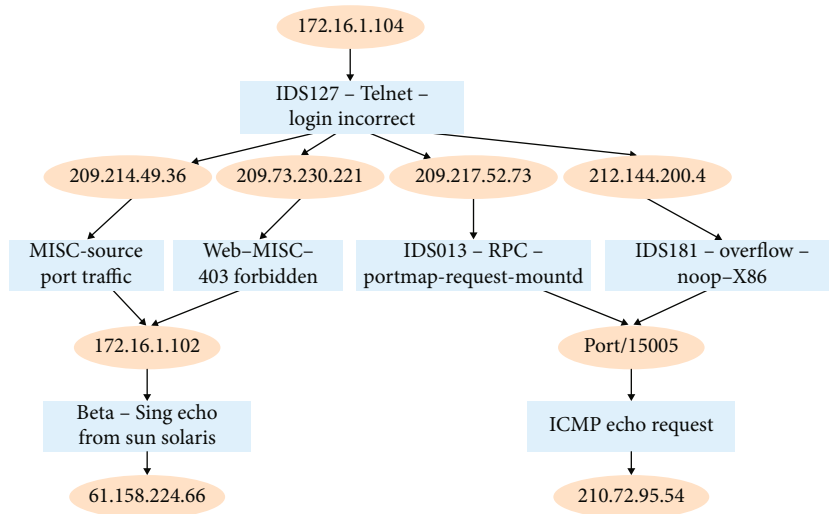


FIGURE 4: Attack figure 2.

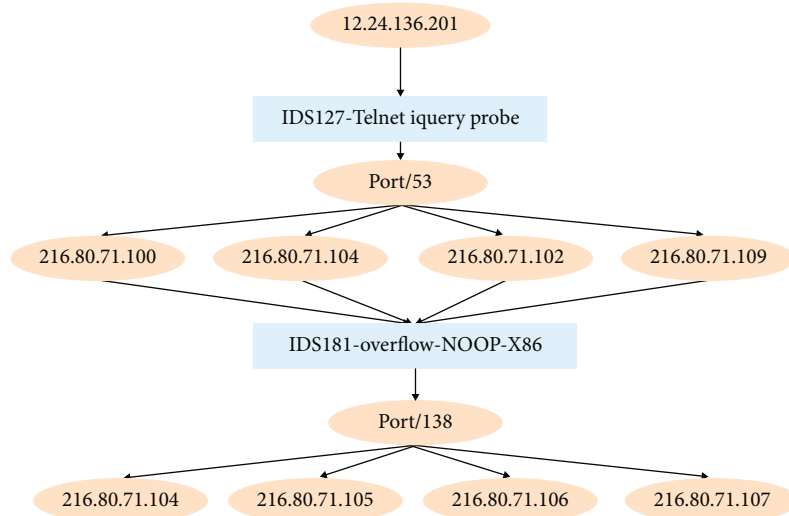


FIGURE 5: Attack figure 3.

TABLE 3: Comparison of correlation ratio and false alarm rate.

Correlation analysis method	FAR	CR
The method presented in this paper	2.1%	96.7%
Method in literature [40]	10.7%	83.6%
Method in literature [41]	4.5%	93.2%

alarm rate is only 2.1%, which is much smaller than other comparison algorithms. It shows that our method can effectively find out the correlation between alarm data and restore the complete attack scenario.

## 6. Conclusions

In this paper, we propose an alarm correlation method based on AP clustering algorithm and causality. Our method fully considers the logical relationship of each alarm information in the relevant attributes which analyses the characteristics of multistep attack alarm information and combines the shortcomings of existing alarm correlation methods to propose an attack scenario division method based on AP clustering. The experiment result showed that our method can achieve a correlation efficiency with 96.7% and can fully restore the attack process and construct a complete attack graph.

## Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

## Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this study.

## Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 61962015) and the Science and Technology Program of Guangxi (No. AB17195045).

## References

- [1] Y. B. Wang, "Opportunities and challenges facing the security development of the Internet of Things," *Information Security and Communication Confidentiality*, vol. 39, no. 6, pp. 7–12, 2017.
- [2] X. Cheng, J. L. Zhang, and B. Chen, "Cyber situation comprehension for IoT systems based on APT alerts and logs correlation," *Sensors*, vol. 19, no. 18, p. 4045, 2019.
- [3] Z. Cai and Z. He, "Trading private range counting over big IoT data," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 144–153, Dallas, TX, USA, 2019.
- [4] CCID Consulting, "2019 China cybersecurity development white paper," *China Computer News*, p. 6, 2019.
- [5] Z. P. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.
- [6] X. Zheng and Z. P. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.
- [7] X. Cheng, J. L. Zhang, Y. F. Tu, and B. Chen, "Cyber situation perception for Internet of Things systems based on zero-day attack activities recognition within advanced persistent threat," *Concurrency and Computation: Practice and Experience*, no. e6001, 2020.
- [8] X. L. Tao, Y. Peng, F. Zhao, P. Zhao, and Y. Wang, "A parallel algorithm for network traffic anomaly detection based on isolation forest," *International Journal of Distributed Sensor Networks*, vol. 14, no. 11, 2018.
- [9] Y. C. Yang, L. F. Wu, G. S. Yin, L. J. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.
- [10] F. Valeur, G. Vigna, C. Kruegel, and R. Kemmerer, "Comprehensive approach to intrusion detection alert correlation," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 3, pp. 146–169, 2004.
- [11] X. Qin and W. Lee, "Statistical causality analysis of INFOSEC alert data," in *International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)*, pp. 73–93, Pittsburgh, USA, 2003.
- [12] J. Zhang, X. P. Li, H. J. Wang, J. Q. Li, and B. Yu, "A real-time alarm correlation method based on attack plan diagram," *Computer Application*, vol. 36, no. 6, pp. 1538–1543, 2016.
- [13] Z. Li, J. Lei, L. Wang, and D. Li, "A data mining approach to generating network attack graph for intrusion prediction," in *2007 4th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, pp. 307–311, Haikou, China, 2007.
- [14] A. Ramaki, M. Amini, and R. Ebrahimi Atani, "RTECA: real time episode correlation algorithm for multi-step attack scenarios detection," *Computers & Security*, vol. 49, pp. 206–219, 2015.
- [15] H. S. Gao and Y. M. Li, "An association analysis method of ASON alarm based on hierarchical attribute similarity clustering," *Science and Technology and Engineering*, vol. 15, no. 6, pp. 210–214+225, 2015.
- [16] D. P. Hostiadi, M. D. Susila, and R. R. Huizen, "A new alert correlation model based on similarity approach," in *2019 1st International Conference on Cybernetics and Intelligent System (ICORIS)*, pp. 133–137, Denpasar, Indonesia, 2019.
- [17] X. Tao, Y. Peng, F. Zhao, S. F. Wang, and Z. Liu, "An improved parallel network traffic anomaly detection method based on bagging and GRU," in *2020 15th International Conference on Wireless Algorithms, Systems, and Applications (WASA)*, pp. 420–431, Qingdao, China, 2020.
- [18] J. Navarro, A. Deruyver, and P. Parrend, "A systematic survey on multi-step attack detection," *Computers & Security*, vol. 76, pp. 214–249, 2018.
- [19] X. Fu and L. Xie, "Research on security alarm association technology," *Computer Science*, vol. 37, no. 5, pp. 9–14+29, 2010.
- [20] L. Cheng, Y. Wang, and X. K. Ma, "GSLAC: A general scalable and low-overhead alert correlation method," in *2016 IEEE Trustcom/BigDataSE/ISPA*, pp. 316–323, Tianjin, China, 2016.
- [21] A. Ahmadian Ramaki and A. Rasoolzadegan, "Causal knowledge analysis for detecting and modeling multi-step attacks,"

- Security and Communication Networks*, vol. 9, no. 18, pp. 6042–6065, 2016.
- [22] S. Haas and M. Fischer, “GAC: graph-based alert correlation for the detection of distributed multi-step attacks,” in *SAC 2018: Symposium on Applied Computing*, pp. 979–988, Pau, France, 2018.
- [23] C. Y. Zhang and X. Wu, “Intrusion scenario dynamic correlation algorithm based on single value causality diagram,” *Advanced Materials Research*, vol. 926-930, pp. 3063–3067, 2014.
- [24] K. Y. Li, Y. Li, J. Y. Liu, R. Zhang, and X. Duan, “Attack pattern mining algorithm based on security log,” in *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 205–205, Beijing, China, 2017.
- [25] F. Faraji Daneshgar and M. Abbaspour, “Extracting fuzzy attack patterns using an online fuzzy adaptive alert correlation framework,” *Security and Communication Networks*, vol. 9, no. 14, pp. 2245–2260, 2016.
- [26] X. W. Feng, D. X. Wang, M. H. Huang, and J. Li, “A method for mining causal knowledge based on Markov properties,” *Computer Research and Development*, vol. 51, no. 11, pp. 2493–2504, 2014.
- [27] M. Soleimani and A. Ghorbani, “Multi-layer episode filtering for the multi-step attack detection,” *Computer Communications*, vol. 35, no. 11, pp. 1368–1379, 2012.
- [28] Y. Zhang, S. Zhao, and J. Zhang, “RTMA: real time mining algorithm for multi-step attack scenarios reconstruction,” in *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pp. 2103–2110, Zhangjiajie, China, 2019.
- [29] M. Barzegar and M. Shajari, “Attack scenario reconstruction using intrusion semantics,” *Expert Systems with Applications*, vol. 108, pp. 119–133, 2018.
- [30] J.-w. Tian, X. Li, Z. Tian, and W.-h. Qi, “Network attack path reconstruction based on similarity computation,” in *2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, pp. 2457–2461, Guilin, China, 2017.
- [31] B. Yang, J. J. Li, C. Qi, H. G. Li, and Y. He, “Novel correlation analysis of alarms based on block matching similarities,” *Industrial & Engineering Chemistry Research*, vol. 58, no. 22, pp. 9465–9472, 2019.
- [32] B. Frey and D. Dueck, “Clustering by passing messages between data points,” *Science*, vol. 315, no. 5814, pp. 972–976, 2007.
- [33] N. H. Yang, H. Q. Yu, Z. L. Qian, and H. Sun, “Modeling and quantitatively predicting software security based on stochastic Petri nets,” *Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp. 102–112, 2012.
- [34] S. H. Ahmadijad, S. Jalili, and M. Abadi, “A hybrid model for correlating alerts of known and unknown attack scenarios and updating attack graphs,” *Computer Networks*, vol. 55, no. 9, pp. 2221–2240, 2011.
- [35] L. Q. Zhou and W. X. Wei, “Intrusion detection method based on principal component analysis and Simhash,” *Computer and Digital Engineering*, vol. 43, no. 7, pp. 1291–1294, 2015.
- [36] A. Baláž, N. Ádám, E. Pietriková, and B. Madoš, “ModSecurity IDMEF module,” in *2018 IEEE 16th World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, pp. 43–48, Kosice and Herlany, Slovakia, 2018.
- [37] X. L. Tao, Y. M. Gong, and F. Zhao, “An OSSEC alarm data aggregation method based on classification,” *Computer Engineering and Design*, vol. 41, no. 4, pp. 908–914, 2020.
- [38] P. Ning, C. Yun, and D. Reeves, “Analyzing intensive intrusion alerts via correlation,” in *International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)*, pp. 74–94, Zurich, Switzerland, 2002.
- [39] D. Q. Yang, W. M. Liu, and Z. Yu, “Research on active defence application based on honeypot,” *Journal of Network and Information Security*, vol. 4, no. 1, p. 57, 2018.
- [40] S. Wang, G. M. Tang, J. H. Wang, Y. F. Sun, and G. Kou, “Construction method of attack scenario based on causal knowledge network,” *Computer Research and Development*, vol. 55, no. 12, pp. 2620–2636, 2018.
- [41] C. T. Kawakani, S. B. Junior, and R. S. Miani, “Intrusion alert correlation to support security management,” in *Brazilian Symposium on Information Systems (SBSI)*, pp. 313–320, Florianópolis, Brazil, 2016.





## Research Article

# D-(DP)<sup>2</sup>SGD: Decentralized Parallel SGD with Differential Privacy in Dynamic Networks

Yuan Yuan,<sup>1</sup> Zongrui Zou,<sup>1</sup> Dong Li,<sup>2</sup> Li Yan,<sup>2</sup> and Dongxiao Yu <sup>1</sup>

<sup>1</sup>School of Computer Science and Technology, Shandong University, Qingdao 266237, China

<sup>2</sup>Information & Telecommunications Company, State Grid Shandong Electric Power Company, Jinan 250000, China

Correspondence should be addressed to Dongxiao Yu; [dxyu@sdu.edu.cn](mailto:dxyu@sdu.edu.cn)

Received 12 December 2020; Revised 5 February 2021; Accepted 2 March 2021; Published 24 March 2021

Academic Editor: Zhuojun Duan

Copyright © 2021 Yuan Yuan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Decentralized machine learning has been playing an essential role in improving training efficiency. It has been applied in many real-world scenarios, such as edge computing and IoT. However, in fact, networks are dynamic, and there is a risk of information leaking during the communication process. To address this problem, we propose a decentralized parallel stochastic gradient descent algorithm (D-(DP)<sup>2</sup>SGD) with differential privacy in dynamic networks. With rigorous analysis, we show that D-(DP)<sup>2</sup>SGD converges with a rate of  $O(1/\sqrt{Kn})$  while satisfying  $\epsilon$ -DP, which achieves almost the same convergence rate as previous works without privacy concern. To the best of our knowledge, our algorithm is the first known decentralized parallel SGD algorithm that can implement in dynamic networks and take privacy-preserving into consideration.

## 1. Introduction

Decentralized machine learning, as a modeling mechanism that allocates training tasks and computes resources to achieve a balance between training speed and accuracy, has demonstrated strong potential in various areas, especially for training large models on large datasets [1–3], such as ImageNet [4]. Typically, assume that there are  $n$  workers where each worker has its local data, decentralized machine learning problem is aimed at solving an empirical risk minimization problem as follows:

$$\min_{x \in \mathbb{R}^d} f(x) = \frac{1}{n} \sum_{i=1}^n f_i(x), \quad (1)$$

where  $f_i(x)$  is the local loss function at node  $i$ . The objective  $f(x)$  can be rephrased as a linear combination of the local loss function  $f_i(x)$ . This formulation can be expressed as many popular decentralized learning models including deep learning [5], linear regression [6], and logistic regression [7].

In recent years, decentralized machine learning has attracted much attention to derive convergence solutions

while reducing communication costs [8, 9]. Previous works mainly study decentralized collaborative learning in a static network assumption. For example, decentralized parallel stochastic gradient descent (D-PSGD) is one of the fundamental methods in solving large-scale machine learning tasks in static networks [1]. In D-PSGD, all nodes compute the stochastic gradient using their local dataset and exchange the results with their neighbors iteratively. However, in fact, dynamicity has been an important feature for networks, especially for large-scale networks, such as IoT [10] and V2V networks [11, 12], as nodes in the network can move around and join or leave the network at any time. On the other hand, in large-scale networks, it is hard or even impossible to ensure every node is reliable [13, 14]. Consequently, during the collaborative learning process, it is unavoidable to face the risk of information leaking. Hence, when designing decentralized machine learning algorithms, it has been to consider the impact of the dynamicity of network topology and the demand for privacy preservation. However, to the best of our knowledge, there is no existing work taking both factors simultaneously into consideration. In this work, we focus on this missing piece in decentralized learning.

Specifically, based on differential privacy, we present a new dynamic decentralized stochastic gradient descent algorithm (D-(DP)<sup>2</sup>SGD), which offers a strong protection for local datasets of decentralized nodes. With rigorous analysis, we show that our proposed D-(DP)<sup>2</sup>SGD algorithm satisfies  $\epsilon$ -DP and achieves the convergence rate of  $O(1/\sqrt{Kn})$  when  $K$  is large enough. Empirically, we conduct experiments on CIFAR-10 datasets to accomplish image classification tasks. We conduct extensive experiments to evaluate the performance of our proposed algorithms.

The remainder of this paper is organized as follows. We present our survey on related work in Section 2. We then introduce our model, problem, and some useful preliminary knowledge in Section 3. Our algorithm, main results, and analysis are presented in Section 4, Section 5, and Section 6, respectively. Experimental results are illustrated in Section 7. The whole paper is concluded in Section 8.

## 2. Related Work

In this section, we introduce some closed related work.

*2.1. Decentralized Parallel Stochastic Gradient Algorithms.* Most existing work on decentralized parallel stochastic gradient focus on static networks in both synchronous and asynchronous settings [1, 15–18]. Under the synchronous setting, Lian et al. [1] illustrated the advantage of decentralized algorithms over centralized ones and showed that the proposed D-PSGD converges with a rate of  $O(1/\sqrt{Kn})$  when  $K$  is large enough, where  $K$  is the number of iterations and  $n$  is the total number nodes in the network. Qureshi et al. [17] proposed an algorithm called S-ADDOPT, and it converges with a rate of  $O(1/K)$ .

Feyzmahdavian et al. [19] and Agarwal et al. [20] considered decentralized SGD in the asynchronous setting. They allowed workers to use stale weights to compute gradients in S-PSGD. Asynchronous algorithms avoid idling any worker to reduce the communication overhead, and it is very robust because it can still work well when part of the computing workers are down. For asynchronous algorithms, Lian et al. [16] proposed the asynchronous decentralized parallel SGD algorithm for convex optimization and showed AD-PSGD converges at  $O(1/\sqrt{K})$ . Then, Lian et al. [21] proposed the asynchronous decentralized parallel stochastic gradient descent algorithm for nonconvex optimization and showed the ergodic convergence rate is  $O(1/\sqrt{K})$ . They proved that the linear speedup is achievable when the number of workers is bounded by  $\sqrt{K}$ .

*2.2. Differentially Privacy Decentralized Learning.* Most existing work on differentially private decentralized learning focuses on the static network [22–25]. Our work combines decentralized learning and dynamic network in a DP setting. In contrast, Lu et al. [24] proposed an asynchronous federated learning scheme with differential private for resource sharing in vehicular networks. Hsin-Pai et al. [26] proposed a new learning algorithm LEASGD (Leader-Follower Elastic Averaging Stochastic Gradient Descent), which is driven by a novel Leader-Follower topology and a differential privacy

model. And they provide a theoretical analysis of the convergence rate and the trade-off between the performance and privacy in the private setting. Based on the research in [16], Xu et al. [2] designed an algorithm on asynchronous decentralized parallel stochastic gradient descent algorithm with differential privacy (A(DP)<sup>2</sup>SGD). They showed that A(DP)<sup>2</sup>SGD converges at  $O(1/\sqrt{K})$ . For all of these reviewed papers, the study of decentralized parallel SGD for differential privacy in dynamic networks is still an open problem.

## 3. System Model and Problem Description

We consider a network consisting of  $n$  computational nodes (could be a machine or a GPU). At each iterate  $k$ , the network topology is denoted by a network  $\mathcal{G}_k = (\mathcal{V}, \mathcal{E}_k)$ , where  $\mathcal{V}$  is the set of  $n$  computational nodes,  $\mathcal{V} = \{1, 2, \dots, n\}$ , and  $\mathcal{E}_k \subset \mathcal{V} \times \mathcal{V}$  is the set of communication edges at iterate  $k$ . If there exists an edge from node  $i$  to node  $j$  at iterate  $k$ , then  $(i, j) \in \mathcal{E}_k$ . In a connected network, two nodes are neighbors if the node can be connected directly by an edge, i.e., the nodes can communicate with each other. The set of neighbors of node  $i$  at iterate  $k$  is denoted by  $\mathcal{N}_k(i) = \{j \mid (i, j) \in \mathcal{E}_k\}$ , and define  $\mathcal{C}_k(i) = \mathcal{N}_k(i) \cup \{i\}$ . We assume that the nodes keep unchanged, but the connection between nodes can be changed after every iteration. The network  $\mathcal{G}_k$  is assumed to be strongly connected, i.e., for all nodes  $i, j \in \mathcal{V}$ , there exists a path from  $i$  to  $j$  at each iterate  $k \geq 0$ . Some frequently used notations are summarized in Table 1.

In a decentralized network, the data is stored at nodes, and each node is associated with a local loss function

$$f_i(x) = \mathbb{E}_{\xi \sim \mathcal{D}_i} F_i(x; \xi), \quad (2)$$

where  $\mathcal{D}_i$  is a distribution associated with the local data at node  $i$  and  $\xi$  is a data sampled via  $\mathcal{D}_i$ .

In this work, we consider the following optimization problem:

$$\min_{x \in \mathbb{R}^d} f(x) = \mathbb{E}_{i \sim \mathcal{I}} f_i(x) = \mathbb{E}_{i \sim \mathcal{I}} \mathbb{E}_{\xi \sim \mathcal{D}_i} F_i(x; \xi), \quad (3)$$

where  $\mathcal{I}$  is a uniform distribution of nodes.

Similarity, we gives an  $\delta$ -approximation solution if

$$K^{-1} \left( \sum_{k=0}^{K-1} \mathbb{E} \|\nabla f(\bar{x}_k)\|^2 \right) \leq \delta, \quad (4)$$

where  $\bar{x}_k$  is the average local variable with all nodes at iterate  $k$  and  $K$  is the maximum iterations.

We next review the definition of differential privacy, which is originally proposed by Dwork [27].

*Definition 1* (see [27] (Differential Privacy)). Given a  $\epsilon \geq 0$ , a randomized mechanism  $\mathcal{M}$  with domain  $\mathfrak{D}$  preserves  $\epsilon$ -differential privacy if for all  $\mathcal{S} \subseteq \text{Range}(\mathcal{M})$  and for any adjacent datasets (Given two datasets  $D = \{x_1, x_2, \dots, x_n\}$  and  $D' = \{x'_1, x'_2, \dots, x'_n\}$ ,  $D$  and  $D'$  are adjacent if there exist  $i \in [n]$  such that  $x_i \neq x'_i$  and for  $j \neq i$ ,  $x_j = x'_j$ , i.e.,  $\|D - D'\|_1 = 1$ .)  $D, D'$

TABLE 1: Frequently used notations.

Notation	Description
$\ \cdot\ $	The vector $\ell_2$ norm or the matrix spectral norm depending on the argument
$\ \cdot\ _F$	The matrix Frobenius norm
$f(\cdot)$	The optimization function
$\nabla f(\cdot)$	The gradient of a function $f$
$\mathbf{1}_n$	The column vector in $\mathbb{R}^n$ with 1 for all elements
$f^*$	The optimal solution of problem
$\lambda_i(\cdot)$	The $i$ th largest eigenvalue of a matrix
$\mathcal{G}_k$	The network topology at iterate $k$
$\mathcal{V}$	The set of nodes
$\mathcal{E}_k$	The set of edges at iterate $k$
$K$	The total number of iterations
$\mathcal{N}_k(i)$	The set of neighbors of node $i$ at iterate $k$
$x_{k,i}$	The local variable in node $i$ at iterate $k$
$\bar{x}_k$	The average local variable with all nodes at iterate $k$
$\xi_{k,i}$	The sampled training data in node $i$ at iterate $k$
$\tilde{x}_{k,i}$	The perturbed variable in node $i$ at iterate $k$
$\eta_{k,i}$	The Laplace noise drawn from $Lap(\zeta)$
$X_k$	The concatenation of all local variables
$\tilde{X}_k$	The concatenation of all perturbed variables
$\eta_k$	The concatenation of all Laplace noises
$\xi_k$	The concatenation of all random samples
$\partial F(X_k, \xi_k)$	The concatenation of all stochastic gradients

$\in \mathfrak{D}$  such that:

$$\mathbb{P}[\mathcal{M}(D) \in \mathcal{S}] \leq \exp(\varepsilon) \mathbb{P}[\mathcal{M}(D') \in \mathcal{S}], \quad (5)$$

where  $\text{Range}(\mathcal{M})$  is the output range of mechanism  $\mathcal{M}$ .

Informally, differential privacy means that the distributions over the outputs of the randomized algorithm should be nearly identical for two adjacent input datasets. The constant  $\varepsilon$  measures the privacy level of the randomized mechanism  $\mathcal{M}$ , i.e., a large  $\varepsilon$  implies a lower privacy level. Therefore, an appropriate constant  $\varepsilon$  should be chosen to balance the accuracy and the privacy level of the mechanism  $\mathcal{M}$ .

Then, we introduce the definition of sensitivity, which plays a key role in the design of differential privacy mechanisms.

*Definition 2* (see [28] (Sensitivity)). The sensitivity of a function  $f : \mathfrak{D} \rightarrow \mathbb{R}^d$  is defined as follows:

$$\Delta = \sup_{D, D' : \|D - D'\|_1 = 1} \|f(D) - f(D')\|_1. \quad (6)$$

The sensitivity of a mechanism  $\mathcal{M}$  captures the magnitude by which a single individual's data can change the mechanism  $\mathcal{M}$  in the worse case. Moreover, we will introduce the Laplace mechanism.

*Definition 3* (see [27] (The Laplace mechanism)). Given any function  $f : \mathfrak{D} \rightarrow \mathbb{R}^d$ , the Laplace mechanism is defined as:

$$\mathcal{M}(D, f(\cdot), \varepsilon) = f(D) + \eta_{k,i}, \quad (7)$$

where  $\eta_{k,i}$  are i.i.d. random variables drawn from  $Lap(\zeta)$ . The variable of Laplace distribution is  $2\zeta^2$ , where  $\zeta = \Delta/\varepsilon$  according to the property of differential privacy.

Throughout the paper, we adopt the following commonly used assumptions:

- (1) Lipschitzian gradient: all functions  $f_i(\cdot)$ 's are  $L$ -Lipschitzian gradients.
- (2) Unbiased estimation:

$$\begin{aligned}\mathbb{E}_{\xi \sim \mathcal{D}_i} \nabla F_i(x; \xi) &= \nabla f_i(x), \\ \mathbb{E}_{i \sim \mathcal{I}} \mathbb{E}_{\xi \sim \mathcal{D}_i} \nabla F_i(x; \xi) &= \nabla f(x).\end{aligned}\quad (8)$$

- (3) Bounded variance: assume the variance of stochastic gradient

$$\mathbb{E}_{i \sim \mathcal{I}} \mathbb{E}_{\xi \sim \mathcal{D}_i} \|\nabla F_i(x; \xi) - \nabla f(x)\|^2, \quad (9)$$

is bounded for any  $x$  with  $i$  sampled from the distribution  $\mathcal{I}$  and  $\xi$  from the distribution  $\mathcal{D}_i$ . It implies there exist constants  $\sigma$  and  $\zeta$  such that

$$\begin{aligned}\mathbb{E}_{\xi \sim \mathcal{D}_i} \|\nabla F_i(x; \xi) - \nabla f_i(x)\|^2 &\leq \sigma^2, \quad \forall i, \forall x, \\ \mathbb{E}_{i \sim \mathcal{I}} \|\nabla f_i(x) - \nabla f(x)\|^2 &\leq \zeta^2, \quad \forall x.\end{aligned}\quad (10)$$

- (4) Bounded subgradient: assume that the subgradient  $\nabla F_i(x; \xi)$  of  $F_i(x; \xi)$  is  $G_i$ -bounded for all  $i \in \mathcal{I}$  and  $x \in \mathbb{R}^d$ , i.e.,  $\|\nabla F_i(x; \xi)\| \leq G_i$  and  $G = \max_{i \in \mathcal{I}} G_i$ .

#### 4. Algorithm

The D-(DP)<sup>2</sup>SGD algorithm can be described as follows: each node maintains its own local variable  $x_{k,i}$  and run the following steps.

- (i) Sample data: each node samples a training data  $\xi_{k,i}$ .
- (ii) Compute gradient: each node computes the stochastic gradient  $\nabla F_i(x_{k,i}, \xi_{k,i})$  using the current local variable  $x_{k,i}$  and the data  $\xi_{k,i}$ , where  $i$  is the node index and  $k$  is the iterate number.
- (iii) Add noise: random generate the Laplace noise  $\eta_{k,i} \sim \text{Lap}(\varsigma)$  and add noise to the variable  $x_{k,i}$ , to get the perturbed variable  $\tilde{x}_{k,i} = x_{k,i} + \eta_{k,i}$ .
- (iv) Communication: send the perturbed variable  $\tilde{x}_{k,i}$  and the degree  $d_{k,i}$  to its neighbors; receive  $\tilde{x}_{k,j}$  and  $d_{k,j}$  from neighbors, where  $j \in \mathcal{N}_k(i)$ .
- (v) Determine the matrix  $W_k$ : determine the matrix  $W_k$  according to the local network topology, i.e.,

$$w_{k,ij} = \begin{cases} \frac{1}{\max\{d_{k,i}, d_{k,j}\}} & \text{if } i \neq j, \text{ and } j \in \mathcal{N}_k(i), \\ 1 - \sum_{m \in \mathcal{N}_k(i)} w_{k,im} & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases} \quad (11)$$

where  $w_{k,ij}$  describes how much node  $j$  can affect node  $i$  at iterate  $k$ .

- (vi) Weighted average: compute the weighted average by obtaining perturbed variable from neighbors and the matrix  $W_k$ :  $x_{k+(1/2),i} = \sum_{j \in \mathcal{N}_k(i)} w_{k,ij} \tilde{x}_{k,j}$ .
- (vii) Gradient update: each node updates its local variable using the weighted average and the local stochastic gradient  $x_{k+1,i} = x_{k+(1/2),i} - \gamma \nabla F_i(x_{k,i}, \xi_{k,i})$ .

From a global view, we define the concatenation of all local variables, perturbed variables, Laplace noises, random samples, and stochastic gradients by matrix  $X_k \in \mathbb{R}^{d \times n}$ ,  $\tilde{X}_k \in \mathbb{R}^{d \times n}$ , and  $\eta_k \in \mathbb{R}^{d \times n}$ , vector  $\xi_k \in \mathbb{R}^n$ , and  $\partial F(X_k, \xi_k)$ , respectively:

$$\begin{aligned}X_k &= [x_{k,1}, \dots, x_{k,n}] \in \mathbb{R}^{d \times n}, \eta_k = [\eta_{k,1}, \dots, \eta_{k,n}] \in \mathbb{R}^{d \times n}, \\ \tilde{X}_k &= [\tilde{x}_{k,1}, \dots, \tilde{x}_{k,n}] \in \mathbb{R}^{d \times n}, \xi_k = [\xi_{k,1}, \dots, \xi_{k,n}] \in \mathbb{R}^n, \\ \partial F(X_k, \xi_k) &= [\nabla F_1(x_{k,1}; \xi_{k,1}) \nabla F_2(x_{k,2}; \xi_{k,2}) \dots \nabla F_n(x_{k,n}; \xi_{k,n})] \in \mathbb{R}^{d \times n}.\end{aligned}\quad (12)$$

Then, the  $k$ th iterate of Algorithm 1 can be described as the following update

$$X_{k+1} = \tilde{X}_k W_k - \gamma \partial F(X_k, \xi_k), \quad (13)$$

i.e.,  $X_{k+1} = (X_k + \eta_k) W_k - \gamma \partial F(X_k, \xi_k)$ .

#### 5. Main Results

In this section, we present the main results, which guarantees the privacy and the convergence rate of our proposed algorithm.

**Theorem 4.** *Let assumptions hold. If  $\eta_{k,i}$ 's are i.i.d. random variables drawn according to the Laplace distribution with parameter  $\varsigma$ , such that  $\varsigma = \Delta/\varepsilon$  for all  $k \in \{0, \dots, K-1\}$  and  $\varepsilon > 0$ . Then, our proposed algorithm guarantees  $\varepsilon$ -differential private.*

**Theorem 5.** *Let  $B_1 = ((1/2) - ((18\gamma^2(n-1)L^2)/((1-\sqrt{\rho})^2 B_2)))$ ,  $B_2 = (1 - ((36\gamma^2(n-1)L^2)/((1-\sqrt{\rho})^2)))$ . Under the assumptions, we can get the convergence rate of Algorithm 1 as follows:*

$$\begin{aligned}& \frac{((1-\gamma L)/2) \sum_{k=0}^{K-1} \mathbb{E} \|\partial f(X_k) 1_n / n\|^2 + B_1 \sum_{k=0}^{K-1} \mathbb{E} \|\nabla f((X_k 1_n) / n)\|^2}{K} \\ & \leq \frac{f(0) - f^*}{\gamma K} + \frac{4(1+2L)G^2 d\gamma}{\varepsilon^2} + \frac{\gamma L}{n} \sigma^2 + \frac{24(n-1)L^2 G^2 \gamma^2}{\varepsilon^2 (1-\sqrt{\rho})^2 B_2} \\ & \quad + \frac{2\gamma^2 L^2 (n-1)\sigma^2}{(1-\rho)B_2} + \frac{18\gamma^2 (n-1)L^2 \zeta^2}{(1-\sqrt{\rho})^2 B_2},\end{aligned}\quad (14)$$

where  $((X_k 1_n) / n) = (1/n) \sum_{i=1}^n x_{k,i} = \bar{x}_k$ .

This theorem characterizes the convergence of the average of all local optimization variables  $x_{k,i}$ . To take a closer

**Initialization**

Initial point  $x_{0,i} = x_0 = 0$ , step length  $\gamma$ , noise variance  $\varsigma$  and number of iterations  $K$

**end**

**for**  $k = 0, 1, \dots, K - 1$  *in parallel for nodes*  $i \in \mathcal{V}$  **do**

Sample a training data  $\xi_{k,i}$ ;

Compute the stochastic gradient  $\nabla F_i(x_{k,i}, \xi_{k,i})$  using the current local variable  $x_{k,i}$  and the data  $\xi_{k,i}$ ;

Randomly generate the Laplace noise  $\eta_{k,i} \sim \text{Lap}(\varsigma)$  and add noise to the variable  $x_{k,i}$ , to get the perturbed variable  $\tilde{x}_{k,i}$ :  $\tilde{x}_{k,i} = x_{k,i} + \eta_{k,i}$ ;

Send the perturbed variable  $\tilde{x}_{k,i}$  and its degree  $d_{k,i}$  to its neighbors;

Receive  $\tilde{x}_{k,j}$  and  $d_{k,j}$  from its neighbors,  $j \in \mathcal{N}_k(i)$ ;

Determine  $W_k$  according to Equation (11);

Compute the neighborhood weighted average by obtaining perturbed variables from neighbors:  $x_{k+(1/2),i} = \sum_{j \in \mathcal{N}_k(i)} w_{k,ij} \tilde{x}_{k,j}$ ;

Update its local variable  $x_{k+1,i} = x_{k+(1/2),i} - \gamma \nabla F_i(x_{k,i}, \xi_{k,i})$ ;

**end**

**Output:**  $(1/n) \sum_{i=1}^n x_{K,i}$ .

ALGORITHM 1: D-(DP)<sup>2</sup>SGD: Dynamic Decentralized Parallel Stochastic Gradient Descent.

look at this result, we choose an appropriate step length in Theorem 5 to obtain the following result:

**Corollary 6.** *Under the same assumptions as in Theorem 5, let  $(G/\varepsilon) \leq \sqrt{((f(0) - f^* + L)\sigma)/(4(1 + 2L)dn)}$ , by setting  $\gamma = 1/(2L + \sigma\sqrt{K/n})$ , we have the following convergence rate:*

$$\frac{\sum_{k=0}^{K-1} \mathbb{E} \|\nabla f((X_k L_n)/n)\|^2}{K} \leq \frac{8L(f(0) - f^*)}{K} + \frac{12(f(0) - f^* + L)\sigma}{\sqrt{Kn}}, \quad (15)$$

if the total number of iterates  $K$  is sufficiently large,

$$K \geq \max \left\{ \frac{16n^3(n-1)^2 L^4}{\sigma^6(f(0) - f^* + L)^2} \left( \frac{12G^2}{\varepsilon^2(1-\sqrt{\rho})^2} + \frac{\sigma^2}{(1-\rho)} + \frac{\varrho^2}{(1-\sqrt{\rho})^2} \right), \frac{144n(n-1)L^2}{\sigma^2(1-\sqrt{\rho})^2} \right\}. \quad (16)$$

## 6. Result Analysis

In this section, we will give the analysis for privacy preservation and convergence rate of D-(DP)<sup>2</sup>SGD.

For convenience, we define

$$\partial f(X_k) = [\nabla f_1(x_{k,1}) \nabla f_2(x_{k,2}) \cdots \nabla f_n(x_{k,n})] \in \mathbb{R}^{d \times n}, \quad (17)$$

and

$$\Phi(k : s) = \begin{cases} W_k W_{k-1} \cdots W_s, & k \geq s, \\ I, & s = k + 1. \end{cases} \quad (18)$$

### 6.1. Privacy Analysis

*Proof* (Proof of Theorem 4). From the definition of sensitivity, we obtain

$$\|x_{k,i} - x'_{k,i}\|_1 \leq \Delta. \quad (19)$$

Note that  $x_{k,i}$  and  $x'_{k,i}$  are in space  $\mathbb{R}^d$ . According to the

definition of 1-norm, we have

$$\sum_{l=1}^d |x_{k,i}^l - x'_{k,i}^l| = \|x_{k,i} - x'_{k,i}\|_1 \leq \Delta, \quad (20)$$

where  $x_{k,i}^l$  and  $x'_{k,i}^l$  are the  $l$ th component of  $x_{k,i}$  and  $x'_{k,i}$ , respectively.

Consider an output vectors  $y_{k,i}$ . Then, we follow from the property of Laplace distribution, we get

$$\mathbb{P}[\mathcal{M}(D_k) \in \mathcal{S}] = \prod_{l=1}^d \frac{1}{2\varsigma} \exp\left(-\frac{|y_{k,i}^l - x_{k,i}^l|}{\varsigma}\right), \quad (21)$$

$$\mathbb{P}[\mathcal{M}(D'_k) \in \mathcal{S}] = \prod_{l=1}^d \frac{1}{2\varsigma} \exp\left(-\frac{|y_{k,i}^l - x'_{k,i}^l|}{\varsigma}\right).$$

Then,

$$\begin{aligned} \frac{\mathbb{P}[\mathcal{M}(D_k) \in \mathcal{S}]}{\mathbb{P}[\mathcal{M}(D'_k) \in \mathcal{S}]} &= \prod_{l=1}^d \exp\left(-\frac{|y_{k,i}^l - x_{k,i}^l| - |y_{k,i}^l - x'_{k,i}^l|}{\varsigma}\right) \\ &\leq \prod_{l=1}^d \exp\left(\frac{|x_{k,i}^l - x'_{k,i}^l|}{\varsigma}\right) = \exp\left(\frac{\|x_{k,i} - x'_{k,i}\|_1}{\varsigma}\right) \\ &\leq \exp\left(\frac{\Delta}{\varsigma}\right), \end{aligned} \quad (22)$$

where the first inequality comes from the triangle inequality, and the last inequality follows from (19).

Therefore, we know  $\varepsilon = \Delta/\varsigma$ , we can obtain

$$\frac{\mathbb{P}[\mathcal{M}(D) \in \mathcal{S}]}{\mathbb{P}[\mathcal{M}(D') \in \mathcal{S}]} \leq \exp(\varepsilon). \quad (23)$$



**6.2. Convergence Rate Analysis.** In order to obtain the result of convergence rate, we first give some lemmas.

**Lemma 7.**  $W_k$  is a symmetric doubly stochastic matrix.

*Proof.* From the definition of Equation (11), we can obtain that

$$w_{k,ij} \in [0, 1], \quad \forall i, j, \quad (24)$$

- (1)  $w_{k,ij} \in [0, 1]$ , for all  $i, j$ ;
- (2)  $w_{k,ij} = w_{k,ji}$ , for all  $i, j$ ;
- (3)  $\sum_j w_{k,ij} = 1$ , for all  $i$ .

Therefore,  $W_k$  is a symmetric doubly stochastic matrix.

**Lemma 8.** Define  $\Phi(K-1, 0) = I$ , where  $I$  is the identity matrix. Assume that there exists a  $\rho \in [0, 1)$  such that

$$\max \{ |\lambda_2(\mathbb{E}[W_s^T W_s])|, |\lambda_n(\mathbb{E}[W_s^T W_s])| \} \leq \rho, \quad \forall s. \quad (25)$$

Then

$$\mathbb{E} \left\| \frac{I_n}{n} - \Phi(K-1, 0)e_i \right\|^2 \leq \frac{n-1}{n} \rho^K, \quad \forall K \geq 0. \quad (26)$$

*Proof.* Let  $y_s = (1_n/n) - \Phi(s-1, 0)e_i$ . We prove this lemma by induction. For  $s=0$ ,  $\|y_0\|^2 = \|(1_n/n) - e_i\|^2 = ((n-1)^2/n^2) + \sum_{i=1}^{n-1} (1/n^2) = ((n^2 - 2n + 1 + n - 1)/n^2) = (n-1)/n$ .

We assume that  $s=K$  hold, i.e.,  $\mathbb{E}\|y_K\|^2 \leq ((n-1)/n)\rho^K$ . Then, for  $s=K+1$ , note that  $y_{K+1} = W_K y_K$ , then we have

$$\begin{aligned} \mathbb{E}\|y_{K+1}\|^2 &= \mathbb{E}\|W_K y_K\|^2 = \mathbb{E}\langle W_K y_K, W_K y_K \rangle = \mathbb{E}\langle y_K, W_K^T W_K y_K \rangle \\ &= \mathbb{E}\langle y_K, \mathbb{E}(W_K^T W_K) y_K \rangle. \end{aligned} \quad (27)$$

According to Lemma 7,  $\mathbb{E}(W_K^T W_K)$  is symmetric and doubly stochastic. Then,  $1_n$  is an eigenvector of  $\mathbb{E}(W_K^T W_K)$ , and 1 is the eigenvalue. According to the spectral theorem of Hermitian matrices, we can construct a basis of  $\mathbb{R}^n$  composed by the eigenvectors of  $\mathbb{E}(W_K^T W_K)$  starting from  $1_n$ . From Equation (25), the magnitude of all other eigenvectors' associated eigenvalues should be smaller or equal to  $\rho$ . Note that  $y_K$  is orthogonal to  $1_n$ , then we can find

$$\mathbb{E}\|y_{K+1}\|^2 \leq \rho \mathbb{E}\|y_K\|^2. \quad (28)$$

By induction, we complete the proof.

In Lemma 9, we give the bound of the sensitivity of our proposed algorithm.

**Lemma 9.** Under assumption 4, the sensitivity of the algorithm can be bounded as

$$\Delta \leq 2G\sqrt{d}\gamma, \quad (29)$$

where  $G = \max_{i \in \mathcal{T}} G_i$  and  $d$  is the dimensionality of vectors.

*Proof.* Assume that  $D_k$  and  $D'_k$  are any two adjacent datasets at iterate  $k$ . Assume that  $x_{k,i}$  and  $x'_{k,i}$  be the executions for  $\mathcal{M}(D_k)$  and  $\mathcal{M}(D'_k)$ , respectively. Then, from our proposed algorithm, we have

$$\begin{aligned} \left\| \mathcal{M}(D_k) - \mathcal{M}(D'_k) \right\|_1 &= \|x_{k+1,i} - x'_{k+1,i}\|_1 \\ &= \gamma \left\| \nabla F_i(x_{k,i}; \xi_{k,i}) - \nabla F_i(x_{k,i}; \xi'_{k,i}) \right\|_1 \\ &\leq \sqrt{d}\gamma \left\| \nabla F_i(x_{k,i}; \xi_{k,i}) - \nabla F_i(x_{k,i}; \xi'_{k,i}) \right\| \\ &\leq \sqrt{d}\gamma \left( \left\| \nabla F_i(x_{k,i}; \xi_{k,i}) \right\| + \left\| \nabla F_i(x_{k,i}; \xi'_{k,i}) \right\| \right), \end{aligned} \quad (30)$$

where the first inequality comes from the norm inequality and the last inequality is from the triangle inequality. From assumption 4, we have

$$\nabla F_i(x_{k,i}; \xi_{k,i}) \leq G_i \leq G. \quad (31)$$

Since we can choose the pair of adjacent datasets  $D_k, D'_k$  arbitrarily, and we can obtain

$$\Delta \leq 2G\sqrt{d}\gamma. \quad (32)$$

The lemma is obtained.

From Lemma 9, we know that the learning rate  $\gamma$ , the dimensionality of vectors  $d$ , the maximal bound of subgradient  $G$ , and the privacy level  $\epsilon$  have an effect on the magnitude of the added random noise. Based on Lemma 9, we next provide the bound of the noise.

**Lemma 10.** We give the following inequalities:

$$\mathbb{E} \left\| \frac{\eta_s 1_n}{n} \right\|^2 \leq \frac{8G^2 d \gamma^2}{\epsilon^2} \text{ and } \mathbb{E}\|\eta_s\|^2 \leq \frac{8nG^2 d \gamma^2}{\epsilon^2}. \quad (33)$$

*Proof.* According to the property of the Laplace mechanism  $\mathbb{E}\|\eta_{s,i}\|^2 \leq 2\zeta^2$  and  $\zeta = \Delta/\epsilon$ , we obtain a bound on  $\eta_s$  in the following:

$$\begin{aligned} \mathbb{E} \left\| \frac{\eta_s 1_n}{n} \right\|^2 &\leq \mathbb{E} \left\| \frac{\sum_{i=1}^n \eta_{s,i}}{n} \right\|^2 \leq \frac{1}{n} \sum_{i=1}^n \mathbb{E}\|\eta_{s,i}\|^2 \leq \frac{1}{n} \cdot n \cdot 2\zeta^2 = 2\zeta^2 \stackrel{(19)}{\leq} 2 \left( \frac{2G\sqrt{d}\gamma}{\epsilon} \right)^2 \\ &= \frac{8G^2 d \gamma^2}{\epsilon^2}. \end{aligned} \quad (34)$$

And we can get a bound on  $\eta_s$ .

$$\begin{aligned} \mathbb{E}\|\eta_s\|^2 &\leq \mathbb{E}\|\eta_s\|_F^2 \leq \sum_{i=1}^n \mathbb{E}\|\eta_{s,i}\|^2 \leq n \cdot 2\zeta^2 \leq 2n \left( \frac{2G\sqrt{d}\gamma}{\varepsilon} \right)^2 \\ &= \frac{8nG^2d\gamma^2}{\varepsilon^2}. \end{aligned} \quad (35)$$

**Lemma 11** (see [1]). *Under assumption 1, the following inequality holds:*

$$\mathbb{E}\|\partial f(X_s)\|^2 \leq \sum_{h=1}^n 3\mathbb{E}L^2 \left\| \frac{\sum_{i'=1}^n x_{s,i'}}{n} - x_{s,h} \right\|^2 + 3n\zeta^2 + 3\mathbb{E} \left\| \nabla f \left( \frac{X_s \mathbf{1}_n}{n} \right) \mathbf{1}_n^T \right\|^2, \quad \forall s \in K. \quad (36)$$

The proof of this lemma can be found in the full version of [1]. And we define  $\text{Dis}_{k,i}$  as the squared distance of the local optimization variable on node  $i$  from the averaged local optimization variable on all nodes at iterate  $k$ , i.e.,  $\text{Dis}_{k,i} = \mathbb{E} \left\| \left( \frac{\sum_{i'=1}^n x_{k,i'}}{n} \right) - x_{k,i} \right\|^2$ . In the following, we will present the bound of  $\text{Dis}_{k,i}$ .

**Lemma 12.** *Under the definition of  $\text{Dis}_{k,i}$ , we can get:*

$$\begin{aligned} \text{Dis}_{k,i} &\leq \frac{48(n-1)G^2d\gamma^2}{\varepsilon^2(1-\sqrt{\rho})^2} + 2\gamma^2 \left( \frac{2(n-1)\sigma^2}{1-\rho} + \frac{18(n-1)\zeta^2}{(1-\sqrt{\rho})^2} + \frac{6(n-1)}{n} \right. \\ &\quad \cdot \sum_{s=0}^{k-1} \mathbb{E} \left\| \nabla f \left( \frac{X_s \mathbf{1}_n}{n} \right) \mathbf{1}_n^T \right\|^2 \left( \frac{2\sqrt{\rho}^{k-s-1}}{1-\sqrt{\rho}} + \rho^{k-s-1} \right) \\ &\quad \left. + \frac{6(n-1)}{n} \sum_{s=0}^{k-1} \sum_{h=1}^n \mathbb{E}L^2 \text{Dis}_{s,h} \left( \frac{2\sqrt{\rho}^{k-s-1}}{1-\sqrt{\rho}} + \rho^{k-s-1} \right) \right). \end{aligned} \quad (37)$$

*Proof.* According to the update method of  $X_k$ , we split  $\text{Dis}_{k,i}$  into two terms:

$$\begin{aligned} \text{Dis}_{k,i} &= \mathbb{E} \left\| \frac{\sum_{i'=1}^n x_{k,i'}}{n} - x_{k,i} \right\|^2 = \mathbb{E} \left\| \frac{X_k \mathbf{1}_n}{n} - X_k e_i \right\|^2 \\ &= \mathbb{E} \left\| \frac{(X_{k-1} + \eta_{k-1}) W_{k-1} \mathbf{1}_n - \gamma \partial F(X_{k-1}; \xi_{k-1}) \mathbf{1}_n}{n} \right. \\ &\quad \left. - ((X_{k-1} + \eta_{k-1}) W_{k-1} e_i - \gamma \partial F(X_{k-1}; \xi_{k-1}) e_i) \right\|^2 \\ &= \mathbb{E} \left\| \frac{X_{k-1} \mathbf{1}_n + \eta_{k-1} \mathbf{1}_n - \gamma \partial F(X_{k-1}; \xi_{k-1}) \mathbf{1}_n}{n} \right. \\ &\quad \left. - (X_{k-1} W_{k-1} e_i + \eta_{k-1} W_{k-1} e_i - \gamma \partial F(X_{k-1}; \xi_{k-1}) e_i) \right\|^2 \\ &= \mathbb{E} \left\| \frac{X_0 \mathbf{1}_n}{n} + \frac{\sum_{s=0}^{k-1} \eta_s \mathbf{1}_n}{n} - \frac{\sum_{s=0}^{k-1} \gamma \partial F(X_s; \xi_s) \mathbf{1}_n}{n} \right. \\ &\quad \left. - \left( X_0 \Phi(k-1, 0) e_i + \sum_{s=0}^{k-1} \eta_s \Phi(k-1, s) e_i - \gamma \partial F(X_{k-1}; \xi_{k-1}) e_i \right) \right. \\ &\quad \left. - \sum_{s=0}^{k-2} \gamma \partial F(X_s; \xi_s) \Phi(k-1, s+1) e_i \right\|^2 \end{aligned}$$

$$\begin{aligned} &\stackrel{(18)}{=} \mathbb{E} \left\| X_0 \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, 0) e_i \right) + \sum_{s=0}^{k-1} \eta_s \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s) e_i \right) \right. \\ &\quad \left. - \gamma \sum_{s=0}^{k-1} \partial F(X_s; \xi_s) \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s+1) e_i \right) \right\|^2 \\ &= \mathbb{E} \left\| \sum_{s=0}^{k-1} \eta_s \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s) e_i \right) - \gamma \sum_{s=0}^{k-1} \partial F(X_s; \xi_s) \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s+1) e_i \right) \right\|^2 \\ &= 2\mathbb{E} \underbrace{\left\| \sum_{s=0}^{k-1} \eta_s \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s) e_i \right) \right\|^2}_{A_1} \\ &\quad + 2\gamma^2 \mathbb{E} \underbrace{\left\| \sum_{s=0}^{k-1} \partial F(X_s; \xi_s) \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s+1) e_i \right) \right\|^2}_{A_2}, \end{aligned} \quad (38)$$

where the seventh equation comes from  $x_{0,i} = x_0 = 0$  for  $\forall i$ . Firstly, we split  $A_1$  into two terms,

$$\begin{aligned} A_1 &= \mathbb{E} \left\| \sum_{s=0}^{k-1} \eta_s \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s) e_i \right) \right\|^2 \\ &= \underbrace{\sum_{s=0}^{k-1} \mathbb{E} \left\| \eta_s \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s) e_i \right) \right\|^2}_{=A_3} \\ &\quad + \underbrace{\sum_{s \neq s'}^{k-1} \mathbb{E} \left\langle \eta_s \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s) e_i \right), \eta_{s'} \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s') e_i \right) \right\rangle}_{=A_4}. \end{aligned} \quad (39)$$

To bound  $A_1$ , we first bound  $A_3$  and  $A_4$ :

$$\begin{aligned} A_3 &= \sum_{s=0}^{k-1} \mathbb{E} \left\| \eta_s \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s) e_i \right) \right\|^2 \\ &\leq \sum_{s=0}^{k-1} \mathbb{E} \|\eta_s\|^2 \left\| \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s) e_i \right) \right\|^2 \stackrel{(33)}{\leq} \sum_{s=0}^{k-1} \frac{8nG^2d\gamma^2}{\varepsilon^2} \cdot \frac{n-1}{n} \rho^{k-s} \\ &\leq \frac{8(n-1)G^2d\gamma^2}{\varepsilon^2} \frac{1}{1-\rho}. \end{aligned} \quad (40)$$

Moreover,  $A_4$  can be bound as follows:

$$\begin{aligned} A_4 &= \sum_{s \neq s'}^{k-1} \mathbb{E} \left\langle \eta_s \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s) e_i \right), \eta_{s'} \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s') e_i \right) \right\rangle \\ &\leq \sum_{s \neq s'}^{k-1} \mathbb{E} \left\| \eta_s \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s) e_i \right) \right\| \left\| \eta_{s'} \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s') e_i \right) \right\| \\ &\leq \sum_{s \neq s'}^{k-1} \mathbb{E} \|\eta_s\| \left\| \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s) e_i \right) \right\| \left\| \eta_{s'} \right\| \left\| \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s') e_i \right) \right\| \\ &\leq \sum_{s \neq s'}^{k-1} \mathbb{E} \frac{\|\eta_s\|^2}{2} \left\| \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s) e_i \right) \right\|^2 \\ &\quad + \sum_{s \neq s'}^{k-1} \mathbb{E} \frac{\|\eta_{s'}\|^2}{2} \left\| \left( \frac{\mathbf{1}_n}{n} - \Phi(k-1, s') e_i \right) \right\|^2 \\ &\stackrel{(26)}{\leq} \sum_{s \neq s'}^{k-1} \mathbb{E} \left( \frac{\|\eta_s\|^2}{2} + \frac{\|\eta_{s'}\|^2}{2} \right) \frac{n-1}{n} \rho^{k-\frac{s+s'}{2}} \end{aligned}$$

$$\begin{aligned}
&= \frac{n-1}{n} \sum_{s \neq s'} \rho^{k-1} \mathbb{E} \|\eta_s\|^2 \rho^{k-((s+s')/2)} \\
&\stackrel{(33)}{\leq} 2 \frac{n-1}{n} \cdot \frac{8nG^2 d\gamma^2}{\varepsilon^2} \sum_{s=0}^{k-1} \sum_s \rho^{k-s+1} k-1 \rho^{k-((s+s')/2)} \\
&\leq 2 \frac{n-1}{n} \cdot \frac{8nG^2 d\gamma^2}{\varepsilon^2} \sum_{s=0}^{k-1} \frac{\rho^{(k-s+1)/2} (1-\rho^{(k+1)/2})}{1-\sqrt{\rho}} \\
&\leq \frac{16(n-1)G^2 d\gamma^2}{\varepsilon^2} \frac{(1-\rho^{(k-1)/2})(\rho-\rho^{(k+1)/2})}{(1-\sqrt{\rho})^2} \\
&\leq \frac{16(n-1)G^2 d\gamma^2}{\varepsilon^2} \frac{1}{(1-\sqrt{\rho})^2}.
\end{aligned} \tag{41}$$

Then, plugging  $A_3$  and  $A_4$  into  $A_1$ ,

$$\begin{aligned}
A_1 &= \frac{8(n-1)G^2 d\gamma^2}{\varepsilon^2} \frac{1}{1-\rho} + \frac{16(n-1)G^2 d\gamma^2}{\varepsilon^2} \frac{1}{(1-\sqrt{\rho})^2} \\
&= \frac{8(n-1)G^2 d\gamma^2}{\varepsilon^2} \left( \frac{1}{1-\rho} + \frac{2}{(1-\sqrt{\rho})^2} \right) \leq \frac{24(n-1)G^2 d\gamma^2}{\varepsilon^2 (1-\sqrt{\rho})^2}.
\end{aligned} \tag{42}$$

where the last inequality comes from the fact that  $(1/(1-\rho)) \leq (1/((1-\sqrt{\rho})^2))$ .

Moreover, we split  $A_2$  into two terms:

$$\begin{aligned}
A_2 &= \mathbb{E} \left\| \sum_{s=0}^{k-1} \partial F(X_s; \xi_s) \left( \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right) \right\|^2 \\
&\leq 2 \mathbb{E} \left\| \sum_{s=0}^{k-1} (\partial F(X_s; \xi_s) - \partial f(X_s)) \left( \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right) \right\|^2 \\
&\quad \underbrace{\hspace{10em}}_{=A_5} \\
&\quad + 2 \mathbb{E} \left\| \sum_{s=0}^{k-1} \partial f(X_s) \left( \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right) \right\|^2. \\
&\quad \underbrace{\hspace{10em}}_{=A_6}
\end{aligned} \tag{43}$$

We give an upper bound  $A_5$  as follows:

$$\begin{aligned}
A_5 &= \mathbb{E} \left\| \sum_{s=0}^{k-1} (\partial F(X_s; \xi_s) - \partial f(X_s)) \left( \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right) \right\|^2 \\
&= \sum_{s=0}^{k-1} \mathbb{E} \left\| (\partial F(X_s; \xi_s) - \partial f(X_s)) \left( \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right) \right\|^2 \\
&\leq \sum_{s=0}^{k-1} \mathbb{E} \|\partial F(X_s; \xi_s) - \partial f(X_s)\|^2 \left\| \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right\|^2 \\
&\leq \sum_{s=0}^{k-1} \mathbb{E} \|\partial F(X_s; \xi_s) - \partial f(X_s)\|_F^2 \left\| \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right\|^2 \\
&\leq n\sigma^2 \sum_{s=0}^{k-1} \frac{n-1}{n} \rho^{k-s-1} = \frac{(n-1)\sigma^2}{1-\rho},
\end{aligned} \tag{44}$$

where the last second inequality comes from Lemma 8 and assumption 3.

For  $A_6$ , we will give the following upper bound:

$$\begin{aligned}
A_6 &= \mathbb{E} \left\| \sum_{s=0}^{k-1} \partial f(X_s) \left( \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right) \right\|^2 \\
&= \sum_{s=0}^{k-1} \mathbb{E} \left\| \partial f(X_s) \left( \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right) \right\|^2 \\
&\quad \underbrace{\hspace{10em}}_{=A_7} \\
&\quad + \sum_{s \neq s'} \mathbb{E} \left\langle \partial f(X_s) \left( \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right), \partial f(X_{s'}) \left( \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right) \right\rangle. \\
&\quad \underbrace{\hspace{10em}}_{=A_8}
\end{aligned} \tag{45}$$

To bound  $A_6$ , we first bound  $A_7$  and  $A_8$ , for  $A_7$ :

$$\begin{aligned}
A_7 &= \sum_{s=0}^{k-1} \mathbb{E} \left\| \partial f(X_s) \left( \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right) \right\|^2 \\
&\leq \sum_{s=0}^{k-1} \mathbb{E} \|\partial f(X_s)\|^2 \left\| \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right\|^2 \\
&\leq 3 \sum_{s=0}^{k-1} \sum_{h=1}^n \mathbb{E} L^2 \text{Dis}_{s,h} \left\| \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right\|^2 \\
&\quad + 3n\zeta^2 \sum_{s=0}^{k-1} \frac{n-1}{n} \rho^{k-s-1} + 3 \sum_{s=0}^{k-1} \mathbb{E} \left\| \nabla f \left( \frac{X_s 1_n}{n} \right) 1_n^T \right\|^2 \\
&\quad \cdot \left\| \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right\|^2 \\
&\leq \frac{3(n-1)}{n} \sum_{s=0}^{k-1} \left( \sum_{h=1}^n \mathbb{E} L^2 \text{Dis}_{s,h} + \mathbb{E} \left\| \nabla f \left( \frac{X_s 1_n}{n} \right) 1_n^T \right\|^2 \right) \rho^{k-s-1} \\
&\quad + \frac{3(n-1)\zeta^2}{1-\rho},
\end{aligned} \tag{46}$$

where the last inequality comes from Lemmas 8 and 11.

Then, we bound  $A_8$  as follows:

$$\begin{aligned}
A_8 &= \sum_{s \neq s'} \rho^{k-1} \mathbb{E} \left\langle \partial f(X_s) \left( \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right), \partial f(X_{s'}) \left( \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right) \right\rangle \\
&\leq \sum_{s \neq s'} \rho^{k-1} \mathbb{E} \left\| \partial f(X_s) \left( \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right) \right\| \left\| \partial f(X_{s'}) \left( \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right) \right\| \\
&\leq \sum_{s \neq s'} \rho^{k-1} \mathbb{E} \|\partial f(X_s)\| \left\| \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right\| \left\| \partial f(X_{s'}) \right\| \left\| \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right\| \\
&\leq \sum_{s \neq s'} \rho^{k-1} \mathbb{E} \frac{\|\partial f(X_s)\|^2}{2} \left\| \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right\| \\
&\quad + \sum_{s \neq s'} \rho^{k-1} \mathbb{E} \frac{\|\partial f(X_{s'})\|^2}{2} \left\| \frac{1_n}{n} - \Phi(k-1, s+1)e_i \right\| \\
&\stackrel{(26)}{\leq} \sum_{s \neq s'} \rho^{k-1} \mathbb{E} \left( \frac{\|\partial f(X_s)\|^2}{2} + \frac{\|\partial f(X_{s'})\|^2}{2} \right) \frac{n-1}{n} \rho^{k-((s+s')/2)-1} \\
&= \frac{n-1}{n} \sum_{s \neq s'} \rho^{k-1} \mathbb{E} (\|\partial f(X_s)\|^2) \rho^{k-((s+s')/2)-1} \\
&\stackrel{(36)}{\leq} \frac{3(n-1)}{n} \sum_{s \neq s'} \left( \sum_{h=1}^n \mathbb{E} L^2 \text{Dis}_{s,h} + \mathbb{E} \left\| \nabla f \left( \frac{X_s 1_n}{n} \right) 1_n^T \right\|^2 \right) \rho^{k-((s+s')/2)-1} \\
&\quad \underbrace{\hspace{10em}}_{=A_9} \\
&\quad + \sum_{s \neq s'} \rho^{k-1} 3(n-1)\zeta^2 \rho^{k-((s+s')/2)-1}, \\
&\quad \underbrace{\hspace{10em}}_{=A_{10}}
\end{aligned} \tag{47}$$

where  $A_{10}$  can be bounded by  $\zeta$  and  $\rho$ :

$$\begin{aligned} A_{10} &= 6(n-1)\zeta^2 \sum_{s>s'}^{k-1} \rho^{k-((s+s')/2)-1} = 6(n-1)\zeta^2 \sum_{s=0}^{k-1} \sum_{s'}^{l=s+1} k-1 \rho^{k-((s+s')/2)-1} \\ &= 6(n-1)\zeta^2 \frac{(\rho^{k/2}-1)(\rho^{k/2}-\sqrt{\rho})}{(\sqrt{\rho}-1)^2(\sqrt{\rho}+1)} \leq 6(n-1)\zeta^2 \frac{1}{(1-\sqrt{\rho})^2}, \end{aligned} \quad (48)$$

and we give a bound of  $A_9$ :

$$\begin{aligned} A_9 &= \frac{3(n-1)}{n} \sum_{s \neq s'}^{k-1} \left( \sum_{h=1}^n \mathbb{E} L^2 \text{Dis}_{s,h} + \mathbb{E} \left\| \nabla f \left( \frac{X_s \mathbf{1}_n}{n} \right) \mathbf{1}_n^T \right\|^2 \right) \rho^{k-((s+s')/2)-1} \\ &= \frac{6(n-1)}{n} \sum_{s=0}^{k-1} \left( \sum_{h=1}^n \mathbb{E} L^2 \text{Dis}_{s,h} + \mathbb{E} \left\| \nabla f \left( \frac{X_s \mathbf{1}_n}{n} \right) \mathbf{1}_n^T \right\|^2 \right) \sum_{s'}^{l=s+1} k-1 \sqrt{\rho}^{2k-(s+s')-2} \\ &\leq \frac{6(n-1)}{n} \sum_{s=0}^{k-1} \left( \sum_{h=1}^n \mathbb{E} L^2 \text{Dis}_{s,h} + \mathbb{E} \left\| \nabla f \left( \frac{X_s \mathbf{1}_n}{n} \right) \mathbf{1}_n^T \right\|^2 \right) \frac{\sqrt{\rho}^{k-s-1}}{1-\sqrt{\rho}}. \end{aligned} \quad (49)$$

Then, we plug  $A_9$ ,  $A_{10}$  into  $A_8$ , plug  $A_8$ ,  $A_7$  into  $A_6$ . We can yield the upper bound for  $A_6$ .

$$\begin{aligned} A_6 &\leq \frac{6(n-1)}{n} \sum_{s=0}^{k-1} \left( \sum_{h=1}^n \mathbb{E} L^2 \text{Dis}_{s,h} + \mathbb{E} \left\| \nabla f \left( \frac{X_s \mathbf{1}_n}{n} \right) \mathbf{1}_n^T \right\|^2 \right) \frac{\sqrt{\rho}^{k-s-1}}{1-\sqrt{\rho}} + \frac{6(n-1)\zeta^2}{(1-\sqrt{\rho})^2} \\ &\quad + \frac{3(n-1)}{n} \sum_{s=0}^{k-1} \left( \sum_{h=1}^n \mathbb{E} L^2 \text{Dis}_{s,h} + \mathbb{E} \left\| \nabla f \left( \frac{X_s \mathbf{1}_n}{n} \right) \mathbf{1}_n^T \right\|^2 \right) \rho^{k-s-1} + \frac{3(n-1)\zeta^2}{1-\rho} \\ &\leq \frac{3(n-1)}{n} \sum_{s=0}^{k-1} \mathbb{E} \left\| \nabla f \left( \frac{X_s \mathbf{1}_n}{n} \right) \mathbf{1}_n^T \right\|^2 \left( \frac{2\sqrt{\rho}^{k-s-1}}{1-\sqrt{\rho}} + \rho^{k-s-1} \right) \\ &\quad + \frac{3(n-1)}{n} \sum_{s=0}^{k-1} \sum_{h=1}^n \mathbb{E} L^2 \text{Dis}_{s,h} \left( \frac{2\sqrt{\rho}^{k-s-1}}{1-\sqrt{\rho}} + \rho^{k-s-1} \right) + \frac{9(n-1)\zeta^2}{(1-\sqrt{\rho})^2}. \end{aligned} \quad (50)$$

Then, we plug  $A_5$  and  $A_6$  into  $A_2$  yielding the upper bound of  $A_2$ .

$$\begin{aligned} A_2 &\leq \frac{2(n-1)\sigma^2}{1-\rho} + \frac{6(n-1)}{n} \sum_{s=0}^{k-1} \mathbb{E} \left\| \nabla f \left( \frac{X_s \mathbf{1}_n}{n} \right) \mathbf{1}_n^T \right\|^2 \left( \frac{2\sqrt{\rho}^{k-s-1}}{1-\sqrt{\rho}} + \rho^{k-s-1} \right) \\ &\quad + \frac{6(n-1)}{n} \sum_{s=0}^{k-1} \sum_{h=1}^n \mathbb{E} L^2 \text{Dis}_{s,h} \left( \frac{2\sqrt{\rho}^{k-s-1}}{1-\sqrt{\rho}} + \rho^{k-s-1} \right) + \frac{18(n-1)\zeta^2}{(1-\sqrt{\rho})^2}. \end{aligned} \quad (51)$$

Finally, we can describe  $\text{Dis}_{k,i}$  as follows:

$$\begin{aligned} \text{Dis}_{k,i} &= 2A_1 + 2\gamma^2 A_2 \leq \frac{48(n-1)G^2 d\gamma^2}{\varepsilon^2(1-\sqrt{\rho})^2} + 2\gamma^2 \left( \frac{2(n-1)\sigma^2}{1-\rho} \right. \\ &\quad + \frac{18(n-1)\zeta^2}{(1-\sqrt{\rho})^2} + \frac{6(n-1)}{n} \sum_{s=0}^{k-1} \mathbb{E} \left\| \nabla f \left( \frac{X_s \mathbf{1}_n}{n} \right) \mathbf{1}_n^T \right\|^2 \\ &\quad \cdot \left( \frac{2\sqrt{\rho}^{k-s-1}}{1-\sqrt{\rho}} + \rho^{k-s-1} \right) + \frac{6(n-1)}{n} \sum_{s=0}^{k-1} \sum_{h=1}^n \mathbb{E} L^2 \text{Dis}_{s,h} \\ &\quad \cdot \left. \left( \frac{2\sqrt{\rho}^{k-s-1}}{1-\sqrt{\rho}} + \rho^{k-s-1} \right) \right). \end{aligned} \quad (52)$$

The lemma is obtained.

Based on these lemmas above, we prove Theorem 5 subsequently.

*Proof* (Proof of Theorem 5). We start from  $f((X_{k+1} \mathbf{1}_n)/n)$ :

$$\begin{aligned} \mathbb{E} f \left( \frac{X_{k+1} \mathbf{1}_n}{n} \right) &= \mathbb{E} f \left( \frac{(X_k + \eta_k) W_k \mathbf{1}_n}{n} - \gamma \frac{\partial F(X_k; \xi_k) \mathbf{1}_n}{n} \right) \\ &= \mathbb{E} f \left( \frac{X_k W_k \mathbf{1}_n}{n} + \frac{\eta_k W_k \mathbf{1}_n}{n} - \gamma \frac{\partial F(X_k; \xi_k) \mathbf{1}_n}{n} \right) \\ &\stackrel{\text{Lemma 7}}{=} \mathbb{E} f \left( \frac{X_k \mathbf{1}_n}{n} + \frac{\eta_k \mathbf{1}_n}{n} - \gamma \frac{\partial F(X_k; \xi_k) \mathbf{1}_n}{n} \right) \\ &\leq \mathbb{E} f \left( \frac{X_k \mathbf{1}_n}{n} \right) + \mathbb{E} \left\langle \nabla f \left( \frac{X_k \mathbf{1}_n}{n} \right), \frac{\eta_k \mathbf{1}_n}{n} - \gamma \frac{\partial f(X_k) \mathbf{1}_n}{n} \right\rangle \\ &\quad + \frac{L}{2} \mathbb{E} \left\| \frac{\eta_k \mathbf{1}_n}{n} - \gamma \frac{\partial F(X_k; \xi_k) \mathbf{1}_n}{n} \right\|^2 \\ &\leq \mathbb{E} f \left( \frac{X_k \mathbf{1}_n}{n} \right) + \mathbb{E} \left\langle \nabla f \left( \frac{X_k \mathbf{1}_n}{n} \right), \frac{\eta_k \mathbf{1}_n}{n} \right\rangle \\ &\quad - \mathbb{E} \left\langle \nabla f \left( \frac{X_k \mathbf{1}_n}{n} \right), \gamma \frac{\partial f(X_k) \mathbf{1}_n}{n} \right\rangle + L \mathbb{E} \left\| \frac{\sum_{i=1}^n \eta_{k,i}}{n} \right\|^2 \\ &\quad + \gamma^2 L \mathbb{E} \left\| \frac{\sum_{i=1}^n \nabla F_i(x_{k,i}; \xi_{k,i})}{n} \right\|^2, \end{aligned} \quad (53)$$

where the last step comes from  $\|a-b\|^2 \leq 2\|a\|^2 + 2\|b\|^2$ .

Then, we split the second term according to  $2\langle a, b \rangle \leq \|a\|^2 + \|b\|^2$ ,

$$\begin{aligned} \mathbb{E} \left\langle \nabla f \left( \frac{X_k \mathbf{1}_n}{n} \right), \frac{\eta_k \mathbf{1}_n}{n} \right\rangle &\leq \frac{1}{2} \mathbb{E} \left\| \nabla f \left( \frac{X_k \mathbf{1}_n}{n} \right) \right\|^2 + \frac{1}{2} \mathbb{E} \left\| \frac{\eta_k \mathbf{1}_n}{n} \right\|^2 \\ &= \frac{1}{2} \mathbb{E} \left\| \nabla f \left( \frac{X_k \mathbf{1}_n}{n} \right) \right\|^2 + \frac{1}{2} \mathbb{E} \left\| \frac{\sum_{i=1}^n \eta_{k,i}}{n} \right\|^2. \end{aligned} \quad (54)$$

We split the last term of (53) into two terms because of  $\mathbb{E}_{\xi_{k,i}} \nabla F_i(x_{k,i}; \xi_{k,i}) = \nabla f_i(x_{k,i})$ ,

$$\begin{aligned} \mathbb{E} \left\| \frac{\sum_{i=1}^n \nabla F_i(x_{k,i}; \xi_{k,i})}{n} \right\|^2 &= \mathbb{E} \left\| \frac{\sum_{i=1}^n \nabla F_i(x_{k,i}; \xi_{k,i}) - \sum_{i=1}^n \nabla f_i(x_{k,i})}{n} \right\|^2 \\ &\quad + \mathbb{E} \left\| \frac{\sum_{i=1}^n \nabla f_i(x_{k,i})}{n} \right\|^2. \end{aligned} \quad (55)$$

According to (54) and (55), (53) can be expressed as:

$$\begin{aligned} \mathbb{E} f \left( \frac{X_{k+1} \mathbf{1}_n}{n} \right) &\leq \mathbb{E} f \left( \frac{X_k \mathbf{1}_n}{n} \right) - \gamma \mathbb{E} \left\langle \nabla f \left( \frac{X_k \mathbf{1}_n}{n} \right), \frac{\partial f(X_k) \mathbf{1}_n}{n} \right\rangle \\ &\quad + \frac{1}{2} \mathbb{E} \left\| \nabla f \left( \frac{X_k \mathbf{1}_n}{n} \right) \right\|^2 + \frac{1+2L}{2} \mathbb{E} \left\| \frac{\sum_{i=1}^n \eta_{k,i}}{n} \right\|^2 \\ &\quad + \gamma^2 L \mathbb{E} \left\| \frac{\sum_{i=1}^n \nabla F_i(x_{k,i}; \xi_{k,i}) - \sum_{i=1}^n \nabla f_i(x_{k,i})}{n} \right\|^2 \\ &\quad + \gamma^2 L \mathbb{E} \left\| \frac{\sum_{i=1}^n \nabla f_i(x_{k,i})}{n} \right\|^2. \end{aligned} \quad (56)$$

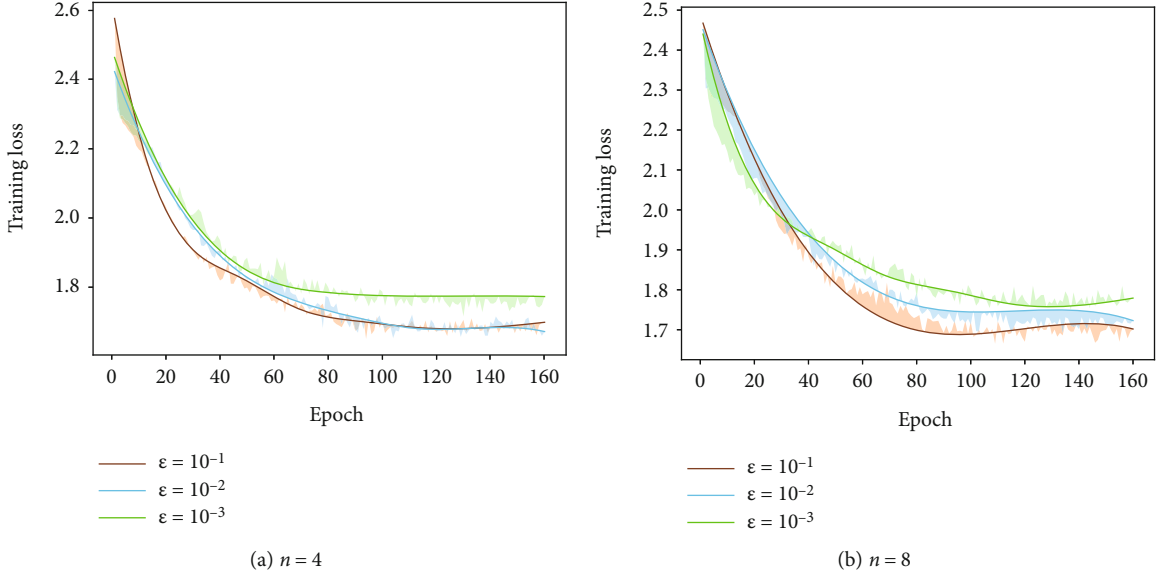


FIGURE 1: The convergence rate with different privacy budgets.

We can bound the second last term using  $\sigma$ :

$$\begin{aligned}
& \gamma^2 L \mathbb{E} \left\| \frac{\sum_{i=1}^n \nabla F_i(x_{k,i}; \xi_{k,i}) - \sum_{i=1}^n \nabla f_i(x_{k,i})}{n} \right\|^2 \\
&= \frac{\gamma^2 L}{n^2} \sum_{i=1}^n \mathbb{E} \|\nabla F_i(x_{k,i}; \xi_{k,i}) - \nabla f_i(x_{k,i})\|^2 + \frac{2\gamma^2 L}{n^2} \sum_{i=1}^n \sum_{i'=i+1}^n n \mathbb{E} \langle \nabla F_i(x_{k,i}; \xi_{k,i}) \\
&\quad - \nabla f_i(x_{k,i}), \nabla F_{i'}(x_{k,i'}; \xi_{k,i'}) - \nabla f_{i'}(x_{k,i'}) \rangle = \frac{\gamma^2 L}{n^2} \sum_{i=1}^n \mathbb{E} \|\nabla F_i(x_{k,i}; \xi_{k,i}) \\
&\quad - \nabla f_i(x_{k,i})\|^2 + \frac{2\gamma^2 L}{n^2} \sum_{i=1}^n \sum_{i'=i+1}^n n \mathbb{E} \langle \nabla F_i(x_{k,i}; \xi_{k,i}) \\
&\quad - \nabla f_i(x_{k,i}), \mathbb{E}_{\xi_{k,i'}} \nabla F_{i'}(x_{k,i'}; \xi_{k,i'}) - \nabla f_{i'}(x_{k,i'}) \rangle \\
&= \frac{\gamma^2 L}{n^2} \sum_{i=1}^n \mathbb{E} \|\nabla F_i(x_{k,i}; \xi_{k,i}) - \nabla f_i(x_{k,i})\|^2 \leq \frac{\gamma^2 L}{n} \sigma^2,
\end{aligned} \tag{57}$$

where the last step is true because of assumption 3.

Then, it follows from (56):

$$\begin{aligned}
\mathbb{E} f\left(\frac{X_{k+1} \mathbf{1}_n}{n}\right) &\leq \mathbb{E} f\left(\frac{X_k \mathbf{1}_n}{n}\right) - \gamma \mathbb{E} \left\langle \nabla f\left(\frac{X_k \mathbf{1}_n}{n}\right), \frac{\partial f(X_k) \mathbf{1}_n}{n} \right\rangle \\
&\quad + \frac{1}{2} \mathbb{E} \left\| \nabla f\left(\frac{X_k \mathbf{1}_n}{n}\right) \right\|^2 + \frac{1+2L}{2} \mathbb{E} \left\| \frac{\sum_{i=1}^n \eta_{k,i}}{n} \right\|^2 \\
&\quad + \frac{\gamma^2 L}{n} \sigma^2 + \gamma^2 L \mathbb{E} \left\| \frac{\sum_{i=1}^n \nabla f_i(x_{k,i})}{n} \right\|^2 \\
&\stackrel{(33)}{\leq} \mathbb{E} f\left(\frac{X_k \mathbf{1}_n}{n}\right) - \frac{\gamma - 2\gamma^2 L}{2} \mathbb{E} \left\| \frac{\partial f(X_k) \mathbf{1}_n}{n} \right\|^2 \\
&\quad - \frac{\gamma - 1}{2} \mathbb{E} \left\| \nabla f\left(\frac{X_k \mathbf{1}_n}{n}\right) \right\|^2 + \frac{4(1+2L)G^2 d \gamma^2}{\varepsilon^2} \\
&\quad + \frac{\gamma^2 L}{n} \sigma^2 + \underbrace{\frac{\gamma}{2} \mathbb{E} \left\| \nabla f\left(\frac{X_k \mathbf{1}_n}{n}\right) - \frac{\partial f(X_k) \mathbf{1}_n}{n} \right\|^2}_{=X},
\end{aligned} \tag{58}$$

where the last step comes from  $2\langle a, b \rangle = \|a\|^2 + \|b\|^2 - \|a - b\|^2$ .

We then bound the equation X:

$$\begin{aligned}
X &= \mathbb{E} \left\| \nabla f\left(\frac{X_k \mathbf{1}_n}{n}\right) - \frac{\partial f(X_k) \mathbf{1}_n}{n} \right\|^2 \\
&= \mathbb{E} \left\| \frac{\sum_{i=1}^n \nabla f_i\left(\left(\frac{\sum_{i'=1}^n x_{k,i'}}{n}\right)\right)}{n} - \frac{\sum_{i=1}^n \nabla f_i(x_{k,i})}{n} \right\|^2 \\
&\leq \frac{1}{n} \sum_{i=1}^n \mathbb{E} \left\| \nabla f_i\left(\frac{\sum_{i'=1}^n x_{k,i'}}{n}\right) - \nabla f_i(x_{k,i}) \right\|^2 \\
&\stackrel{\text{Assumption 1}}{\leq} \frac{L^2}{n} \sum_{i=1}^n \underbrace{\mathbb{E} \left\| \frac{\sum_{i'=1}^n x_{k,i'}}{n} - x_{k,i} \right\|^2}_{=Dis_{k,i}},
\end{aligned} \tag{59}$$

where the first inequality comes from  $\|\sum_{i=1}^n a_i\|^2 \leq n \sum_{i=1}^n \|a_i\|^2$ .

According to Equation (37) in Lemma 12, we have the bound of  $Dis_{k,i}$ . Then, we will bound its average  $M_k$  on all nodes as follows:

$$\begin{aligned}
\mathbb{E} M_k &= \frac{\mathbb{E} \sum_{i=1}^n Dis_{k,i}}{n} = \frac{48(n-1)G^2 d \gamma^2}{\varepsilon^2 (1-\sqrt{\rho})^2} + \frac{4\gamma^2 (n-1) \sigma^2}{1-\rho} \\
&\quad + \frac{36\gamma^2 (n-1) \zeta^2}{(1-\sqrt{\rho})^2} + 12(n-1)\gamma^2 L^2 \sum_{s=0}^{k-1} \mathbb{E} M_k \\
&\quad \cdot \left( \frac{2\sqrt{\rho}^{k-s-1}}{1-\sqrt{\rho}} + \rho^{k-s-1} \right) + \frac{12(n-1)}{n} \gamma^2 \sum_{s=0}^{k-1} \mathbb{E} \left\| \nabla f\left(\frac{X_s \mathbf{1}_n}{n}\right) \mathbf{1}_n^T \right\|^2 \\
&\quad \cdot \left( \frac{2\sqrt{\rho}^{k-s-1}}{1-\sqrt{\rho}} + \rho^{k-s-1} \right).
\end{aligned} \tag{60}$$



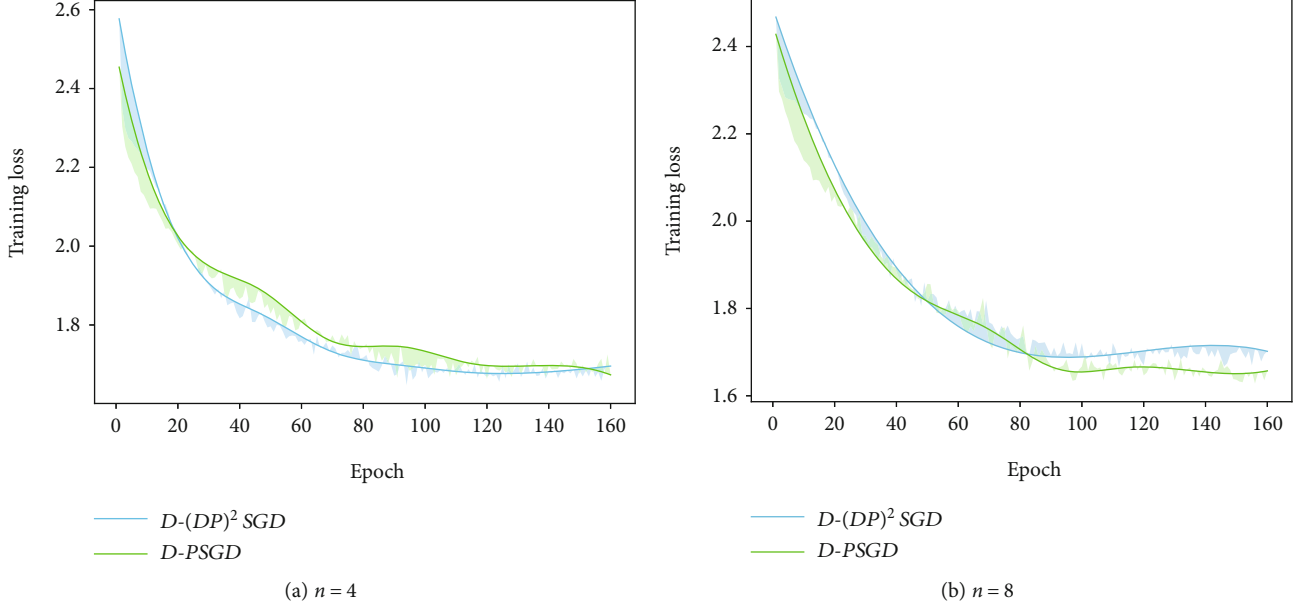


FIGURE 2: Comparison between dynamic networks and static networks.

Summing it from  $k = 0$  to  $K - 1$ , we can get the following result:

$$\begin{aligned}
\sum_{k=0}^{K-1} \mathbb{E}M_k &\leq \frac{48(n-1)G^2d\gamma^2K}{\varepsilon^2(1-\sqrt{\rho})^2} + \frac{4\gamma^2(n-1)\sigma^2K}{1-\rho} + \frac{36\gamma^2(n-1)\zeta^2K}{(1-\sqrt{\rho})^2} \\
&\quad + 12(n-1)\gamma^2L^2 \sum_{k=0}^{K-1} \sum_{s=0}^{k-1} \mathbb{E}M_k \left( \frac{2\sqrt{\rho}^{k-s-1}}{1-\sqrt{\rho}} + \rho^{k-s-1} \right) \\
&\quad + \frac{12(n-1)}{n} \gamma^2 \sum_{k=0}^{K-1} \sum_{s=0}^{k-1} \mathbb{E} \left\| \nabla f \left( \frac{X_s \mathbf{1}_n}{n} \right) \mathbf{1}_n^T \right\|^2 \left( \frac{2\sqrt{\rho}^{k-s-1}}{1-\sqrt{\rho}} + \rho^{k-s-1} \right) \\
&\leq \frac{48(n-1)G^2d\gamma^2K}{\varepsilon^2(1-\sqrt{\rho})^2} + \frac{4\gamma^2(n-1)\sigma^2K}{1-\rho} + \frac{36\gamma^2(n-1)\zeta^2K}{(1-\sqrt{\rho})^2} \\
&\quad + 12(n-1)\gamma^2L^2 \sum_{k=0}^{K-1} \mathbb{E}M_k \left( \frac{1}{1-\rho} + \frac{2}{(1-\sqrt{\rho})^2} \right) \\
&\quad + \frac{12(n-1)}{n} \gamma^2 \sum_{k=0}^{K-1} \mathbb{E} \left\| \nabla f \left( \frac{X_s \mathbf{1}_n}{n} \right) \mathbf{1}_n^T \right\|^2 \left( \frac{1}{1-\rho} + \frac{2}{(1-\sqrt{\rho})^2} \right) \\
&\leq \frac{48(n-1)G^2d\gamma^2K}{\varepsilon^2(1-\sqrt{\rho})^2} + \frac{4\gamma^2(n-1)\sigma^2K}{1-\rho} + \frac{36\gamma^2(n-1)\zeta^2K}{(1-\sqrt{\rho})^2} \\
&\quad + \frac{36(n-1)\gamma^2L^2}{(1-\sqrt{\rho})^2} \sum_{k=0}^{K-1} \mathbb{E}M_k + \frac{36\gamma^2(n-1)}{(1-\sqrt{\rho})^2n} \sum_{k=0}^{K-1} \mathbb{E} \left\| \nabla f \left( \frac{X_k \mathbf{1}_n}{n} \right) \mathbf{1}_n^T \right\|^2.
\end{aligned} \tag{61}$$

We then can get the bound of the summation of  $\mathbb{E}M_k$ 's from  $k = 0$  to  $K - 1$ :

$$\begin{aligned}
\left( 1 - \frac{36\gamma^2(n-1)L^2}{(1-\sqrt{\rho})^2} \right) \sum_{k=0}^{K-1} \mathbb{E}M_k &\leq \frac{48(n-1)G^2d\gamma^2K}{\varepsilon^2(1-\sqrt{\rho})^2} + \frac{4\gamma^2(n-1)\sigma^2K}{1-\rho} \\
&\quad + \frac{36\gamma^2(n-1)\zeta^2K}{(1-\sqrt{\rho})^2} \\
&\quad + \frac{36\gamma^2(n-1)}{(1-\sqrt{\rho})^2n} \sum_{k=0}^{K-1} \mathbb{E} \left\| \nabla f \left( \frac{X_k \mathbf{1}_n}{n} \right) \mathbf{1}_n^T \right\|^2.
\end{aligned} \tag{62}$$

Rearranging the term, it can be obtained that

$$\begin{aligned}
\sum_{k=0}^{K-1} \mathbb{E}M_k &\leq \frac{48(n-1)G^2d\gamma^2K}{\varepsilon^2(1-\sqrt{\rho})^2 \left( 1 - \left( (36\gamma^2(n-1)L^2) / \left( (1-\sqrt{\rho})^2 \right) \right) \right)} \\
&\quad + \frac{4\gamma^2(n-1)\sigma^2K}{(1-\rho) \left( 1 - \left( (36\gamma^2(n-1)L^2) / \left( (1-\sqrt{\rho})^2 \right) \right) \right)} \\
&\quad + \frac{36\gamma^2(n-1)\zeta^2K}{(1-\sqrt{\rho})^2 \left( 1 - \left( (36\gamma^2(n-1)L^2) / \left( (1-\sqrt{\rho})^2 \right) \right) \right)} \\
&\quad + \frac{36\gamma^2(n-1)}{(1-\sqrt{\rho})^2n \left( 1 - \left( (36\gamma^2(n-1)L^2) / \left( (1-\sqrt{\rho})^2 \right) \right) \right)} \\
&\quad \cdot \sum_{k=0}^{K-1} \mathbb{E} \left\| \nabla f \left( \frac{X_k \mathbf{1}_n}{n} \right) \mathbf{1}_n^T \right\|^2.
\end{aligned} \tag{63}$$

Plugging the bound of  $M_k$  into  $X$ :

$$X \leq \frac{L^2}{n} \sum_{i=1}^n \mathbb{E}Dis_{k,i} = L^2 \mathbb{E}M_k. \tag{64}$$

Then, we bound the  $\mathbb{E}f((X_{k+1}\mathbf{1}_n)/n)$  by the above bound,

$$\begin{aligned}
\mathbb{E}f\left(\frac{X_{k+1}\mathbf{1}_n}{n}\right) &\leq \mathbb{E}f\left(\frac{X_k\mathbf{1}_n}{n}\right) - \frac{\gamma-2\gamma^2L}{2} \mathbb{E} \left\| \frac{\partial f(X_k)\mathbf{1}_n}{n} \right\|^2 - \frac{\gamma-1}{2} \mathbb{E} \left\| \nabla f\left(\frac{X_k\mathbf{1}_n}{n}\right) \right\|^2 \\
&\quad + \frac{4(1+2L)G^2d\gamma^2}{\varepsilon^2} + \frac{\gamma^2L\sigma^2}{n} + \frac{\gamma}{2} X \\
&\leq \mathbb{E}f\left(\frac{X_k\mathbf{1}_n}{n}\right) - \frac{\gamma-2\gamma^2L}{2} \mathbb{E} \left\| \frac{\partial f(X_k)\mathbf{1}_n}{n} \right\|^2 - \frac{\gamma-1}{2} \mathbb{E} \left\| \nabla f\left(\frac{X_k\mathbf{1}_n}{n}\right) \right\|^2 \\
&\quad + \frac{4(1+2L)G^2d\gamma^2}{\varepsilon^2} + \frac{\gamma^2L\sigma^2}{n} + \frac{\gamma}{2} L^2 \mathbb{E}M_k.
\end{aligned} \tag{65}$$

Summing from  $k = 0$  to  $k = K - 1$ :

$$\begin{aligned}
& \frac{\gamma - 2\gamma^2 L}{2} \sum_{k=0}^{K-1} \mathbb{E} \left\| \frac{\partial f(X_k) 1_n}{n} \right\|^2 + \frac{\gamma - 1}{2} \sum_{k=0}^{K-1} \mathbb{E} \left\| \nabla f \left( \frac{X_k 1_n}{n} \right) \right\|^2 \\
& \leq f(0) - f^* + \frac{4(1+2L)G^2 d \gamma^2 K}{\varepsilon^2} + \frac{\gamma^2 K L \sigma^2}{n} + \frac{\gamma}{2} L^2 \sum_{k=0}^{K-1} \mathbb{E} M_k \\
& \stackrel{(61)}{\leq} f(0) - f^* + \frac{4(1+2L)G^2 d \gamma^2 K}{\varepsilon^2} + \frac{\gamma^2 K L \sigma^2}{n} \\
& \quad + \frac{\gamma}{2} L^2 \left( \frac{48(n-1)G^2 d \gamma^2 K}{\varepsilon^2 (1-\sqrt{\rho})^2 \left( 1 - \left( (36\gamma^2(n-1)L^2) / \left( (1-\sqrt{\rho})^2 \right) \right) \right)} \right) \\
& \quad + \frac{\gamma}{2} L^2 \left( \frac{4\gamma^2(n-1)\sigma^2 K}{(1-\rho) \left( 1 - \left( (36\gamma^2(n-1)L^2) / \left( (1-\sqrt{\rho})^2 \right) \right) \right)} \right) \\
& \quad + \frac{\gamma}{2} L^2 \left( \frac{36\gamma^2(n-1)\zeta^2 K}{(1-\sqrt{\rho})^2 \left( 1 - \left( (36\gamma^2(n-1)L^2) / \left( (1-\sqrt{\rho})^2 \right) \right) \right)} \right)
\end{aligned}$$

$$\begin{aligned}
& + \frac{\gamma}{2} L^2 \left( \frac{36\gamma^2(n-1)}{(1-\sqrt{\rho})^2 n \left( 1 - \left( (36\gamma^2(n-1)L^2) / \left( (1-\sqrt{\rho})^2 \right) \right) \right)} \right) \\
& \quad \cdot \sum_{k=0}^{K-1} \mathbb{E} \left\| \nabla f \left( \frac{X_k 1_n}{n} \right) 1_n^T \right\|^2 = f(0) - f^* + \frac{4(1+2L)G^2 d \gamma^2 K}{\varepsilon^2} + \frac{\gamma^2 K L \sigma^2}{n} \\
& \quad + \frac{24(n-1)L^2 G^2 \gamma^3 K}{\varepsilon^2 (1-\sqrt{\rho})^2 \left( 1 - \left( (36\gamma^2(n-1)L^2) / \left( (1-\sqrt{\rho})^2 \right) \right) \right)} \\
& \quad + \frac{2\gamma^3 L^2 (n-1)\sigma^2}{(1-\rho) \left( 1 - \left( (36\gamma^2(n-1)L^2) / \left( (1-\sqrt{\rho})^2 \right) \right) \right)} K \\
& \quad + \frac{18\gamma^3 L^2 (n-1)\zeta^2}{(1-\sqrt{\rho})^2 \left( 1 - \left( (36\gamma^2(n-1)L^2) / \left( (1-\sqrt{\rho})^2 \right) \right) \right)} K \\
& \quad + \frac{18\gamma^3 L^2 (n-1)}{(1-\sqrt{\rho})^2 \left( 1 - \left( (36\gamma^2(n-1)L^2) / \left( (1-\sqrt{\rho})^2 \right) \right) \right)} \sum_{k=0}^{K-1} \mathbb{E} \left\| \nabla f \left( \frac{X_k 1_n}{n} \right) \right\|^2.
\end{aligned} \tag{66}$$

Rearranging the terms, we get the following result:

$$\begin{aligned}
& \frac{(1-\gamma L/2) \sum_{k=0}^{K-1} \mathbb{E} \left\| \frac{\partial f(X_k) 1_n}{n} \right\|^2 + \left( (1/2) - \left( (18\gamma^2(n-1)L^2) / \left( (1-\sqrt{\rho})^2 \left( 1 - \left( (36\gamma^2(n-1)L^2) / \left( (1-\sqrt{\rho})^2 \right) \right) \right) \right) \right) \sum_{k=0}^{K-1} \mathbb{E} \left\| \nabla f \left( \frac{X_k 1_n}{n} \right) \right\|^2}{K} \\
& \leq \frac{f(0) - f^*}{\gamma K} + \frac{4(1+2L)G^2 d \gamma}{\varepsilon^2} + \frac{\gamma L}{n} \sigma^2 + \frac{24(n-1)L^2 G^2 \gamma^2}{\varepsilon^2 (1-\sqrt{\rho})^2 \left( 1 - \left( (36\gamma^2(n-1)L^2) / \left( (1-\sqrt{\rho})^2 \right) \right) \right)} + \frac{2\gamma^2 L^2 (n-1)\sigma^2}{(1-\rho) \left( 1 - \left( (36\gamma^2(n-1)L^2) / \left( (1-\sqrt{\rho})^2 \right) \right) \right)} \\
& \quad + \frac{18\gamma^2(n-1)L^2 \zeta^2}{(1-\sqrt{\rho})^2 \left( 1 - \left( (36\gamma^2(n-1)L^2) / \left( (1-\sqrt{\rho})^2 \right) \right) \right)}.
\end{aligned} \tag{67}$$

This completes the proof.

*Proof* (Proof of Corollary 6). Substituting  $\gamma = 1/(2L + \sigma\sqrt{K/n})$  into the result of Theorem 5 and removing the first term of the RHS on the LHS, we can obtain that

$$\begin{aligned}
& \frac{B_1 \sum_{k=0}^{K-1} \mathbb{E} \left\| \nabla f \left( \frac{X_k 1_n}{n} \right) \right\|^2}{K} \leq \frac{(2L + \sigma\sqrt{K/n})(f(0) - f^*)}{K} + \frac{4(1+2L)G^2 d}{(2L + \sigma\sqrt{K/n})\varepsilon^2} \\
& \quad + \frac{L\sigma^2}{2nL + \sigma\sqrt{Kn}} + \left( \frac{2(n-1)L^2}{(2L + \sigma\sqrt{K/n})^2 B_2} \right) \\
& \quad \cdot \left( \frac{12G^2}{\varepsilon^2 (1-\sqrt{\rho})^2} + \frac{\sigma^2}{(1-\rho)} + \frac{9\zeta^2}{(1-\sqrt{\rho})^2} \right) \\
& \leq \frac{2L(f(0) - f^*)}{K} + \frac{(f(0) - f^*)\sigma}{\sqrt{Kn}} + \frac{4(1+2L)G^2 d}{\sigma\sqrt{Kn}\varepsilon^2} \\
& \quad + \frac{L\sigma^2}{\sigma\sqrt{Kn}} + \left( \frac{2(n-1)L^2}{(\sigma\sqrt{K/n})^2 B_2} \right) \\
& \quad \cdot \left( \frac{12G^2}{\varepsilon^2 (1-\sqrt{\rho})^2} + \frac{\sigma^2}{(1-\rho)} + \frac{9\zeta^2}{(1-\sqrt{\rho})^2} \right).
\end{aligned} \tag{68}$$

Let  $(G/\varepsilon) \leq \sqrt{((f(0) - f^*) + L)\sigma / (4(1+2L)d n)}$ , and we show  $B_1$  and  $B_2$  are approximately constants when (16) is

satisfied.

$$\begin{aligned}
B_1 &= \left( \frac{1}{2} - \frac{18\gamma^2(n-1)L^2}{(1-\sqrt{\rho})^2 B_2} \right), \\
B_2 &= \left( 1 - \frac{36\gamma^2(n-1)L^2}{(1-\sqrt{\rho})^2} \right).
\end{aligned} \tag{69}$$

Note that

$$\begin{aligned}
\gamma^2 &\leq \frac{(1-\sqrt{\rho})^2}{72(n-1)L^2} \Rightarrow B_2 \geq \frac{1}{2}, \\
\gamma^2 &\leq \frac{(1-\sqrt{\rho})^2}{144(n-1)L^2} \Rightarrow B_1 \geq \frac{1}{4}.
\end{aligned} \tag{70}$$

Since  $\gamma^2 \leq (n/(\sigma^2 K))$ , as long as we have

$$\frac{n}{\sigma^2 K} \leq \frac{(1-\sqrt{\rho})^2}{144(n-1)L^2}, \tag{71}$$

$B_2 \geq 1/2$  and  $B_1 \geq 1/4$  will be satisfied. Then, we can obtain  $K \geq (144n(n-1)L^2) / (\sigma^2(1-\sqrt{\rho})^2)$ .

Let  $K \geq ((16n^3(n-1)^2L^4)/(\sigma^6(f(0) - f^* + L)^2))$   
 $((12G^2/(\varepsilon^2(1 - \sqrt{\rho})^2)) + (\sigma^2/(1 - \rho)) + (9\xi^2/((1 - \sqrt{\rho})^2)))^2$ ,  
 then

$$\frac{\sum_{k=0}^{K-1} \mathbb{E} \|\nabla f((X_k 1_n)/n)\|^2}{K} \leq \frac{8L(f(0) - f^*)}{K} + \frac{12(f(0) - f^* + L)\sigma}{\sqrt{Kn}}. \quad (72)$$

## 7. Experiments

In this section, we perform extensive simulations to evaluate our proposed algorithm. In particular, we compare the convergence rate of our proposed algorithm with the best-known D-PSGD algorithm give in [1], in the settings of different privacy budgets, different number of nodes and different extents of dynamicity.

In our experiments, we evaluate our proposed algorithm on image classification tasks. We train ResNet model on CIFAR-10 dataset. Moreover, we use MPI to implement the communication scheme. We run our experiments on a CPU server cluster. Each server has 32 cores, which is an Intel Xeon E5-2620 v4 @ 2.10GHz cluster. Each server is equipped with 128G memory.

**7.1. Impact of Privacy Budgets.** We evaluate the import of privacy budget on the convergence of our proposed algorithm in a dynamic network. Here, we run our algorithm in a dynamic network with different number of nodes under different privacy budgets. The results are illustrated in Figure 1, where the privacy budget  $\varepsilon$  is set to  $10^{-1}$ ,  $10^{-2}$ , and  $10^{-3}$ , respectively. It can be seen that the smaller  $\varepsilon$  is, the slower the learning converges. This is because a smaller privacy budget means more noise are added, which affects the convergence speed of the algorithm.

**7.2. Impact of Dynamicity.** We compare our algorithm with the best-known D-PSGD algorithm (with privacy protection) in a static network. Due to D-PSGD is applied to a ring structure, we set the expected degree in the dynamic network as 2. Here, the privacy budget is set to  $10^{-1}$ , and the number of nodes is 4 and 8. From Figure 2, we can find that our proposed algorithm can reach the same convergence rate in dynamic networks as the D-PSGD algorithm (with privacy protection) in static networks.

## 8. Conclusion

We presented D-(DP)<sup>2</sup>SGD, a decentralized parallel stochastic gradient descent algorithm with privacy preservation in dynamic networks. With theoretical analysis and extensive experiments, it shows that our proposed algorithm can achieve the same convergence rate as the best know previous work in static networks without considering privacy issue. Based on this work, it is meaningful to further devise privacy-preserving algorithms in an asynchronous dynamic environment.

## Data Availability

1. The CIFAR-10 data used to support the findings of this study have been deposited in <http://www.cs.toronto.edu/~kriz/cifar.html>. 2. The software code used to support the findings of this study have been deposited in <https://github.com/zongruisdu/D-DPDP-SGD>.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This work is partially supported by the National Key R&D Program of China with grant no. 2019YFB2102600 and NSFC (No. 61971269).

## References

- [1] X. Lian, C. Zhang, H. Zhang, C.-J. Hsieh, W. Zhang, and J. Liu, "Can decentralized algorithms outperform centralized algorithms? A case study for decentralized parallel stochastic gradient descent," in *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017*, pp. 5330–5340, Long Beach, CA, USA, December 2017.
- [2] J. Xu, W. Zhang, and F. Wang, "A(dp)2sgd: asynchronous decentralized parallel stochastic gradient descent with differential privacy," 2020, <https://arxiv.org/abs/2008.09246>.
- [3] M. Zhu and Q. Chen, "Big data image classification based on distributed deep representation learning model," *IEEE Access*, vol. 8, pp. 133890–133904, 2020.
- [4] W. Zhang, S. Gupta, X. Lian, and J. Liu, "Staleness-aware async-sgd for distributed deep learning," in *Proceedings of the Twenty-Fifth International Joint Conference on Artificial Intelligence, IJCAI 2016*, pp. 2350–2356, New York, NY, USA, July 2016.
- [5] Y. LeCun, Y. Bengio, and G. E. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.
- [6] W. Xu, H. Peng, X. Zeng, F. Zhou, X. Tian, and X. Peng, "A hybrid modelling method for time series forecasting based on a linear regression model and deep learning," *Applied Intelligence*, vol. 49, no. 8, pp. 3002–3015, 2019.
- [7] S. Yang, B. Ren, X. Zhou, and L. Liu, "Parallel distributed logistic regression for vertical federated learning without third-party coordinator," 2019, <https://arxiv.org/abs/1911.09824>.
- [8] S. H. Alsamhi, O. Ma, and M. S. Ansari, "Convergence of machine learning and robotics communication in collaborative assembly: mobility, connectivity and future perspectives," *Journal of Intelligent & Robotic Systems*, vol. 98, no. 3-4, pp. 541–566, 2020.
- [9] A. Elgabli, J. Park, A. S. Bedi, M. Bennis, and V. Aggarwal, "Communication efficient framework for decentralized machine learning," in *54th Annual Conference on Information Sciences and Systems, CISS 2020*, pp. 1–5, Princeton, NJ, USA, March 2020.
- [10] S. Y. Hashemi and F. S. Aliee, "Fuzzy, dynamic and trust based routing protocol for iot," *Journal of Network and Systems Management*, vol. 28, no. 4, pp. 1248–1278, 2020.

- [11] Z. Cai, Z. Xu, and Y. Jiguo, "A differential-private framework for urban traffic flows estimation via taxi companies," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6492–6499, 2019.
- [12] K. Lim and K. M. Tuladhar, "LIDAR: lidar information based dynamic V2V authentication for roadside infrastructure-less vehicular networks," in *16th IEEE Annual Consumer Communications & Networking Conference, CCNC 2019*, pp. 1–6, Las Vegas, NV, USA, January 2019.
- [13] S. Chen, Y. Tao, D. Yu, F. Li, B. Gong, and X. Cheng, "Privacy-preserving collaborative learning for multiarmed bandits in iot," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3276–3286, 2021.
- [14] Z. Xu, Z. Cai, J. Yu, C. Wang, and Y. Li, "Follow but no track: privacy preserved profile publishing in cyber-physical social systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1868–1878, 2017.
- [15] S. Chen, Y. Tao, D. Yu, F. Li, and B. Gong, "Distributed learning dynamics of multi-armed bandits for edge intelligence," *Journal of Systems Architecture*, vol. 114, p. 101919, 2020.
- [16] X. Lian, W. Zhang, C. Zhang, and J. Liu, "Asynchronous decentralized parallel stochastic gradient descent," in *Proceedings of the 35th International Conference on Machine Learning, ICML 2018*, pp. 3049–3058, Stockholm, Sweden, July 2018.
- [17] M. I. Qureshi, R. Xin, S. Kar, and U. A. Khan, "S-ADDOPT: decentralized stochastic first-order optimization over directed graphs," *IEEE Control Systems Letters*, vol. 5, no. 3, pp. 953–958, 2021.
- [18] Y. Yuan, F. Li, D. Yu, J. Zhao, J. Yu, and X. Cheng, "Distributed social learning with imperfect information," *IEEE Transactions on Network Science and Engineering*, 2020.
- [19] H. R. Feyzmahdavian, A. Aytekin, and M. Johansson, "An asynchronous mini-batch algorithm for regularized stochastic optimization," *IEEE Transactions on Automatic Control*, vol. 61, no. 12, pp. 3740–3754, 2016.
- [20] A. Agarwal and J. C. Duchi, "Distributed delayed stochastic optimization," in *Advances in Neural Information Processing Systems 24: 25th Annual Conference on Neural Information Processing Systems 2011. Proceedings of a meeting held 12-14 December 2011*, pp. 873–881, Granada, Spain, 2011.
- [21] X. Lian, Y. Huang, Y. Li, and J. Liu, "Asynchronous parallel stochastic gradient for nonconvex optimization," in *Advances in Neural Information Processing Systems 28: Annual Conference on Neural Information Processing Systems 2015*, pp. 2737–2745, Montreal, Quebec, Canada, December 2015.
- [22] Z. Cai and Z. He, "Trading private range counting over big iot data," in *39th IEEE International Conference on Distributed Computing Systems, ICDCS 2019*, pp. 144–153, Dallas, TX, USA, July 2019.
- [23] Z. Cai and Z. Xu, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.
- [24] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Differentially private asynchronous federated learning for mobile edge computing in urban informatics," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2134–2143, 2020.
- [25] Y. Zhou and S. Tang, "Differentially private distributed learning," *INFORMS Journal on Computing*, vol. 32, no. 3, pp. 779–789, 2020.
- [26] H.-P. Cheng, P. Yu, H. Hu et al., "LEASGD: an efficient and privacy-preserving decentralized algorithm for distributed learning," 2018, <https://arxiv.org/abs/1811.11124>.
- [27] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3-4, pp. 211–407, 2014.
- [28] J. Zhu, C. Xu, J. Guan, and D. O. Wu, "Differentially private distributed online algorithms over time-varying directed networks," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 4–17, 2018.

## Research Article

# A High-Quality Authenticatable Visual Secret Sharing Scheme Using SGX

Denghui Zhang  and Zhaoquan Gu 

Cyberspace Institute of Advanced Technology, Guangzhou University, China

Correspondence should be addressed to Zhaoquan Gu; zqgu@gzhu.edu.cn

Received 12 November 2020; Revised 14 December 2020; Accepted 26 February 2021; Published 17 March 2021

Academic Editor: Zhuojun Duan

Copyright © 2021 Denghui Zhang and Zhaoquan Gu. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Visual cryptography scheme (VCS) is a secret-sharing scheme which encrypts images as shares and can decrypt shares without digital devices. Although a participant can reveal the secret image by merely stacking a sufficient number of shares, the visual quality of recovered images is reduced, and malicious adversaries can cheat participants by giving faked shares. The paper presents a novel VCS called T-VCS (trusted VCS) which consists of two main components: a high-quality VCS and an enhanced verification scheme of shares based on the emerging Intel Software Guard eXtensions (SGX). While providing high-quality recovery, T-VCS keeps the size of the shares the same as the original secret image. We use SGX to act as a trusted third party (TTP) to verify the validity of the shares in an attested enclave without degrading the image quality. The experimental results show that T-VCS can achieve a balance among contrast, share size, and verification efficiency.

## 1. Introduction

With the development of the Internet of things (IoT), wearable and mobile devices are forming more and more social and big data networks. It is now common to take and transfer personal and sensitive data on an untrusted communication channel [1]. Unfortunately, both diverse social datasets and big data technologies raise stringent privacy concerns. Malicious users can perceive, collect, analyze, and upload large amounts of data; the privacy issues related to the collection of data have been widely concerned and become a research hotspot [2–4]. There is an urgent need to ensure the security of data that include images.

In 1994, Naor and Shamir [5] introduced a VCS which combines the notions of perfect ciphers and secret sharing in cryptography with those of raster graphics. In the Naor and Shamir's  $k$ -out-of- $n$  threshold VCS, they split up a secret binary image into  $n$  shares (known as sheets or pieces) and distribute them to each participant (known as shareholder). The decryption is impossible unless  $k$  or more participants superimpose any  $k$  transparencies together. Participants can print out shares onto transparencies and superimpose them

to reconstruct the original image. The merit of VCS lies in the fact that the Human Visual System (HVS) can recover the shared secret directly. Thus, the decryption process is computation-free. This feature makes VCS particularly suitable for human-computer interaction scenarios with limited computing or networks, such as ATM [6, 7] and electronic voting [8].

Despite the fact that VCS eliminates complex computation of the traditional cryptography, there remain two significant drawbacks. One is the pixel expansion and contrast depression of the recovered secret, while human eyes can only identify patterns of secret image when the contrast is good enough. Figure 1 illustrates the Naor and Shamir VCS. As shown in the first two columns, if the secret pixel  $p$  is white, superposition of the two shares always outputs a gray region where half of the pixels are white and half are black, no matter which column of subpixel pairs are chosen. As shown in the last two columns, if  $p$  is black, it yields the original black pixel. There is a contrast loss in this scheme since the original white pixel only yields a gray region. The width of the decoded image is twice that of the original secret image because  $p$  is expanded to two subpixels in each share.



Secret pixel	Share <sub>1</sub>	Share <sub>2</sub>	Stacked pixel
White	Black	White	White
White	White	Black	White
Black	Black	White	Black
Black	White	Black	Black

FIGURE 1: Construction of black and white pixels in a 2-out-of-2 VCS.

Pixel expansion of the shares implies that the size of secret image cannot be too big because a big transparency is inconvenient to align for recovery.

The other one is cheating problems in VCS. If there is a cheater who gives a faked share, sharevictims will fail to decrypt the secret image or believe that the decoded fake image is a genuine secret image. Figure 2 shows an example of cheating participants in the 2-out-of-2 VCS. If both participants are honest, they can recover the true secret image. However, if a malicious participant has information about the Share<sub>1</sub> that the participant A holds, he can construct a faked share FakeShare and cheat A to believe that the secret image is false, which Share<sub>1</sub> + FakeShare reveals.

Sharing secrets with high-quality recovery is interesting, and consequently, many improved VCSs have been proposed. Some schemes present methods where high-quality secret recovery is possible [9]. These schemes, however, rely on complicated computation or archive at the expense of expanding pixels. Other schemes avoid to expand the pixels on secret images at the expense of reducing image contrast [10].

Researchers have experimented with the idea of cheating VCS and proposed many cheating immune visual cryptography schemes (CIVCS). These schemes often expand the pixel or decline in contrast [11]. Furthermore, analysis results imply that these CIVCS are not enough to secure against cheater colluding [12]. One alternative is to make use of an online trusted authority to verify the validity of the stacked shares. These TTPs often run in untrusted remote environments, while software-based security is often insufficient due to vulnerabilities in applications or operating systems [13, 14].

In this paper, we propose a novel visual secret sharing scheme called T-VCS to address all the drawbacks listed above. This method retains the advantage of traditional visual cryptography without any cryptography computation. T-VCS eliminates pixel expansion by encrypting the pixels of secret images block by block instead of a single pixel. It first constructs a basis matrices' query table which corresponds precisely to the encrypted pixel block and then generates multiple share images by the odd-even quantization watermarking algorithm. The stacked shares have the same pixel permutation with the original image. So, we can recover a higher-quality image.

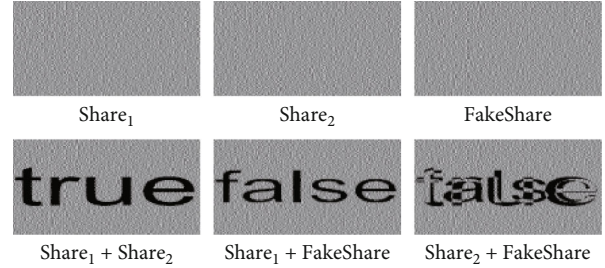


FIGURE 2: Cheating 2-out-of-2 VCS.

We make use of Intel SGX to ensure the validity of validation results. Intel SGX is a processor instruction set extension that allows the creation of a CPU-based TEE (Trusted Execution Environment), that is, a secure enclave.

We carry out verification in an attested enclave where participants can ensure even OS and higher priority software do not tamper with verification code. T-VCS seals the query table and watermark file into a disk to make watermarks undetectable.

The main contributions of this paper are as follows:

- (1) We propose a novel VCS that can both recover secret images with high quality and eliminate pixel expansion
- (2) We develop a self-attesting framework to verify the validity of shares based on TEE. This method neither requires the user to maintain additional verification data nor reduces image quality
- (3) We elaborately evaluate the performance of applying T-VCS to encode grayscale and color images and verifying sheets in TEE

The remainder of this paper is organized as follows. Section 2 introduces existing VCS and CIVCS and highlight their known limitations. Section 3 explains the proposed T-VCS and shows its effectiveness. After that, Section 4 gives experimental results and comparisons. Finally, Section 5 presents conclusions and future works.

## 2. Related Work

Born in 1994, VCS has been an emerging research field in the field of information security [15]. To address drawbacks of VCS, many improvements and extensions follow.

**2.1. Visual Cryptography Scheme.** To keep the size of the sharing images the same as the original secret image, Chen et al. [16] maps a block in a secret image onto a corresponding equal-sized block in the shared image. This scheme, however, may lose some information when the number of pixels describing the information only occupies a tiny part of a secret image. In the scheme of Yang et al. [17], we can distinguish the black and white due to the frequency of white pixels in a white area which is higher than that in a black area. However, this scheme is based on a probabilistic method and the value of contrast is not consistent with the recovered image.

TABLE 1: Feature comparisons among our proposal and previous schemes.

Schemes	Size invariant	Quality improvement	Cheating immune
Naor and Shamir [20]	×	√	×
Hu and Tzeng [11], Liu et al. [12]	×	×	√
Chen et al. [21]	√	√	√
T-VCS			

Hou and Tu [18] takes advantage of image contrast reduction and halftone technology to avoid expanding pixels in secret images. This method degrades the contrast of the resulting image by 50%. Superimposing shares is equivalent to an OR-logical operation on the corresponding rows. New visual cryptography models which utilize the polarisation of the light and XOR operation can keep image size [19], but this method does not work with printed transparencies since it is the idea behind VC.

To obtain a better contrast than the previous one, Naor and Shamir propose an alternative model for reconstruction [20]. This model improves the contrast from  $1/2$  to  $1 - 1/c$ , where  $c$  is both the number of sheets and the number of subpixels to map each pixel. This scheme expanded each pixel in the original image into  $c$  subpixels. The set of operations they call the cover semigroup inspires the design of T-VCS, while T-VCS can archive the same contrast without pixel expansion.

Most of the previous research work on black and white VCS, while it is an essential area of research to apply visual cryptography techniques to color images. This method allows the use of natural color images to secure information. The scheme of Hou [22] is one of the first color decomposition techniques to generate visual cryptograms for color images. Every color within the image can be decomposed into one of three primary colors. In contrast to color decomposition, Yang [17] proposes an additive color mixing scheme based on probabilities. One of the problems with these schemes is that the overall contrast is reduced when revealing secret images.

**2.2. Cheating Immune Visual Cryptography Schemes.** VCS assumes shareholders to be semihonest, and the image shown on the stacking of shares is a real secret image. Researchers, however, have present methods for cheating the basic VCS schemes [21] and consequently proposed many CIVCS by generating extra verification shares or expanding the pixel to embed extra authentication information. Hu and Tzeng [11] propose a generic method to convert a VCS to another VCS that has the property of cheating prevention. The overhead of the conversion is near-optimal in both contrast degression and pixel expansion. Liu et al. [12] first analyze the drawbacks of some known cheating immune visual cryptography schemes, then proposed a new CIVCS, which avoids all the previous drawbacks. However, this scheme has to randomly select  $t$  pixels from the original secret image to act as authentication pixels in each participant, which inevitably increases the burden of share management.

An alternative to prevent cheating in VCS is to use a TTP to validate shares. Yang and Lai proposed [23] used a TTP to perform the verification between the participants. Chen et al. [21] find that if an attacker knows the exact distribution of

black and white pixels of each share, then they can attack and cheat the TPP. Table 1 presents the comparison of existing methods and our scheme.

**2.3. Intel SGX.** A practice challenge of TTP is that they often run in an untrusted cloud environment [24], so the participant is not sure if a validation result is valid [25]. TEEs such as Intel SGX and ARM TrustZone [26] enable execution of programs in secure enclaves.

As an important research progress in the field of trusted computing, Intel SGX offers an efficient solution for anonymous authentication and verification. Besides shielding systems [27–29], SGX has been used in a number of applications including a map-reduce framework [30], machine learning and big data models [31, 32], and SQL querying [33]. The security of these client-server applications is based on the establishment of trust in a remotely executing program. The procedure requires an enclave to generate a hash of the code running inside it, which is signed by an Intel-provided service enclave running on the same platform. Participants are then able to verify the report through the Intel Attestation Service (IAS) provided by Intel. More details about SGX can be found in [34, 35].

### 3. T-VCS

In this section, we propose a novel VCS to address the contrast degression and pixel expansion problems at the same time. The contrast determines the clarity of the recovered secret by HVS. Having shares that are close to the original secret's size is easier to manage and transmit.

There are three modes of images: black and white, gray, and color. We treat a color image as the composition of three primary color images. Then, the halftone technology can transform a single-color image with gray levels into a binary image. So the research of black and white image is fundamental even in the study of color images.

We firstly deal with the black and white image, where a white pixel is denoted by the number 0 and a black pixel by 1. To construct shares of an image for participants, we need to prepare two groups,  $C_0$  and  $C_1$ , which consist of bit matrices. A row in matrix  $C_0$  and  $C_1$  corresponds to  $m$  subpixels of a pixel. For a white (or black) pixel in the image, we randomly choose a matrix from  $C_0$  or  $C_1$  and assign the row of groups to the corresponding position of share  $S_i$ ,  $i < n$ . Each pixel of the original image will be encoded into  $n$  subpixels, each of which consists of  $m$  subpixels. Instead of constructing  $C_0$  and  $C_1$  directly, we can construct two basis matrices  $S^0$  and  $S^1$  and let  $C_0$  and  $C_1$  be the set of all matrices obtained by permuting columns of  $S^0$  and  $S^1$ , respectively. So, we can write the basis matrices and collections of the 2-out-of-2 VCS as

Equation (2). By merging the sheets of participant *A* and participant *B*, that is, putting the *i*th sheet of *B* on top of the *i* sheet of *A*, we can reconstruct the secret images.

$$S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix},$$

$$S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \quad (1)$$

$$C^0 = \left\{ \left[ \begin{array}{c|c} 0 & 1 \\ 0 & 1 \end{array} \right] \mid \left[ \begin{array}{c|c} 1 & 0 \\ 1 & 0 \end{array} \right] \right\},$$

$$C^1 = \left\{ \left[ \begin{array}{c|c} 0 & 1 \\ 1 & 0 \end{array} \right] \mid \left[ \begin{array}{c|c} 1 & 0 \\ 0 & 1 \end{array} \right] \right\}. \quad (2)$$

**3.1. Generate Pixel Blocks.** The drawback of the traditional VCS is that the shares are  $n:m$  times the size of the secret image. So, we adopt block-wise operation and generate shares block by block for the nonexpansion scheme. A block in a share image corresponds to an equal-sized block in the secret image, while in the traditional expansionary VCS, a pixel is mapped onto a subpixel.

The cover semigroup operation inspires the design of T-VCS; Table 2 demonstrates the cover color rule of the monochromatic construction, where the top opaque wins. If we superimpose three pixels, that is, transparency, black, and white, respectively, we will get a white pixel at the top.

Figure 3(a) demonstrates the revealing procedure of the pixel block in which  $c = 4$  and the revealed pixels are [B; W; W; W]. The stacked pixels in Figure 3(a) represent neither the original single black nor white pixel, but the pixel block [B; W; W; W]. We number sheets from bottom to top, starting with zero. The participant *B* hold sheets numbered even, that is, {0, 2, 4, 6}th sheet. When stacking the four sheets, *B* only obtains an all-white image. The participant *A* holds sheets numbered odd, that is, {1, 3, 5, 7}, respectively. When stacking the four sheets, *A* only sees an all-black image.

Figure 4 illustrates sheets. There are two opaque colors (black and white) and a completely transparent one in the new model. It is obvious that the proposed share images do not leak any secret information from the share images. It should be noted that the white color in Figure 4 indicates transparency. To display white pixels on the white background, we replace the white sheets held by *B* with gray. The reconstruction is done by merging the sheets of *A* and *B*. When stacking them all together, we can obtain a clear secret image, as shown in Figure 5(d).

*A* holds  $c$  odd sheets, while *B* holds  $c$  even sheets. By rolling sheets held by *B* down a row (for the whole sheets, it is equivalent to roll down two rows), the position of the *i*th sheet will be  $(i + 1)\%c$ th. We are able to obtain the pixel block [B; B; W; W] as shown in Figure 3(b). Naor and Shamir have proved the contrast is  $1 - 1/c$  in the construction method [20]. By such a method, T-VCS can generate the basis matrices for kinds of pixel blocks.

TABLE 2: Color rule in shares and stacked images.

Color	White (W)	Black (B)	Transparent (T)
W	W	B	B
B	W	B	B
T	W	B	T

T-VCS gives a certain way to construct the basis matrices. There are  $4! = 24$  permutations for the case of 4 black pixels (the number of white pixels is 0). For the case of 3 black pixels (the number of white pixels is 1) or 1 black pixel (the number of white pixels is 3), taking 1 black pixel as an example, the black and white pixel must locate in the top (7) and bottom (2) layers; otherwise, there will be a white pixel in the bottom (2) layer, and this column will be covered by black pixels, resulting in the number of revealed black pixel pixels which is greater than 1. The number of permutations for the other three columns of white pixels are  $3! = 6$ .

For the case of 2 black pixels (the number of white pixels is 2), taking the 2 black pixels ([B; B; W; W]) as an example, the black pixels in columns 1 and 2 can only be selected from layers 5 and 7. Respectively, the white pixels in columns 1 and 2 can be selected in layers 2 and 4, to ensure that the superimposed pixels in columns 1 and 2 are black. However, if the white and black pixels in columns 1 and 2 are located in layers 1 and 3, after rolling twice, the superimposed white pixels will appear in columns 1 and 2, which is inconsistent with the precondition. So, there are two ways to arrange the white pixels in columns 1 and 2. The white pixels in columns 3 and 4 are similar, and there also are two ways to arrange them. So, the total arrangement is  $2 + 2 = 4$ . There are still other ways to construct the basis matrices besides the rotation method. So, what is given here is not the total number of permutations. The relationship between rows to roll and generated pixel blocks as shown in Table 3.

Each pixel block has multiple permutations. The scheme not only ensures the security of image encryption but also provides conditions for the subsequent zero watermark verification.

It should be noted that the roll period of the pixel block is 4 for the case  $c = 4$ , so when rolling down 4 rows, repeated pixel block will be generated. So, this scheme cannot generate all-black pixel block or all-white pixel block (in Table 3, the pixel block [W; W; W; W] cannot be generated). We replace the basis matrices of all-white blocks with those of 3 black and 1 white situation.

Our new scheme contains several important changes from previous work. The first difference is the order in which the transparencies are stacked. There is a requirement for order to correctly recover secret images. Therefore, we need to record the order of each share. The second change is that each participant has  $c$  sheets, rather than a single transparency. Each pixel in the original image is mapped into  $c$  subpixels. In order to facilitate the user to manage the sheets, we can use color images to store sheets of grayscale images and use the TIFF multilayer image format to store sheets of color images.



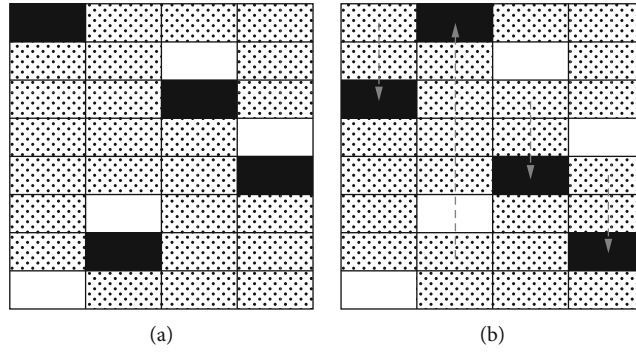


FIGURE 3: Stacking of gray-level visual cryptography without pixel expansion (the dot block represents transparency).

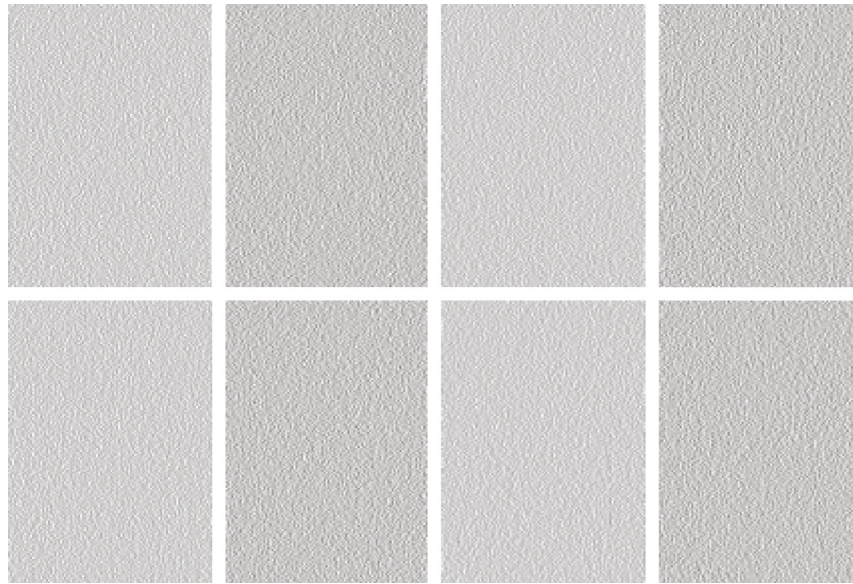


FIGURE 4: Encrypted sheets ( $c = 4$ ; contrast =  $1 - 1/c = c$ ).



Mode	Halftone	Hou [18]	Random T-VCS	T-VCS
PSNR	100.00%	51.57%	51.62%	68.06%
	(a)	(b)	(c)	(d)

FIGURE 5: Contrast comparison between Hou's VCS and T-VCS.

TABLE 3: Generate pixel blocks by rolling.

Rows to roll	Pixel block	Number of permutations
0	[B, B, B, B]	24
1	[B, B, B, W]	6
2	[W, B, B, W]	4
3	[W, W, W, B]	6
4	[W, W, W, W]	24

3.2. *Generate the Permutation of a Pixel Block.* In the halftone image, there are not only different pixel blocks but also different arrangements of the same pixel block. By permuting columns in Table 3 until getting the same arrangement as the original color blocks, T-VCS precomputes  $C_0$  and  $C_1$  for kinds of pixel blocks and permutations.

An objective way to test alteration between the original image and the recovered image is to use PSNR (Peak

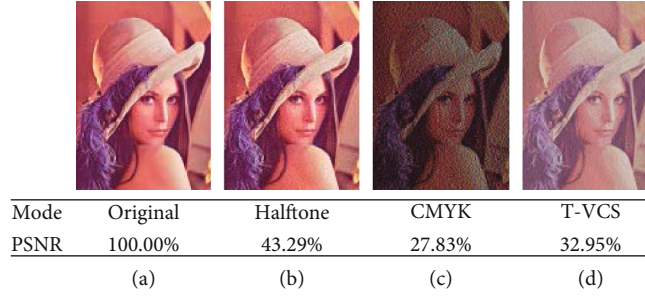


FIGURE 6: Contrast comparison between color VCSs.

Signal-to-Noise Ratio) given in Equation (3) to measure the difference, where  $x(i, j)$  and  $y(i, j)$  are corresponding pixels in the  $i$ th row and  $j$ th column in the secret image  $x$  and the recovered image  $y$ . When the PSNR value is greater than 30, it means that the transparency of the watermark [36] is better. The larger the PSNR value, the better the clarity.

$$\text{PSNR} = 10 \times \log_{10} \left( \frac{\text{MAX}_I^2 \times m \times n}{\sum_{i=0}^{n-1} \sum_{j=0}^{m-1} (x(i, j) - y(i, j))^2} \right). \quad (3)$$

Figure 5 shows a contrast comparison between kinds of halftone VCS. We select the halftone image of Lena (Figure 5(a)) as the reference image. As shown in Figure 5(b), since Hou's scheme takes advantage of image contrast reduction, the recovered image is darker, and its PSNR is the lowest. By limiting selectable matrices to the same space as the original block of pixels, we archive to increase the PSNR from 51.62% to 68.06%. It can be inferred that T-VCS has a higher quality of secret recovery than directly applying the block-wise operation, which generates pixel blocks with a random permutation. Most of VCSs have the property of perfect black. The reconstructed image in T-VCS also is perfect black since stacked blocks associated with black pixels of the secret image are all black.

**3.3. Color T-VCS.** In this section, we propose a nonexpansion VCS for color images based on the above gray-level scheme [37]. We first divide a color image into three color channels: cyan (C), magenta (M), and yellow (Y), since most color printers use C, M, and Y inks to display color. This scheme represents the gray levels of each color channel of the secret image by vectors of 8 bits; that is, the secret image is divided into 8-bit levels and each bit level forms a binary image. For each bit level  $j$  and each color channel  $h$ , we choose a block in the secret image and encrypt it by the query table. For a color image with a bit depth of 8, it is equivalent to repeating the black and white image encryption operation 24 times.

The method has the characteristic of gradual restoration. The more the superimposed share image, the higher the clarity of the restored image. So participants do not need to generate all the shares for all the bit levels. We can recover a clear enough image by selecting the highest number of bits, since the information about a higher bit level is not as important as that of a lower bit level for HVS.

Figure 6 shows the experimental results of the color T-VCS. We calculate the PSNR of color images by summing and averaging each channel's PSNR where the maximum pixel value MAX is 255. Figure 6(a) is the original color image. Due to the fact that digital halftoning is a lossy process in itself, it is impossible to reconstruct the original secret image fully, so the PSNR reduces to 43.29% in Figure 6(b). The PSNR of image recovered from the T-VCS is 32.95% in Figure 6(d), while the PSNR of image recovered from random T-VCS is 27.83% shown in Figure 6(c). It can be inferred that a careful arrangement of pixels in encryption improves the quality of color images.

**3.4. Verify Sheets by SGX.** Despite visual cryptography's secure nature, it would be terrible if participants cannot verify distributed shares. Not only can we use VCS to encrypt images, but we can also verify sheets. But the disadvantage of VCS is that once malicious attackers tamper with authentication information, human vision cannot detect it. We introduce TEE to prevent malicious systems from tampering with the verification data on untrusted remote environments.

The verification process is shown in Figure 7, which briefly includes the distribution phase and verification phase. During the distribution phase, T-VCS first constructs a basis matrices' query table according to the method above and then generates sheet images according to the watermark image [38].

- (A.1) Generate basis matrices. Based on the value of each pixel in the watermark image, the basis matrices are selected randomly from odd parts if the pixel  $pw$  in watermark image ( $W$ ) is white or even parts if  $pw$  is black, respectively. We can generate the watermark image dynamically in the enclave or select from existing images. We then seal the query table to the disk for subsequent verification. The watermark image is the only sensitive data in the T-VCS. Sealing enables encrypting and authenticating the enclave's data such that no process other than the exact enclave can decrypt or modify it. The security of the watermark can also be guaranteed since no secret information will leak out in the enclave.
- (A.2) Generate sheets and serialize them to disk through the *OCALL* instruction of the Intel protected file



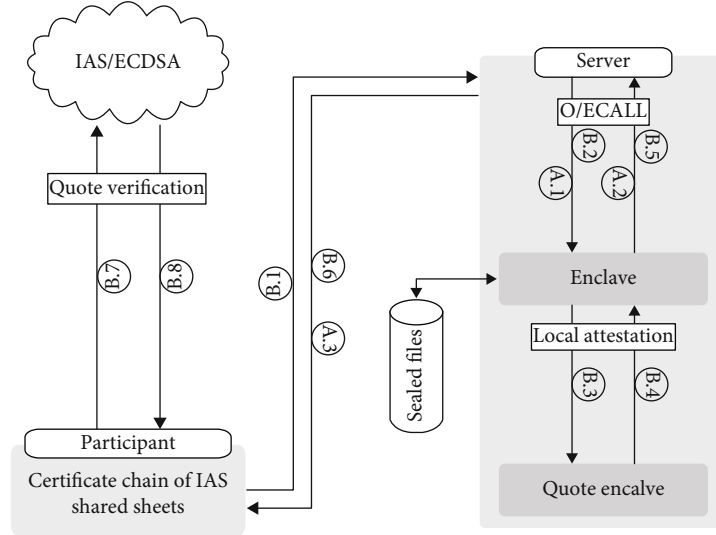


FIGURE 7: Sheet attestation workflow.

system. Isolated execution of an enclave process restricts access to a subset of memory such that only that particular enclave can access it. Entry points defined in trusted code are called *ECALL*. Valid interaction with an enclave is only possible via explicit *ECALL*. Similarly, entry points defined in untrusted code are called *OCALL*, which calls out of the enclave.

#### (A.3) Distribute sheet images to each participant.

During the verification phase, T-VCS acts as a TPP to provide an integrity validation service for participants by hardware attestation. The phase includes the following steps:

- (B.1) The participant  $P$  sends a held sheet and received sheet images to the T-VCS server for verification.
- (B.2) The server transfers the two images which may contain multiple channels to the verification enclave ( $E$ ).  $E$  first reads the pixel value  $p_s$  of the watermark image which is involved with received sheets and then determines whether  $p_s$  is consistent with parts from which the basis matrices are selected. This procedure is repeated until traversing all the pixel values. If all of the pixels match, that is,  $p_{wi} == p_{si}, \forall \{i\} \in \{W\}$ , the verification is passed, otherwise failed.
- (B.3)  $E$  requests the quote enclave ( $Q$ ) to sign the MRr (MRENCLAVE) and verification result and generate the quote report ( $R$ ).  $R$  consists of and attached report data  $R_a$  and enclave data  $R_e$ .  $Q$  first performs local attestation with  $E$ . After passing attestation,  $Q$  signs the hash value of the authentication result ( $a$ ), the requested sheets  $S_{ri}$  and write  $R$  into the report data field, that is,  $R = \text{hash}(a \| S_{ri} \cdots \| S_{rn})$ ; , where  $n$  is the number of sheets. We patch the *key\_exchange* library in SGX SDK to generate a custom report data field.

It is crucial to include a hash of verification information into the report to avoid masquerading attacks, as this binds validation results to this enclave.  $R_e$  contains the enclave measurement/identity (MRENCLAVE), and the signing identity (MRSIGNER) verifies that the enclave contained the expected code/data pages at launch. Although the length of report data is limited in SGX, the quote report can still ensure the authenticity of sheet images and verification results by the hash value  $R$ .

- (B.4) The signature information of  $R$  can only be verified by the IAS, so the participant needs to send the quote report to IAS for authentication. Remote attestation is digital signatures produced by the SGX over the code of enclaves.  $P$  (challenger) can verify it using the manufacturer's public key [39] to ensure that an enclave has been deployed correctly and is running on a trustworthy Intel SGX hardware platform.
- (B.5-8) After receiving the verification report returned by IAS,  $P$  first verifies the report by signature chains and then compares the  $MR_r$  with local stored  $MR_p$ , the image hash of  $S_{ri}$  in the report with the local cache  $S_{li}$ . After verification is passed, the participant can confirm the validation of sheet images.

In the validation procedure, participants and the T-VCS server do not need to establish a trusted channel, which makes the whole process much more secure and user-friendly. Through the Intel remote attestation service, participants can be sure that the specified enclave completes the image sharing and verification operation. Ensuring the integrity of operation is necessary because a malicious OS could drop messages and tamper with data and validation process. We call this CIVCS self-attesting because the enclave attests itself before verifying integrity of sheets. The only situation

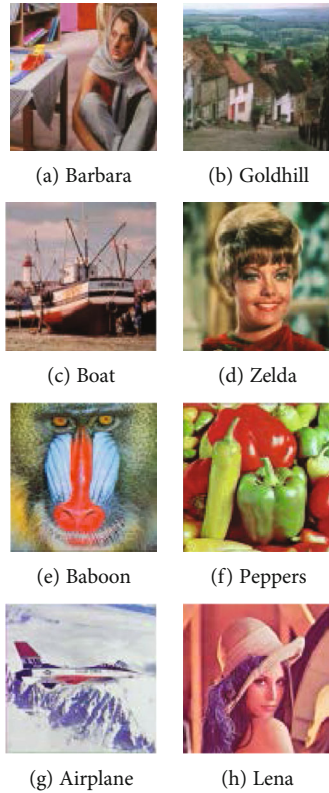


FIGURE 8: Color test images.

TABLE 4: Performance comparison of gray images between Hou and Tu's algorithm and T-VCS.

Images	PSNR (Hou and Tu [18])	PSNR (random T-VCS)	PSNR (T-VCS)
Barbara	51.50%	51.86%	67.86%
Goldhill	51.35%	51.74%	67.17%
Boat	51.63%	51.49%	70.31%
Zelda	52.02%	54.69%	61.70%
Baboon	51.93%	52.06%	63.54%
Peppers	52.12%	51.85%	64.08%
Airplane	53.19%	52.95%	60.45%
Lena	53.37%	53.14%	59.64%

the system ends without being suspended is it runs on a trusted, nondisruptive environment.

#### 4. Evaluation

In this section, we select eight commonly used color images which are shown in Figures 8(a)–8(h), to demonstrate the performance of T-VCS. The size of all the secrets is  $512 \times 512$ . All the data shown below are the average of test results for 100 runs on test images.

*4.1. VCS Evaluation.* To illustrate the encryption and recovery results of the T-VCS on grayscale images, we first convert

TABLE 5: Performance comparison of color images among Hou, Liu et al., and T-VCS.

Images	PSNR (Hou [22])	PSNR (Liu et al. [40])	PSNR (T-VCS)
Barbara	27.78%	27.78%	43.49%
Goldhill	27.82%	27.82%	43.20%
Boat	27.90%	27.91%	41.89%
Zelda	27.83%	27.82%	42.90%
Baboon	27.81%	27.81%	44.76%
Peppers	27.86%	27.85%	44.23%
Airplane	27.44%	27.43%	40.92%
Lena	27.83%	27.84%	42.48%

Figures 8(a)–8(h) into grayscale images and then use halftone technology to binarize images. We use the halftone technology to simulate gray levels by altering the density of the printed dots. In the bright parts of an image, the density is sparse, while in the darker parts of the image, the density is dense. There are many halftoning techniques available, where error diffusion produces superior results and is adopted in this paper.

Table 4 shows a performance comparison of gray images between Hou and Tu's algorithm and T-VCS. Hou and Tu's experimental results [18] are shown in the second column of Table 4. They adjust all of the gray values in the grayscale image to more than 127 by linearly interpolating. After halftone conversion, the number of black subpixels in each block is between 2 and 4. They can obtain the same arrangement by transforming the distribution of black and white subpixels. We, however, find that Hou and Tu's method cannot convert all blocks to the requirements of 2 to 4 black blocks. For the Barbara image, there are 41 abnormal blocks with 3 white and 1 black pixels, which accounts for 0.062% of all the blocks. The PSNR for images recovered from this method is between 51.35% and 53.37%, which is similar to the results of random T-VCS, while the values of PSNR for images recovered from T-VCS are all greater than 59%. Although both schemes can keep the image size, it is obvious that our method can recover images with higher quality.

The PSNRs of recovered color image are shown in Table 5. Using this color decomposition, Hou [22] decomposes every color within the image into three primary colors. This proposal is similar to traditional visual cryptography for the pixel expansion that occurs. The loss of contrast will accumulate because color images use sub-channels or bit-by-bit encryption, generally. So, PSNRs of color images are lower than those of grayscale images. As shown in the second column of Table 5, the PSNRs are all around 27%, which is similar to Liu et al.'s scheme [40]). Based on the black and white schemes, Liu et al. propose a color  $k$ -out-of- $n$  VCS to divide a natural color image into 24 binary images. The values of PSNR for this scheme are shown in the third column of Table 5. Although our method also uses bit-wise encryption for color images, images recovering from our scheme have higher quality, whose PSNRs are all above 40%.

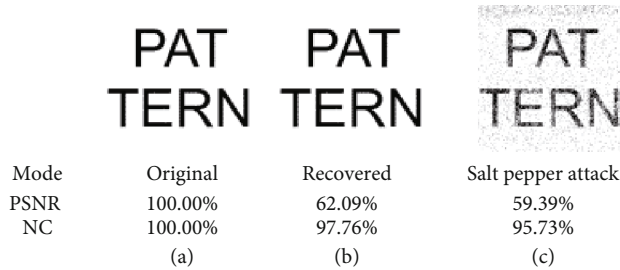


FIGURE 9: Extracted watermarks.

**4.2. Robustness Evaluation.** There are usually two metrics with respect to evaluate watermarking algorithms: imperceptibility and robustness. (i) Imperceptibility means that the presence of the watermark should not distort the perceived quality of the host image. The PSNR is typically used to measure imperceptibility. (ii) Robustness is a measure of the immunity of the watermark against attempts to remove or degrade it. We measured the similarity between the original watermark and the watermark extracted from the attacked image using the NC (normal correlation factor) given in the following equation:

$$NC(w, \hat{w}) = \frac{\sum_{i=1}^N w_i \hat{w}_i}{\sqrt{\sum_{i=1}^N w_i^2} \sqrt{\sum_{i=1}^N \hat{w}_i^2}}, \quad (4)$$

where  $N$  is the number of pixels in the watermark and  $w$  and  $\hat{w}$  are the original and extracted watermarks, respectively. In general, an NC of about 0.75 or above is considered acceptable [41].

We first evaluate the performance of the zero watermarking algorithm in T-VCS using a  $512 \times 512$  Lena image as the original cover host image, and a  $256 \times 256$  black-white image with the expression PATTERN as the watermark image. A pseudorandom number generator generates the secret data used in our experiments. Figure 9 shows PSNR and NC values among the original watermark, the watermarks extracted from T-VCS, and the extracted watermark after being subjected to the salt-pepper attack independently. The value of NC for the extracted watermark is higher than 0.95. We can clearly see the expression value from the watermark. We also verify the performance of watermark extraction on the above eight images. As shown in Table 6, the values of PSNR are above 40%. After applying the attack of salt-pepper, the values of PSNR drop by only 1%, which is within acceptable limits. The values of NC are all above 91%, indicating the algorithm has strong robustness and can resist salt-and-pepper noise.

Experimental results show that the proposed scheme does not suffer from salt-and-pepper noise. Although we can use the Discrete Wavelet Transform- (DWT-)/Discrete Cosine Transform- (DCT-) based digital image watermarking algorithms [42] to wavelet transform the image to obtain a more robust watermark, it will further reduce the image resolution. For two sheets, operations such as wavelet transform and inverse transform will destroy the corresponding

TABLE 6: Robustness illustration of T-VCS.

Images	PSNR	PSNR (salt-pepper)	NC (salt-pepper)
Barbara	43.49%	39.27	95.55%
Goldhill	43.20%	39.19	96.12%
Boat	41.89%	38.71	95.78%
Zelda	42.90%	38.99	91.23%
Baboon	44.76%	39.50	94.70%
Peppers	44.23%	39.21	95.18%
Airplane	40.92%	38.37	93.04%
Lena	42.48%	38.57	95.41%

relationship of pixels, resulting in the restoration of recovered image. Therefore, we apply no transform to preprocess sheets but directly use the way of quantization to odd/even to embed the watermark into lossless sheets.

**4.3. Performance Evaluation of Running T-VCS in TEE.** In this section, we mainly evaluate the performance of online verification sharing when running T-VCS in TEE. The performance of sheet distribution is not our main concern because we can do it online or offline.

There are usually two concerns when using SGX to prevent cheating of VCS: one is the code refactoring [43]. It is not an easy task to port an application to run within an SGX container because Intel has envisioned SGX as a protection technology for only small parts of the application code and data. The native application code often has to be modified to meet the implicit prerequisite. While a fully featured library, OS [44] can rapidly deploy unmodified applications.

To quickly verify the proposed TEE solution in this paper, we first develop a T-VCS prototype system on a native OS by Python and then make use of Graphene-SGX and *ptrace* interposition to run the system in SGX. Another reason behind this is that easy data exploration and visualization are often more important than writing the most optimized solution [33]. We selected the Graphene-SGX as the library OS. It should be noted that although the Graphene-SGX supports running Python, and all dependent files must be specified manually, so it is impractical to run complex Python programs like T-VCS which has 516 lines of Python code. We first make use of *ptrace* interposition to trace system calls invoked by the T-VCS and then extract dependencies into a manifest. The patched Graphene-SGX ensures the integrity of T-VCS in runtime by verifying these manifest files.

All benchmarks are measured on an HP Z240 SFF Workstation with Intel Xeon Intel i7-7700 3.6 GHz processor (with Skylake microarchitecture, 4 cores, and SGX version 1) and 16 GB RAM. We install Intel's SGX Linux Driver and SDK 2.0 on the Ubuntu 18.04.3 LTS.

As shown in Figure 10, the processing time to run T-VCS in SGX is higher than that in native Linux. One of the reasons is that the enclave creation time which an application has to pay to run on SGX is relatively higher. The time is determined by the latency of the hardware and the driver. It is primarily a function of the size of the enclave. As shown in Figure 10(a), with the number of processed images

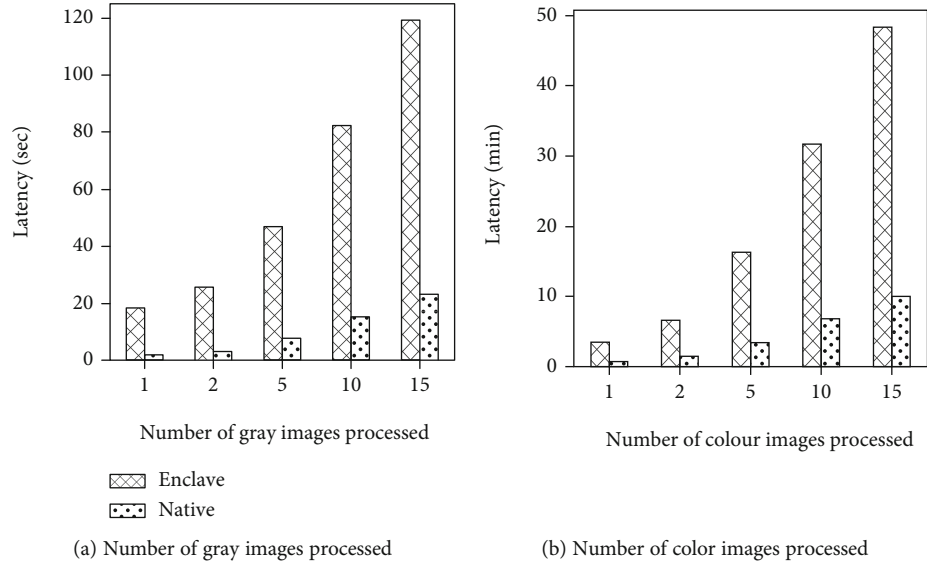


FIGURE 10: Performance overhead to run T-VCS in SGX and native Linux.

TABLE 7: Performance overhead of remote attestation in T-VCS.

Time (sec)	Sigrl	Report	Load enclave	Net	Other
2.5004	1.0274	1.42	0.0105	0.0003	0.0394

increasing, the performance overhead decreases from 11:3x (for one image) to 5:1x (for 15 images). The overload to load enclave and library OS is gradually weakened.

The performance overhead for processing color images is shown in Figure 10(b), which is also about 5x of the native program. The reason why the order of performance overhead rises to the minute is that the color image has three channels, each of which has a bit length of 8. So, it is equivalent to processing 24 black and white images for a color image. However, the SGX and library OS technologies are not friendly to parallel processing. Furthermore, to use the remote attestation feature of SGX, the hyperthreading function, which is vulnerable to side-channel attack, must be disabled in the BIOS, which further limits the parallelism of SGX. So, in the experimental results, the performance overhead of Figure 10(b) is approximately 24x of Figure 10(a).

The overload to verify sheets are as shown in Table 7. It should be noted that in order to achieve a balance between the SGX programming model and the legacy code, the test program only generates a signed verification report. The verification process is still completed in the library OS. The SGX SDK already provides a basic framework for remote attestation. We patched the *key\_exchange* library to add the hash of the sheets to be verified, which ensures this verification is involved with the sheets. It can be seen from Table 7 that the network overload (Sigrl+Report) with the IAS takes up most of the overload (97.88%). The network overload *Net* between the T-VCS and participants is only 0.0003 seconds, which is because the T-VCS and participant programs are on the same host. Compared with the sharing procedure, the overload of the verification code is negligible.

It should be noted that this prototype system does not use optimization techniques and its efficiency needs to be improved. With the development of SGX supported server hardware [45], we can enhance parallel capabilities of T-VCS and launch up a local authentication server to neutralize overload.

## 5. Conclusions

In this paper, we proposed a novel VCS which improves the pixel expansion and contrast properties compared with many of the known results in the literature. By encrypting an image by pixel blocks, we eliminate pixel expansion. We archive higher contrast by elaborately processing the correspondence between a secret image and its sheets. The multiple permutation ways of the same pixel block in T-VCS provides artifice for subsequent zero watermarking verification. The SGX technology used in this paper simplifies the verification model and provides authenticatable verification results even if the software or OS is compromised. The proposed scheme is efficient and straightforward and can be applied to various images, as shown in the experimental results.

Unfortunately, part of the information about the original share images disappears in the recovered secret image in T-VCS. It is hard to eliminate such a phenomenon, but it is possible to find a method to weaken it. Furthermore, in traditional VCSs, each participant only holds a sheet, while the proposed scheme needs each participant to hold multiple sheets, which is inconvenient for management. Reducing the number of sheets will also become our future work.

## Data Availability

The data used to support the findings of this study were supplied by Denghui Zhang under license and so cannot be made freely available. Requests for access to these data should be made to Denghui Zhang (zhang.denghui@foxmail.com).



## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This work is supported in part by the National Key Research and Development Program of China (2019YFB1706003 and 2018YFB1004003), the National Natural Science Foundation of China under Grant 61902082, and the Guangdong Key Research and Development Program of China (2019B010136003).

## References

- [1] Z. He, Z. Cai, J. Yu, X. Wang, Y. Sun, and Y. Li, "Cost-efficient strategies for restraining rumor spreading in mobile social networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2789–2800, 2017.
- [2] X. Wang, L. T. Yang, Y. Wang, L. Ren, and M. J. Deen, "ADTT: a highly efficient distributed tensor-train decomposition method for IIoT big data," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1573–1582, 2021.
- [3] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2018.
- [4] Z. He, Z. Cai, and J. Yu, "Latent-data privacy preserving with customized data utility for social network data," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 665–673, 2018.
- [5] M. Naor and A. Shamir, "Visual cryptography," in *Workshop on the Theory and Application of Cryptographic Techniques*, pp. 1–12, Springer, 1994.
- [6] A. G. Forte, J. A. Garay, T. Jim, and Y. Vahlis, "EyeDecrypt—private inter- actions in plain sight," in *Security and Cryptography for Networks, Lecture Notes in Computer Science*, M. Abdalla and R. Prisco, Eds., pp. 255–276, Springer International Publishing, 2014.
- [7] S. J. Andrabi, M. K. Reiter, and C. Sturton, "Usability of augmented reality for revealing secret messages to users but not their devices," in *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, pp. 89–102, USENIX Association, Ottawa, 2015.
- [8] D. Chaum, "Secret-ballot receipts: true voter-verifiable elections," *IEEE Security Privacy*, vol. 2, no. 1, pp. 38–47, 2004.
- [9] F. Liu, W. Q. Yan, P. Li, and C. Wu, "ESSVCS: an enriched secret sharing visual cryptography," in *Transactions on Data Hiding and Multimedia Security IX: Special Issue on Visual Cryptography, Lecture Notes in Computer Science*, Y. Q. Shi, F. Liu, and W. Yan, Eds., pp. 1–24, Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.
- [10] F. Liu, C. Wu, and X. Lin, "Step construction of visual cryptography schemes," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 27–38, 2010.
- [11] C.-M. Hu and W.-G. Tzeng, "Cheating prevention in visual cryptography," *IEEE Transactions on Image Processing*, vol. 16, no. 1, pp. 36–45, 2006.
- [12] F. Liu, C. Wu, and X. Lin, "Cheating immune visual cryptography scheme," *IET Information Security*, vol. 5, no. 1, pp. 51–59, 2011.
- [13] R. Amankwah, P. K. Kudjo, and S. Y. Antwi, "Evaluation of software vulnerability detection methods and tools: a review," *International Journal of Computers and Applications*, vol. 169, no. 8, pp. 22–27, 2017.
- [14] W. Qiang, Z. Dong, and H. Jin, "Se-Lambda: securing privacy-sensitive server- less applications using SGX enclave," in *Security and Privacy in Communication Networks, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, R. Beyah, B. Chang, Y. Li, and S. Zhu, Eds., pp. 451–470, Springer International Publishing, Cham, 2018.
- [15] A. Ross and A. Othman, "Visual cryptography for biometric privacy," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 70–81, 2011.
- [16] Y.-F. Chen, Y.-K. Chan, C.-C. Huang, M.-H. Tsai, and Y.-P. Chu, "A multiple-level visual secret-sharing scheme without image size expansion," *Information Sciences*, vol. 177, no. 21, pp. 4696–4710, 2007.
- [17] C.-N. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognition Letters*, vol. 25, no. 4, pp. 481–494, 2004.
- [18] Y. Hou and C. Tu, "Visual cryptography techniques for color images without pixel expansion," *Journal of Information, Technology and Society*, vol. 1, pp. 95–110, 2004.
- [19] P. Tuyls, H. D. Hollmann, J. H. Van Lint, and L. Tolhuizen, "XOR-based visual cryptography schemes," *Designs, Codes and Cryptography*, vol. 37, no. 1, pp. 169–186, 2005.
- [20] M. Naor and A. Shamir, "Visual cryptography II: improving the contrast via the cover base," in *Security Protocols, Lecture Notes in Computer Science*, M. Lomas, Ed., pp. 197–202, Springer Berlin Heidelberg, 1997.
- [21] Y.-C. Chen, D.-S. Tsai, and G. Horng, "Visual secret sharing with cheating prevention revisited," *Digital Signal Processing*, vol. 23, no. 5, pp. 1496–1504, 2013.
- [22] Y.-C. Hou, "Visual cryptography for color images," *Pattern Recognition*, vol. 36, no. 7, pp. 1619–1629, 2003.
- [23] C.-N. Yang and C.-S. Lai, "Some new types of visual secret sharing schemes," *National Computer Symposium*, vol. 3, pp. 260–268, 1999.
- [24] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.
- [25] K. A. Küçük, A. Paverd, A. Martin, N. Asokan, A. Simpson, and R. Ankele, "Exploring the use of Intel SGX for secure many-party applications," *Proceedings of the 1st Workshop on System Software for Trusted Execution, SysTEX '16*, , pp. 5:1–5:6, ACM, New York, NY, USA, 2016.
- [26] B. Yang, K. Yang, Y. Qin, Z. Zhang, and D. Feng, "DAA-TZ: an efficient DAA scheme for mobile devices using ARM TrustZone," *IACR Cryptology ePrint Archive*, pp. 209–227, 2015.
- [27] S. Arnautov, B. Trach, F. Gregor et al., "SCONE: secure Linux containers with Intel SGX," in *12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16)*, pp. 689–703, USENIX Association, Savannah, GA, 2016.
- [28] A. Baumann, M. Peinado, and G. Hunt, "Shielding applications from an untrusted cloud with haven," in *11th USENIX Symposium on Operating Systems Design and Implementation (OSDI 14)*, pp. 267–283, USENIX Association, Broom- field, CO, 2014.



- [29] C. C. Tsai, D. E. Porter, and M. Vij, "Graphene-SGX: a practical library OS for unmodified applications on SGX," in *2017 USENIX Annual Technical Conference (USENIX ATC 17)*, pp. 645–658, Santa Clara, CA, 2017.
- [30] F. Schuster, M. Costa, C. Fournet et al., "VC3: trustworthy data analytics in the cloud using SGX," in *2015 IEEE symposium on security and privacy*, pp. 38–54, IEEE, San Jose, CA, 2015.
- [31] F. Tramèr and D. Boneh, "Slalom: fast, verifiable and private execution of neural networks in trusted hardware," in *International Conference on Learning Representations*, New Orleans, LA, USA, 2019.
- [32] Z. Gu, W. Hu, C. Zhang, H. Lu, L. Yin, and L. Wang, "Gradient shielding: towards understanding vulnerability of deep neural networks," *IEEE Transactions on Network Science and Engineering*, 2020.
- [33] F. Shaon, M. Kantarcioglu, Z. Lin, and L. Khan, "SGX-BigMatrix: a practical encrypted data analytic framework with trusted processors," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS '17*, pp. 1211–1228, New York, NY, USA, 2017.
- [34] I. Anati, S. Gueron, S. Johnson, and V. Scarlata, "Innovative technology for CPU based attestation and sealing," *Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy*, , ACM, New York, NY, USA, 2013.
- [35] M. Hoekstra, R. Lal, P. Pappachan, V. Phegade, and J. Del Cuvillo, *Using Innovative Instructions to Create Trustworthy Software Solutions, HASP@ ISCA 11*, 2013.
- [36] Z. Gu, T. Shen, Y. Wang, and F. C. M. Lau, "Efficient rendezvous for heterogeneous interference in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 19, no. 1, pp. 91–105, 2020.
- [37] X. Wang, L. T. Yang, L. Song, H. Wang, L. Ren, and M. J. Deen, "A tensor- based multiattributes visual feature recognition method for industrial intelligence," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 2231–2241, 2021.
- [38] Z. Gu, Y. Wang, T. Shen, and F. C. M. Lau, "On heterogeneous sensing capability for distributed rendezvous in cognitive radio networks," *IEEE Transactions on Mobile Computing*, 2020.
- [39] Z. Cai and Z. He, "Trading private range counting over big IoT data," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 144–153, Dallas, TX, USA, 2019.
- [40] F. Liu, C. K. Wu, and X. J. Lin, "Colour visual cryptography schemes," *IET Information Security*, vol. 4, no. 2, pp. 151–165, 2008.
- [41] A. Al-Haj, "Combined DWT-DCT digital image watermarking," *Journal of Computer Science*, vol. 3, no. 9, pp. 740–746, 2007.
- [42] K. Deb, M. S. Al-Seraj, M. M. Hoque, and M. I. H. Sarkar, "Combined DWT- DCT based digital image watermarking technique for copyright protection," in *2012 7th International Conference on Electrical and Computer Engineering*, pp. 458–461, Dhaka, Bangladesh, 2012.
- [43] J. Lind, C. Priebe, D. Muthukumaran et al., "Glamdring: automatic application partitioning for Intel SGX," in *2017 USENIX Annual Technical Conference (USENIX ATC 17)*, pp. 285–298, Santa Clara, CA, 2017.
- [44] D. E. Porter, S. Boyd-Wickizer, J. Howell, R. Olinsky, and G. C. Hunt, "Rethinking the library OS from the top down," in *ACM SIGARCH Computer Architecture News*, vol. 39, pp. 291–304, ACM, 2011.
- [45] F. McKeen, I. Alexandrovich, I. Anati et al., "Intel software guard extensions (intel sgx) support for dynamic memory management inside an enclave," *Proceedings of the Hardware and Architectural Support for Security and Privacy 2016*, , pp. 1–9, ACM, 2016.

## Research Article

# Certificateless-Based Anonymous Authentication and Aggregate Signature Scheme for Vehicular Ad Hoc Networks

Xin Ye <sup>1</sup>, Gencheng Xu <sup>2</sup>, Xueli Cheng <sup>2</sup>, Yuedi Li <sup>1</sup> and Zhiguang Qin<sup>1</sup>

<sup>1</sup>School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan Province, 610054, China

<sup>2</sup>School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan Province, 611731, China

Correspondence should be addressed to Gencheng Xu; [xugencheng@std.uestc.edu.cn](mailto:xugencheng@std.uestc.edu.cn)

Received 11 December 2020; Revised 18 January 2021; Accepted 11 February 2021; Published 16 March 2021

Academic Editor: Zhuojun Duan

Copyright © 2021 Xin Ye et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Development of Internet of Vehicles (IoV) has aroused extensive attention in recent years. The IoV requires an efficient communication mode when the application scenarios are complicated. To reduce the verifying time and cut the length of signature, certificateless aggregate signature (CL-AS) is used to achieve improved performance in resource-constrained environments like vehicular ad hoc networks (VANETs), which is able to make it effective in environments constrained by bandwidth and storage. However, in the real application scenarios, messages should be kept untamed, unleashed, and authentic. In addition, most of the proposed schemes tend to be easy to attack by signers or malicious entities which can be called coalition attack. In this paper, we present an improved certificateless-based authentication and aggregate signature scheme, which can properly solve the coalition attack. Moreover, the proposed scheme not only uses pseudonyms in communications to prevent vehicles from revealing their identity but also achieves considerable efficiency compared with state-of-the-art work, certificateless signature (CLS), and CL-AS schemes. Furthermore, it demonstrates that when focused on the existential forgery on adaptive chosen message attack and coalition attack, the proposed schemes can be proved secure. Also, we show that our scheme exceeds existing certification schemes in both computing and communication costs.

## 1. Introduction

With the rapid development of communication technology, various vehicles with powerful smart devices can communicate with each other. Therefore, such a novel application has aroused extensive interest in the society. This kind of application is commonly referred to as vehicle ad hoc networks (VANETs), which can provide guarantee for the distance between vehicles and reduce the probability of vehicle collision accidents, help car drivers navigate in real time, and improve the efficiency of traffic operation by communicating with other vehicles and network systems [1].

Although VANETs have a lot of merits, it has a long way to achieve a wide application. One of the obstacles is that the privacy is violated. Without proper privacy protection, malicious adversaries can collect vehicle information, such as routes or status, to perform attacks. Fortunately, using pseu-

donyms in communications can avoid this problem. Then, the vehicle can communicate with each other or with roadside unit (RSU) using a pseudonym, and no one can obtain the true identity of the vehicle except for the trusted authority (TA). Even if the messages between the vehicles and the RSUs are collected by hackers, it will not reveal identity privacy. VANETs have other problems such as privacy issues and being vulnerable to attack.

Recently, some novel schemes and algorithms are proposed to solve these problems. Lin et al. [2] proposed a blockchain-based protocol to reduce the verification cost and storage cost for vehicles. Kumar et al. [3] proposed an efficient scheme using path signature to resist Sybil attack. Jiang et al. [4] proposed an anonymous authentication scheme (AAAS) in VANETs, which adopts group signature mechanism to provide more efficient anonymous authentication service for vehicles. Zheng et al. [5] demonstrated a

certificateless group signature anonymous authentication scheme for VANETs, which shortens the length of the signature and improves the efficiency of the signature. Among various schemes, we find that Kamil et al.'s scheme [6] has a significant efficiency. However, we find that the scheme cannot resist coalition attack which is launched by two collusive vehicles. For example, two vehicles can maliciously exchange their locations to generate their signatures which can be verified successfully so that they can hide their real locations which may lead to serious consequences. The detailed description and analysis are shown in Subsection 4.3. We make the RSU both the aggregator and the verifier and add a random list to properly solve the problem. Our main contributions in this paper are as follows:

- (i) Prove that Kamil et al.'s schemes are not secure enough to defend against attacks from malicious vehicles and propose a solution to settle the problem
- (ii) Propose an improved certificateless-based authentication and aggregate signature scheme in VANETs, and prove that the scheme can perfectly resist the coalition attacks and its correctness
- (iii) Use the efficiency analysis and simulation to show the superiority of our scheme in efficiency and practicality

The rest of this paper is organized as follows. In Section 2, we discuss related works of CLS and CL-AS schemes in VANETs. In Section 3, we describe related concepts and models. In Section 4, we analyze Kamil et al.'s scheme and prove that the scheme cannot resist the coalition attack. We propose our proposed scheme in Section 5 in detail. Experiments and results analysis are described in Section 6. We conclude this paper in Section 7.

## 2. Related Works

To settle the problem of security and some privacy requirements in VANETs, a number of professors and scholars [7–9] proposed a kind of new scheme called Public Key Infrastructure-based (PKI-based) authentication schemes. In their schemes, they either tried to make vehicles compute more to verify the signatures from other vehicles or assume that there exists a trusted certificate authority to issue and maintain certificates of various vehicles. However, the assumption may be unrealistic because a single node cannot afford the oceans of calculation.

Later, a new kind of signature scheme called identity-based signature (IBS) scheme is widely discussed. For example, Liu et al. [10] proposed an IBS scheme which can take the user's identity as the public key, and the private key is generated by public key generation PKG, which can reduce a single node's burden. However, IBS has inherent problems about key escrow which is generated by user's identity.

In Al-Riyami and Paterson's scheme [11], they firstly introduce the certificateless public key cryptography. In recent years, a lot of researches on CLS and CL-AS schemes with bilinear pairing have been carried on by relevant

researchers [12–14]. In their schemes, key generation center (KGC) uses its master key and the user's identity information to calculate a part of the private key and send it to the user, whereafter the user combines part of the private key and his/her secret value together to generate the user's real private key which can protect the user's privacy and make the system secure. The above scheme uses the bilinear pairing which costs relatively large computation.

The elliptic curve cryptography is chosen to use in the CLS and CL-AS because of its high efficiency. In Xie et al.'s scheme [15], they proposed rigorous security proof that shows the scheme is able to resist various malicious attacks and ensure privacy protection. In the field of health care, Du et al. [16] proposed a CLAS scheme with high efficiency and low latency which can be more suitable to apply to the field of healthcare. In 2018, Cui et al. [17] demonstrated their novel CLS and CL-AS scheme with ECC, which significantly reduces computing time during sign and verification process. Kamil et al. [6] declared that the scheme proposed by Cui et al. is not secured against the signature forgery attack, and they advanced an improved signature scheme for VANETs. They claimed that their proposed scheme can address all the needs of VANETs about security and privacy. However, we will demonstrate and prove that their scheme cannot resist coalition attacks and our improved scheme can resist the attack and achieves a better performance.

## 3. Preliminaries

*3.1. Elliptic Curve Cryptography.* As widely used in the cryptographic, the elliptic curve cryptography is an excellent algorithm which has an extremely high efficiency and a relatively excellent security. It can use much fewer bits to encrypt messages of the same length than the RSA algorithm in the field of public key cryptography. Because of its fewer calculation parameters, shorter bond length, and less time cost, the elliptic curve cryptography can be perfectly applied to application scenarios of VANETs. We will give the following three definitions to describe the elliptic curve cryptography.

*Definition 1* (Elliptic curve definition). Our scheme uses an elliptical encryption algorithm with 160 bits. Assume that  $F_q$  is a finite field of the module  $q$ , where  $q$  is a large prime number. The elliptic curve over a finite field  $F_q$  can be defined as follows:  $E : y^2 = x^3 + ax + b \pmod{p}$ , where  $a, b, x, y \in F_q$  and  $\Delta = 4a^3 + 27b^2 \neq 0 \pmod{p}$ .

*Definition 2* (Addition of elliptic curves). Assume that  $P = (x_1, y_1) \in E$ , where  $P$  is a point of the elliptic curve  $E$  and  $-P = (x_1, -y_1) \pmod{p}$  is the negative point of  $P$ . Suppose  $Q = (x_2, y_2) \in E$ ,  $Q \neq -P$ ; we can define a line  $l$  passes through  $P$  and  $Q$ , and intersects the elliptic curve at a point  $R' = (x_3, y_3)$ . The symmetrical point about the  $x$ -axis with  $R'$  is  $R = (x_3, -y_3)$ ; then we can define  $R = P + Q$ . In addition, scalar multiplication operation on the elliptic curve can be

described as follows:

$$k \cdot P = P + P + P + \dots + P \quad (k \in Z_q^*). \quad (1)$$

*Definition 3* (Elliptic curve discrete logarithm problem). Assume that  $P_1$  is a point on the elliptic curve  $E$  on the finite field  $F_q$ , and select a random number  $k \in Z_q^*$ . Then, we can calculate  $P_2 = k \cdot P_1$ . In this case, there is the feasibility of the calculation of  $P_2$  according to Definition 2. According to the elliptic curve discrete logarithm problem (ECDLP), however, it is hardly possible to get  $k$  according the above equation.

### 3.2. Forking Lemma

*Definition 4* (Forking lemma [18]). Suppose that  $A$  is a probabilistic polynomial time turing machine, and its input includes public data. We use  $Q$  and  $R$  to symbolize the number of queries that  $A$  can ask to the random oracle and the number of queries that  $A$  can ask to the signer, respectively. Suppose that over a period of time  $T$ ,  $A$  can generate a legitimate signature  $(m, \sigma_1, h, \sigma_2)$  within probability  $\varepsilon \geq 10(R + 1)(R + Q)/2^k$ . If someone do not know the private key, but successfully forge the signature  $(\sigma_1, h, \sigma_2)$  with an indistinguishable distribution probability, then we can imagine a machine, which can get the secret information from the machine and obtain and replace the interaction with the signer by simulation. Eventually, it can generate two legitimate signatures  $(m, \sigma_1, h, \sigma_2)$  and  $(m, \sigma_1, h', \sigma_2')$  such that  $h \neq h'$  in expected time  $T' \geq 120686QT/\varepsilon$ .

*3.3. Certificateless (Aggregate) Signature Scheme.* Generally, a certificateless signature (CLS) scheme and a certificateless aggregate signature (CL-AS) scheme consist of the following seven algorithms.

- (1) *Setup*: the KGC and TA will execute this probabilistic algorithm, which needs a security parameter  $\lambda$ , then generates an elliptic curve  $E$ , public keys  $PK_{TA}$  and  $PK_{KGC}$ , and master secrets key  $\alpha, \beta$ , respectively, then publishes a number of system parameters which is used for ensuring the system in order.
- (2) *ParitalPrivateKeyGeneration*: in this algorithm, firstly, the entity  $V_i$  transmits a tuple which includes its real identity and partial pseudo identity to TA. Then TA sends a whole pseudo identity to KGC with calculation. Eventually, KGC transmits the partial private key to entity  $V_i$  in a secure channel.
- (3) *VehicleKeyGeneration*: the entity  $V_i$  selects random  $\rho_i \in Z_q^*$  as its secret key and calculates its public key  $PK_{V_i}$ .
- (4) *IndividualSign*: this algorithm is used by each entity  $V_i$ ; after generating a message  $m_i$ , the entity  $V_i$  tries to calculate a set of variables. Then it sends the signature  $\sigma$  to the verifier.

- (5) *IndividualVerify*: this algorithm is executed by the verifier such as RSU. When receiving input including signature  $\sigma$ , pseudo identity  $PID_i$  and current time  $T_{cur}$ , the RSU will check the time validity firstly. Then the algorithm will output true if the signature is valid or false otherwise.
- (6) *AggregateSign*: in this algorithm, generally the aggregate signature generator is RSU in our system. For an aggregating set  $V$  of  $n$  entities  $V_1, V_2, \dots, V_n$ , the pseudo identity  $PID_i$  of each vehicle  $V_i$  as list  $PID$ , the corresponding public key  $PK_{V_i}$  of  $V_i$ , and message signature tuples  $((m_1, \sigma_1), (m_2, \sigma_2), \dots, (m_n, \sigma_n))$  from  $V_i$ , respectively. The aggregate signature generator will generate signature  $\sigma$ ; then it will transmit the tuple including the signature, the list  $PID$ , and time list  $T$  to the verifier.
- (7) *AggregateVerify*: in general, this algorithm is executed by another RSU. It takes an aggregating set  $V$  of  $n$  entities  $\{V_1, V_2, \dots, V_n\}$ , the pseudo identity  $PID_i$  of each entity  $V_i$ . The verifier will check the time validity for each entity firstly. Then it will output true if the signature is valid or false otherwise.

*3.4. Security Model.* In this section, we will demonstrate the security model of CLS and CL-AS schemes. We consider two different types of adversaries: Type 1  $\mathcal{A}_1$  and Type 2  $\mathcal{A}_2$ . To be specific, adversary  $\mathcal{A}_1$  is able to replace a user's public key or private key but cannot access or even replace the master secret key of KGC. And adversary  $\mathcal{A}_2$  is able to access the master secret key of KGC, which can be called an internal attacker. However, it cannot replace or access the public key of a certain user.

Generally, we use two games to model the security of CLS and CL-AS schemes, which is played between an adversary  $\mathcal{A} \in \{\mathcal{A}_1, \mathcal{A}_2\}$  and a challenger  $\mathcal{C}$ .  $\mathcal{A}$  can access five oracles to get what he needs. The details are as follows:

- (1) *GenerateUser*: given a user's ID  $PID_i$  and request for its public key  $PK_{V_i}$ ,  $\mathcal{C}$  returns the public key  $PK_{V_i}$  of  $PID_i$ .
- (2) *RevealPartialPrivateKey*: given a user's pseudo identity  $PID_i$ ,  $\mathcal{C}$  outputs the corresponding partial secret key  $PPK_i$ .
- (3) *RevealSecretKey*: given a user's pseudo identity  $PID_i$ ,  $\mathcal{C}$  submits the user's secret key  $\rho_i$ .
- (4) *ReplaceKey*: given a user's pseudo identity  $PID_i$  and the public key  $PK_{V_i}^*$ ,  $\mathcal{C}$  will replace the public key  $PK_{V_i}$  with  $PK_{V_i}^*$ .
- (5) *Sign*: given a message  $m_i \in \{0, 1\}^*$ ,  $\mathcal{C}$  uses the algorithm to generate a signature  $\sigma_i$  corresponding to user  $PID_i$  on message  $m_i$  and submits it to  $\mathcal{A}$ .

We construct the following two games, Game I and Game II, for our schemes:



(Game I) A Type 1 adversary  $\mathcal{A}_1$  and a challenger  $\mathcal{C}$  will try to play the game as follows:

*Step 1.*  $\mathcal{C}$  runs the Setup algorithm to generate a master secret key  $\beta$ , a list of system parameters, and the system public key  $PK_{KGC}$ . It then sends the system parameters to  $\mathcal{A}_1$  and keeps  $\beta$  secret.

*Step 2.*  $\mathcal{A}_1$  queries the GenerateUser, RevealPartialSecretKey, RevealSecretKey, and Sign oracles in order.

*Step 3.*  $\mathcal{A}_1$  generates the corresponding public key  $PK_{V_i}^*$  and a signature  $\sigma_i^*$  of a user with identity  $PID_i^*$ .

$\mathcal{A}_1$  will win the game if the following conditions are met:

- (i) It neither uses  $PID_i^*$  to access the RevealPartialSecretKey query nor obtains the partial private key
- (ii)  $\sigma^*$  is a valid signature of the user with the identity  $PID_i^*$  and the corresponding public key  $PK_{V_i}^*$
- (iii) It never uses  $(PID_i^*, m_i^*)$  to query the Sign oracle

(Game II) A Type 2 adversary  $\mathcal{A}_2$  and a challenger  $\mathcal{C}$  will try to play the game as follows:

*Step 1.*  $\mathcal{C}$  runs the Setup algorithm to generate a master secret key  $\beta$ , a list of system parameters, and the system public key  $PK_{TA}$ . It then sends the system parameters,  $\beta$ , and  $PK_{TA}$  to  $\mathcal{A}_2$ .

*Step 2.*  $\mathcal{A}_2$  queries the GenerateUser, RevealPartialSecretKey, RevealSecretKey, and Sign oracles in order.

*Step 3.*  $\mathcal{A}_2$  generates the corresponding public key  $PK_{V_i}^*$  and a signature  $\sigma_i^*$  of a user with identity  $PID_i^*$ .

$\mathcal{A}_2$  will win the game if the following conditions are satisfied:

- (i) It never use  $PID_i^*$  to access the RevealSecretKey or ReplaceKey query to obtain the partial private key
- (ii)  $\sigma^*$  is a valid signature of user with identity  $PID_i^*$  and the corresponding public key  $PK_{V_i}^*$
- (iii) It never uses  $(PID_i^*, m_i^*)$  to query the Sign oracle

*Definition 5.* The CLS scheme is provably secure, if neither polynomial time adversary  $\mathcal{A}_1$  or  $\mathcal{A}_2$  is able to win Game I and Game II, respectively with a non-negligible advantage.

We construct the following two games, Game III and Game IV, for our CL-AS scheme.

(Game III) A Type 1 adversary  $\mathcal{A}_1$  and a challenger  $\mathcal{C}$  will try to play the game as follows:

*Step 1.*  $\mathcal{C}$  runs the Setup algorithm to generate the master secret key  $\beta$ , system parameter, and the system public key  $PK_{TA}$ . It then sends the system parameter to  $\mathcal{A}_1$  and keeps  $\beta$  secret.

*Step 2.*  $\mathcal{A}_1$  queries the GenerateUser, RevealPartialSecretKey, RevealSecretKey, and Sign oracles in order.

*Step 3.*  $\mathcal{A}_1$  outputs an aggregate signature  $\sigma^*$  of  $n$  users with identity  $PID^* = \{PID_1^*, PID_2^*, \dots, PID_n^*\}$  and the corresponding public key  $PK_V^* = \{PK_{V_1}^*, PK_{V_2}^*, \dots, PK_{V_n}^*\}$  on messages  $m^* = \{m_1^*, m_2^*, \dots, m_n^*\}$ .

$\mathcal{A}_1$  wins the game if the following conditions are satisfied:

- (i) At least one of the identities has not been submitted to the RevealPartialSecretKey query to obtain the partial secret key
- (ii)  $\sigma^*$  is a valid signature on  $n$  messages  $M^* = \{m_1^*, m_2^*, \dots, m_n^*\}$  of  $n$  users with identities  $PID^* = \{PID_1^*, PID_2^*, \dots, PID_n^*\}$  and the corresponding public key  $PK_V^* = \{PK_{V_1}^*, PK_{V_2}^*, \dots, PK_{V_n}^*\}$ .
- (iii) It never uses  $(PID_i^*, m_i^*)$  to query the Sign oracle

(Game IV) A Type 2 adversary  $\mathcal{A}_2$  and a challenger  $\mathcal{C}$  will try to play the game as follows:

*Step 1.*  $\mathcal{C}$  runs the Setup algorithm to generate the master secret key  $\beta$ , system parameter, and the system public key  $PK_{TA}$ . It then sends the system parameter,  $\beta$ ,  $PK_{TA}$  to  $\mathcal{A}_2$ .

*Step 2.*  $\mathcal{A}_2$  queries the GenerateUser, RevealPartialSecretKey, RevealSecretKey, and Sign oracles in order.

*Step 3.*  $\mathcal{A}_2$  outputs an aggregate signature  $\sigma^*$  of  $n$  users with identity  $ID^* = \{ID_1^*, ID_2^*, \dots, ID_n^*\}$  and the corresponding public key  $PK_V^* = \{PK_{V_1}^*, PK_{V_2}^*, \dots, PK_{V_n}^*\}$  on messages  $M^* = \{m_1^*, m_2^*, \dots, m_n^*\}$ .

$\mathcal{A}_2$  will win the game if the following conditions are satisfied:

- (i) It has not used all of the identities to access the RevealPartialSecretKey query to obtain the partial private key.
- (ii)  $\sigma^*$  is a legitimate signature on  $n$  messages  $m^* = \{m_1^*, m_2^*, \dots, m_n^*\}$  of  $n$  users with identities  $PID^* = \{PID_1^*, PID_2^*, \dots, PID_n^*\}$  and the corresponding public key  $PK_V^* = \{PK_{V_1}^*, PK_{V_2}^*, \dots, PK_{V_n}^*\}$ .
- (iii) It never uses  $(ID_i^*, m_i^*)$  to query the Sign oracle



*Definition 6.* The CL-AS scheme is provably secure, if neither polynomial time adversary  $\mathcal{A}_1$  or  $\mathcal{A}_2$  is able to win Game III and Game IV, respectively, with a nonnegligible advantage.

#### 4. Overview of Kamil et al.'s CLS and CL-AS Scheme

In the scheme proposed by Kamil et al. [6], there mainly exist four entities including TA, regional transport management authority (RTMA), which is a trusted party responsible for partial secret key generation, RSU, and vehicle. The scheme is reviewed as follows:

##### 4.1. Overview of Kamil et al.'s CLS Scheme

- (1) Setup: the TA selects a security parameter  $k$ , two secure primes  $p$  and  $q$ , an elliptic curve  $E$  which can be defined by the equation  $y^2 = x^3 + ax + b \pmod{p}$ , where  $a, b \in F_q$ , a generator  $P$  with order  $q$  of additive group  $G$  consisting of all the points on  $E$ , and five hash functions,  $h_0, h_1, h_2, h_3$ , and  $h_4$ . Then, it picks  $x \in \mathbb{Z}_q^*$  as its master secret key and calculates its public key  $P_{\text{pub}}$ . Also, TA defines a time-function  $f(t_i)$ , where  $t_i$  is the current time. TA publishes the param =  $\{p, q, a, b, P, P_{\text{pub}}, h_0, h_1, h_2, h_3, h_4, f(t_i)\}$ .
- (2) UserRegistration: the RTMA executes the following algorithm to register a vehicle with an identity  $ID_k$ . Firstly, vehicle sends its identity  $ID_k$  to the RTMA. Then RTMA randomly selects  $\tilde{h}_{1,k} \in \mathbb{Z}_q^*$  and calculates hash chain set  $\tilde{h}_{y,k} = \{\tilde{h}_{2,k}, \tilde{h}_{3,k}, \dots, \tilde{h}_{n,k}\}$ ,  $1 \leq y \leq n$ , where  $\tilde{h}_{y,k} = h_0(\tilde{h}_{y-1,k})$ .
- (3) PartialSecretKeyGeneration: after receiving param and a vehicle with identity  $ID_k$ , RTMA runs as follows:
- (4) PseudonymGeneration: after receiving the tuple  $(\tilde{h}_{y,k}, (A_k, x_k))$  from the RTMA, the vehicle executes the following algorithm:
- (5) UserKeyGeneration: vehicle with  $ID_k$  uses the algorithm to generate its private key:
- (6) Sign: after receiving param,  $PSK_k$ ,  $SK_k$ , and  $PK_k$ , a vehicle with pseudo identity  $PID_{y,k}$  can sign on a message  $m_k$  as follows:
- (7) Verify: after receiving the tuple  $(PID_{y,k}, m_k, PK_k, \omega_k, \sigma_k, T_k)$ , verifier can use the algorithm to verify any signature with following steps:

*Step 1.* The RTMA generates its public key  $PK_{\text{RTMA}} = s \cdot P$ , where secret key  $s \in \mathbb{Z}_q^*$  is randomly selected.

*Step 2.* Calculate  $\alpha_k = h_2(\text{param} \| P_{\text{pub}} \| ID_k)$ ,  $\beta_k = h_2(ID_k \| ID_{\text{RTMA}} \| s \| \nabla)$ ,  $t = h_2(\nabla)$ , and  $\xi_k = h_2(ID_k \| PK_{\text{RTMA}})$ .

*Step 3.* Compute  $A_k = t\beta_k \cdot P$  and  $x_k = t\beta_k + \xi_k\alpha_k s$ .

*Step 4.* Publish  $PK_{\text{RTMA}}$ , send  $(PSK_k = (A_k, x_k), \tilde{h}_{y,k})$  to the vehicle and  $(\tilde{h}_{1,k}, ID_k)$  to TA.

*Step 1.* Compute  $\alpha_k = h_2(\text{param} \| P_{\text{pub}} \| ID_k)$ ,  $t = h_2(\nabla)$  and  $\xi_k = h_2(ID_k \| PK_{\text{RTMA}})$ .

*Step 2.* Check  $PSK_k$  is valid or not with the equation holds.

$$x_k \cdot P = A_k + \xi_k \alpha_k \cdot PK_{\text{RTMA}}. \quad (2)$$

*Step 3.* Compute its pseudonym set as  $\{PID_{1,k}, PID_{2,k}, \dots, PID_{n,k}\}$  at timeslot  $ts_{\text{cur}}$ , where  $PID_{y,k} = h_1(ID_k \| \tilde{h}_{y,k} \| \nabla \| ts_{\text{cur}})$ .

*Step 1.* Choose  $a_k, r_k^1, r_k^2 \in \mathbb{Z}_q^*$  in random.

*Step 2.* Calculate  $SK_k^1 = h_3(r_k^1 \| A_k \| PID_{y,k})$  and  $SK_k^2 = h_3(r_k^2 \| x_k \| PID_{y,k})$ .

*Step 3.* Output  $SK_k = a_k(SK_k^1 + SK_k^2)$  and  $PK_k = SK_k \cdot P$  as its private and public keys, respectively.

*Step 1.* Randomly pick  $d_k \in \mathbb{Z}_q^*$  and calculate  $\omega_k = \xi_k \alpha_k$ .

*Step 2.* Calculate  $v_k = h_4(PID_{y,k} \| m_k \| SK_k^1 \| SK_k^2 \| T_k)$ ,  $h_k = h_4(PID_{y,k} \| m_k \| \omega_k \| PK_k \| PK_{\text{RTMA}} \| P_{\text{pub}} \| T_k)$ , and  $\delta_k = h_4(m_k \| PK_k \| \nabla \| T_k)$ .

*Step 3.* Calculate  $y_k = d_k v_k$ ,  $\Omega_k = y_k \cdot P$ ,  $R_k = \delta_k \cdot PK_k + h_k \cdot A_k + \Omega_k$ , and  $\mathcal{V}_k = \delta_k SK_k + h_k x_k + d_k v_k$ .

*Step 4.* Output signature  $\sigma_k = (R_k, \mathcal{V}_k)$  on message  $m_k$  and transmits  $(PID_{y,k}, m_k, PK_k, \omega_k, \sigma_k, T_k)$ , where  $T_k$  is the current timestamp.

*Step 1.* Check whether the time delay equation holds. If it holds, then  $T_k$  is valid and it will accept the signature; otherwise, it will reject it.

*Step 2.* Calculate  $h_k = h_4(PID_{y,k} \| m_k \| \omega_k \| PK_k \| PK_{\text{RTMA}} \| P_{\text{pub}} \| T_k)$ .

*Step 3.* Check whether the following equation holds.

$$\mathcal{V}_k \cdot P = R_k + h_k \omega_k \cdot PK_{\text{RTMA}}, \quad (3)$$

if this equation holds, then the signature is valid; otherwise, it will be discarded.

4.2. *Overview of Kamil et al.'s CL-AS Scheme.* The Setup, UserRegistration, PartialPrivateKeyGeneration, Pseudonym-Generation, VehicleKeyGeneration, Sign, and Verify algorithms are the same as the above CLS scheme. In addition, the Aggregate and AggregateVerify algorithms are described as follows:

- (1) **Aggregate:** in general, the roadside unit (RSU) acts as the aggregator. When receiving  $n$  certificateless signatures  $\{\sigma_1 = (R_1, \mathcal{V}_1), \sigma_2 = (R_2, \mathcal{V}_2), \dots, \sigma_n = (R_n, \mathcal{V}_n)\}$  on messages  $\{(m_1 \| T_1), (m_2 \| T_2), \dots, (m_n \| T_n)\}$  from  $n$  pseudo identities  $\{PID_{y,1}, PID_{y,2}, \dots, PID_{y,n}\}$  under the state information  $\nabla$ , the RSU calculates  $\mathcal{V} = \sum_{k=1}^n \boxtimes \mathcal{V}_k$  and  $R = \sum_{k=1}^n \boxtimes R_k$ , then outputs an aggregate certificateless signature  $\sigma_T = (R, \mathcal{V})$ .
- (2) **AggregateVerify:** generally another RSU or AS acts as the verifier. When receiving a certificateless aggregate signature  $\sigma_T = (R, \mathcal{V})$  signed by  $n$  vehicles. Then it will run as follows:

*Step 1.* Check whether the timestamp  $T_k$  is valid, if not, it aborts, and if it holds, it runs the following steps.

*Step 2.* Compute  $h_k = h_4(PID_{y,k} \| m_k \| \omega_k \| PK_k \| PK_{RTMA} \| P_{pub} \| T_k)$ .

*Step 3.* Check whether the following equation holds.

$$\mathcal{V} \cdot P = R + \sum_{k=1}^n h_k \omega_k \cdot PK_{RTMA}, \quad (4)$$

if it holds, it receives all the signatures; otherwise, the signature is rejected.

4.3. *Cryptanalysis of Kamil et al.'s CL-AS Scheme.* The security problem in the scheme proposed by Kamil et al. [6] mainly lies in the coalition attack, which is a kind of attack by a number of collusive vehicles.

As is described in Figure 1, in the coalition attack, two or more vehicles secretly change a part of their messages such as locations to hide their real locations and routes since the RSU (verifier) receives the exchanged signature. Then something of the collusive vehicles is exchanged officially. Which will definitely harm the system and even worse cause a serious accident.

We describe the coalition attack on Kamil et al.'s CL-AS scheme to illustrate its security flaws.

Assume that two users  $\{U_1, U_2\}$  have pseudonym  $\{PID_{y,1}, PID_{y,2}\}$  and message  $\{m_1, m_2\}$ , respectively. We show that two users can cooperate to generate valid aggregate signatures even if their individual signature is invalid. Two users can implement the coalition attack by executing the following algorithms.

*Step 1.* The user  $U_i$  ( $i \in \{1, 2\}$ ) randomly picks  $d_i \in \mathbb{Z}_q^*$  and calculates  $\omega_i = \xi_i \alpha_i$ .

*Step 2.* Calculate  $\beta_i = h_2(ID_i \| ID_{RTMA} \| s \| \nabla)$ ,  $t = h_2(\nabla)$ ,  $\xi_k = h_2(ID_i \| PK_{RTMA})$ ,  $x_i = t\beta_i + \xi_i \alpha_i s$ ,  $v_i = h_4(PID_{y,i} \| m_i \| SK_i^1 \| SK_i^2 \| T_i)$ ,  $h_i = h_4(PID_{y,i} \| m_i \| \omega_i \| PK_i \| PK_{RTMA} \| P_{pub} \| T_i)$ ,  $\delta_i = h_4(m_i \| PK_i \| \nabla \| T_i)$ ,  $y_i = d_i v_i$ ,  $\Omega = y_i \cdot P$ , and  $R_i = \delta_i \cdot PK_i + h_i \cdot A_i + \Omega$ .

*Step 3.* Then,  $U_1$  sends  $h_1 x_1$  to  $U_2$ ; likewise,  $U_2$  sends  $h_2 x_2$  to  $U_1$  in a secure channel. Then  $U_1$  calculates  $\mathcal{V}_1 = \delta_1 SK_1 + h_2 x_2 + d_1 v_1$ ; likewise,  $U_2$  calculates  $\mathcal{V}_2 = \delta_2 SK_2 + h_1 x_1 + d_2 v_2$ .

*Step 4.* Eventually, they can output signature  $\sigma_i = (R_i, \mathcal{V}_i)$  and transmits  $(PID_{y,i}, m_i, PK_i, \omega_i, \sigma_i, T_i)$ .

$$\begin{aligned} \mathcal{V} \cdot P &= (\mathcal{V}_1 + \mathcal{V}_2) \cdot P = (\delta_1 SK_1 + h_2 x_2 + d_1 v_1 \\ &\quad + \delta_2 SK_2 + h_1 x_1 + d_2 v_2) \\ &\cdot P = \left( \sum_{k=1}^2 [\delta_k SK_k + h_k (t\beta_k + \xi_k \alpha_k s) + d_k v_k] \right) \\ &\cdot P = \left( \sum_{k=1}^2 \delta_k \cdot PK_k + h_k \cdot A_k + \omega_k \right) \\ &\quad + \left( \sum_{k=1}^2 h_k \omega_k \cdot PK_{RTMA} \right) = R + \left( \sum_{k=1}^2 h_k \omega_k \cdot PK_{RTMA} \right) \end{aligned} \quad (5)$$

Obviously, the signature  $\sigma_i = (R_i, \mathcal{V}_i)$  is not a valid signature. However, when the RSU or AS aggregates the signature as  $\sigma = (R = R_1 + R_2, \mathcal{V} = \mathcal{V}_1 + \mathcal{V}_2)$ , it will be a valid signature which satisfies the following equation.

Therefore, the above analysis shows that two malicious users can collude with each other to forge an aggregate signature. Actually, the coalition attack is originally caused by commutative law of addition. Similarly,  $n$  users can also forge an aggregate signature with the same algorithms. Hence, Kamil et al.'s CL-AS scheme cannot resist coalition attacks.

## 5. Our Proposed CLS and CL-AS Schemes

5.1. *System Model.* In this section, we will try to describe our system model in detail including specific explanations. In order to be more specific, the system model is shown in Figure 2. There are four participants in total: trusted authority (TA), key generation center (KGC), road-side unit (RSU), and vehicle, which can be divided into two layers: the upper layer includes TA and KGC, and the lower layer consists of RSUs and vehicles. The demonstration of each participant is as follows:

- (1) **TA:** it is a fully trusted third party that is responsible for system initialization, user registration, system parameter generation, and system security implementation. If necessary, it can track malicious behavior and catch malicious nodes. In addition, it also has enough computing power and storage capacity.

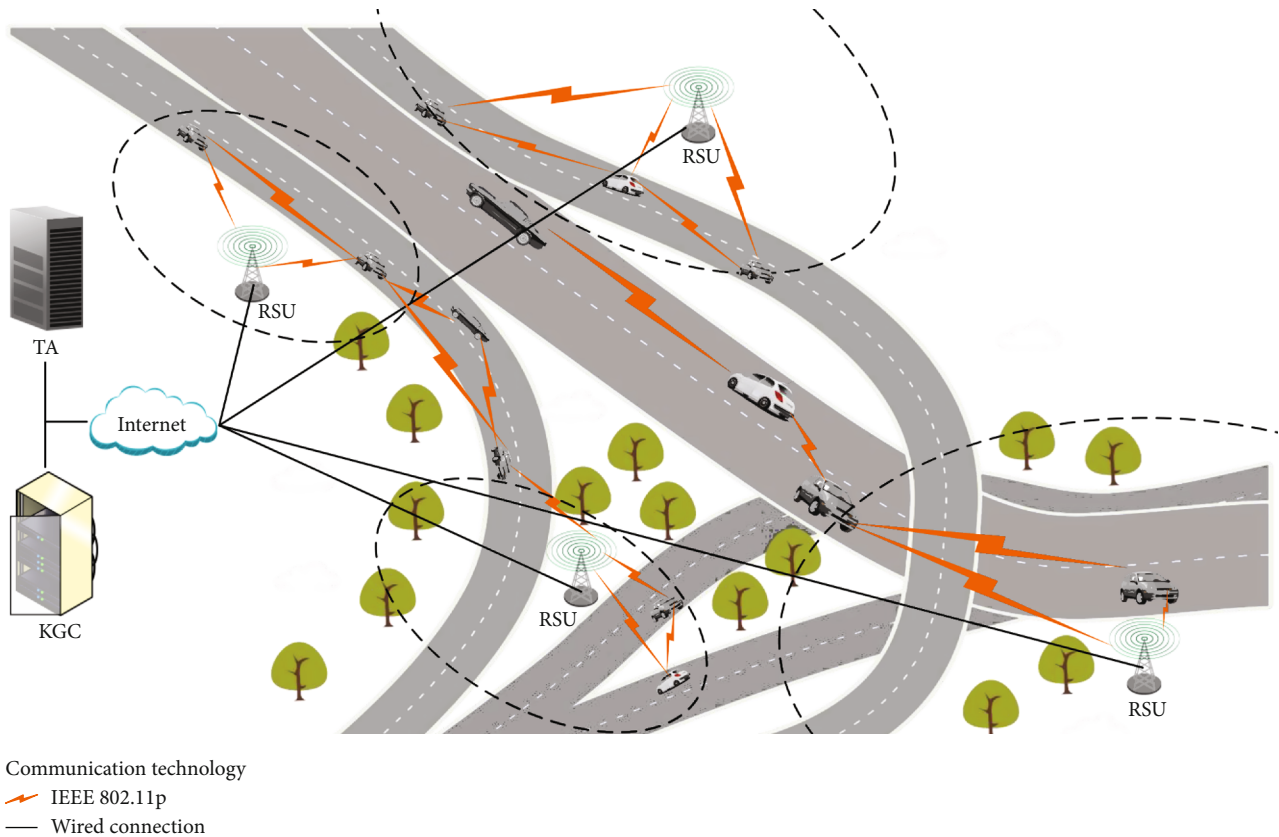


FIGURE 1: Coalition attack diagram.

- (2) KGC: it is a partially trusted party used for generating partial private key. It can help a vehicle generate partial secret key which contribute to its privacy security. Like the TA, it also has sufficient memory, processing, and computing capabilities.
- (3) RSU: it is a smart application device installed in the roadside, which is able to transmit and submit information to TA, KGC, vehicles, or other RSUs in a secure wired connection. In addition, RSU commonly has limited computing power and storage capacity.
- (4) Vehicle: it is the major and basic member in VANETs, which is generally equipped with a smart device which can perform the basic function such as transmitting the vehicle's message and performing simple calculation. In addition, vehicle commonly has limited computing power and storage capacity.

Note that TA and KGC are functionally two completely different entities that can be deployed on a single server during deployment.

**5.2. Design Requirements.** For the safety of communication in VANETs, security and privacy are crucial. According to the latest research in this field, the proposed scheme

for VANETs must satisfy the following security requirements:

- (1) Message Integrity and Authentication: an eligible vehicle should be able to check that whether a message is sent and signed by a legitimate vehicle and is not forged or modified by the malicious entity.
- (2) Identity Privacy Preservation: a vehicle should remain anonymous in all circumstances, which means that other malicious entities cannot infer its identity by taking and analyzing multiple pieces of messages about it.
- (3) Traceability: the TA must have the ability to trace and obtain the vehicle's real identity, even if the vehicle's identity is anonymous.
- (4) Unlinkability: a potentially malicious vehicle must not cross-link two messages sent by the same vehicle to prevent them from extrapolating the route of the vehicle from the information.
- (5) Resistance to Attacks: a reasonable scheme should have the ability to withstand various general attacks such as the coalition attack, the impersonation attack, the modification attack, and the replay attack.

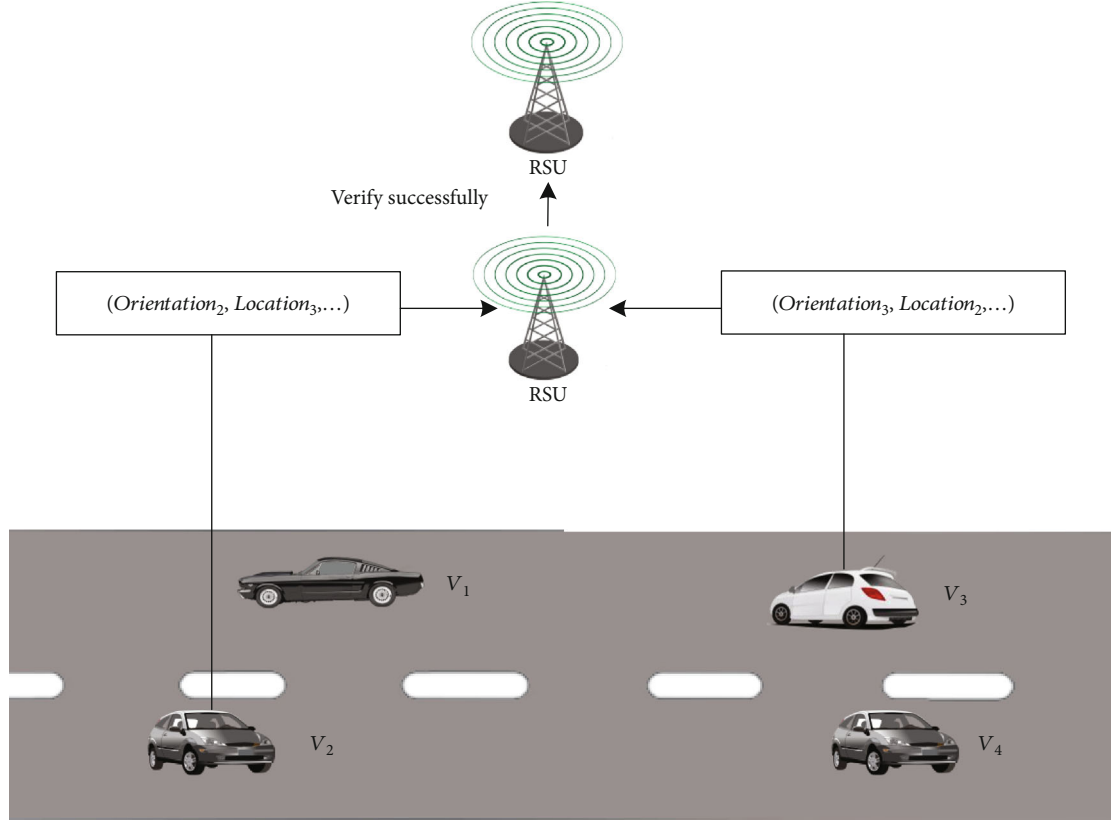


FIGURE 2: Certificateless aggregate signature system model.

TABLE 1: List of notations.

Notation	Description
TA	Trusted authority
KGC	Key generation center
RSU	Road-side unit
$h_i(\cdot), i = 1, 2, 3$	One-way collision-resistant hash function
$p, q$	Two secure prime numbers
$E$	An elliptic curve: $y^2 = x^3 + ax + b \pmod{p}$
$\mathbb{G}$	An additive group, the order of which is $q$
$P$	A generator of the group $\mathbb{G}$
$(PK_{TA}, \alpha)$	The public key and private key of the TA
$(PK_{KGC}, \beta)$	The public key and private key of the KGC
$(PK_{V_i}, \rho_i)$	The public key and private key of the vehicle
$PPK_i$	Partial private key of the vehicle $V_i$
$PID_i$	Pseudo identity of the vehicle $V_i$
TS	The latest timestamp
$\nabla$	State information

**5.3. Our Proposed CLS Scheme.** Our proposed CLS scheme includes five algorithms: Setup, PartialPrivateKeyGeneration, VehicleKeyGeneration, Sign, and Verify. The Notation to be used is listed in Table 1, and descriptions for algorithms are vividly shown in Figure 3 and described as follows:

- (1) **Setup:** when given an appropriate security parameter  $\lambda$ , TA will use the  $\lambda$  to generate and output the param by executing the following algorithms:
- (2) **PartialPrivateKeyGeneration:** the algorithm will eventually generate the vehicle's partial private key through the algorithms as follows:
- (3) **VehicleKeyGeneration:** after receiving the partial private key  $PPK_i$ , the vehicle  $V_i$  check if the equation  $PPK_i \cdot P = Q_i + n_i \cdot PK_{KGC}$  holds. If it holds, the partial private key  $PPK_i$  is valid. The vehicle randomly selects its private key  $\rho_i \in \mathbb{Z}_q^*$ , then calculates its public key  $PK_{V_i} = \rho_i \cdot P$ .
- (4) **Sign:** in order to achieve authentication and message integrity, when the message is received by any entity, it has to be signed and verified. A vehicle  $V_i$  uses its pseudo identity  $PID_i$  and picks the latest timestamp TS. The updated timestamp TS protects a signed message against replay attacks. Given the signing key  $(PPK_i, PK_{V_i})$  and a traffic related message  $m_i$ , the vehicle  $V_i$  performs the following steps, which are repeated every 100 – 300 ms in accordance with DSRC protocol [20]:

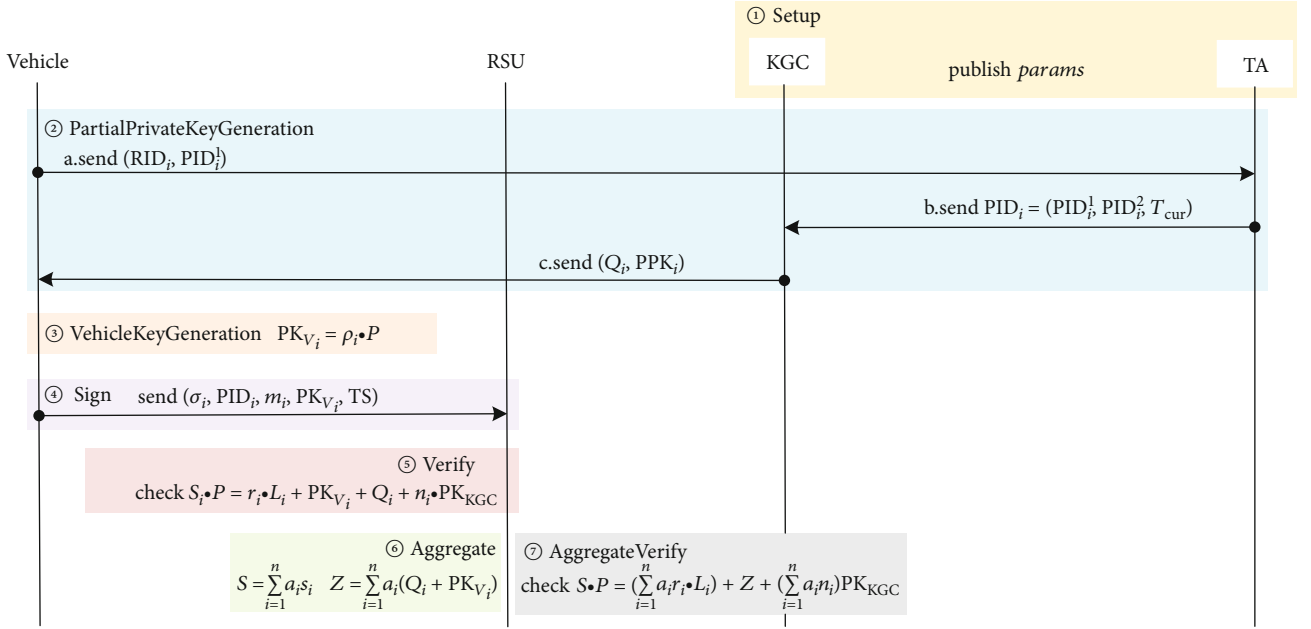


FIGURE 3: The algorithm procedure.

- (5) Verify: when an RSU or other entity receives the signature  $\sigma$  and the tuple  $(Q_i, PID_i, m_i, PK_{V_i}, TS)$  from the vehicle  $V_i$ , it can execute the algorithms to verify the message as follows:

*Step 1.* Firstly, select two secure prime numbers  $p$  and  $q$ , then choose  $a, b \in F_p$ , which generate an elliptic curve  $E$  defined by the equation  $y^2 = x^3 + ax + b \pmod{p}$ , where  $\Delta = 4a^3 + 27b^2 \neq 0 \pmod{p}$  and generator  $P$  of the additive group  $\mathbb{G}$  consisting of all the points on  $E$ .

*Step 2.* Choose  $\alpha \in \mathbb{Z}_q^*$  in random, which serves as the master secret key and computes master public key  $PK_{TA} = \alpha \cdot P$ . KGC selects  $\beta \in \mathbb{Z}_q^*$  in random, then calculates  $PK_{KGC} = \beta \cdot P$  which is the public key of KGC.

*Step 3.* Select three secure hash functions in random:  $h_1 : \mathbb{G} \times \{0, 1\}^* \times \{0, 1\}^* \times \mathbb{G} \times \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$ ,  $h_2 : \{0, 1\}^* \times \mathbb{G} \times \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$ ,  $h_3 : \{0, 1\}^* \times \{0, 1\}^* \times \{0, 1\}^* \times \mathbb{G} \times \mathbb{G} \times \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$ .

*Step 4.* Store its master secret key  $\alpha$  in its repository and keep it safe. Then publish all the system parameter:

$$\text{param} = \{p, q, a, b, P, PK_{TA}, PK_{KGC}, h_1, h_2, h_3\}. \quad (6)$$

*Step 1.* The vehicle  $V_i$  with its real identity  $RID_i$  randomly selects  $x_i \in \mathbb{Z}_q^*$  as its private key and calculates its partial pseudo identity  $PID_i^1 = x_i \cdot P$ . Then vehicle  $V_i$  transmits  $(RID_i, PID_i^1)$  to TA.

*Step 2.* After receiving the tuple, TA calculates another pseudo identity  $PID_i^2 = RID_i \oplus h_1(\alpha PID_i^1 \| T_{cur} \| PK_{TA} \| \nabla)$ , where  $\nabla$  is the system state information [19]; then TA sends the vehicle's pseudo identity  $PID_i = (PID_i^1, PID_i^2, T_{cur})$  to KGC in a secure way.

*Step 3.* KGC calculates  $Q_i = y_i \cdot P$ ,  $n_i = h_2(PID_i \| Q_i \| \nabla)$  and the vehicle's partial private key  $PPK_i = y_i + h_2(PID_i \| Q_i \| \nabla) \times \beta \pmod{p}$ . At last, KGC transmits the tuple  $(Q_i, PPK_i)$  to vehicle  $V_i$ .

*Step 1.* Choose a random number  $l_i \in \mathbb{Z}_q^*$  and calculate  $L_i = l_i \cdot P$ .

*Step 2.* Calculate  $r_i = h_3(m_i \| PID_i \| \nabla \| PK_{V_i} \| L_i \| TS)$ , where timestamp  $TS$  is used to confirm time, and  $S_i = r_i l_i + \rho_i + PPK_i \pmod{p}$ .

*Step 3.* The signature on message  $m_i$  is  $\sigma = (L_i, S_i)$ ; then the vehicle transmits the signature  $\sigma$  and  $(Q_i, PID_i, m_i, PK_{V_i}, TS)$  to the verifier.

*Step 1.* Check whether the  $TS$  is valid, if not, the algorithm aborts; otherwise, execute the next step.

*Step 2.* Calculate  $r_i = h_3(m_i \| PID_i \| \nabla \| PK_{V_i} \| L_i \| TS)$  and  $n_i = h_2(PID_i \| Q_i \| \nabla)$

*Step 3.* Check whether the following equation

$$S_i \cdot P = r_i \cdot L_i + PK_{V_i} + Q_i + n_i \cdot PK_{KGC} \quad (7)$$

holds or not; if it holds, then the RSU or other entity will



accept the signature and the message; otherwise, it will reject the message.

**5.4. Our Proposed CL-AS Scheme.** The Setup, PartialPrivate-KeyGeneration, VehicleKeyGeneration, Sign, and Verify algorithms of CL-AS are similar to the proposed CLS scheme. In addition, the Aggregate and AggregateVerify are described as follows. Note that the Aggregate and AggregateVerify algorithms are usually executed by the same RSU to transmit less data in the communication process.

- (1) **Aggregate:** when an aggregator such as a RSU receives  $n$  vehicles' messages  $M = \{m_1, m_2, \dots, m_n\}$ , signatures  $\sigma = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$ , timestamps  $TS = \{TS_1, TS_2, \dots, TS_n\}$ ,  $Q = \{Q_1, Q_2, \dots, Q_n\}$ , public key of each vehicle  $PK_V = \{PK_{V_1}, PK_{V_2}, \dots, PK_{V_n}\}$ ,  $L = \{L_1, L_2, \dots, L_n\}$ , and pseudo identities  $PID = \{PID_1, PID_2, \dots, PID_n\}$ . It can execute the following algorithms to aggregate the signature:
- (2) **AggregateVerify:** after aggregating  $n$  vehicles' messages, the same RSU will execute the following algorithms to verify the aggregate signature as follows:

*Step 1.* Randomly choose a random list  $RL = \{a_1, a_2, \dots, a_n\}$ , where  $a_i \in \mathbb{Z}_q^*$ ,  $1 \leq i \leq n$ . Note that the random list RL is firstly introduced in [21, 22] and used for resisting coalition attacks here.

*Step 2.* Calculate  $S = \sum_{i=1}^n a_i S_i$  and  $Z = \sum_{i=1}^n a_i (Q_i + PK_{V_i})$ .

*Step 3.* Outputs the signature  $\sigma = (L, S)$  and transmits  $(M, \sigma, Z, RL, PID, Q, TS)$  to the verifier.

*Step 1.* Check whether the timestamp list TS is valid, if not, the algorithm aborts; otherwise, it executes next step.

*Step 2.* For every vehicle, calculate  $r_i = h_3(m_i \| PID_i \| \nabla \| PK_{V_i} \| L_i \| TS)$  and  $n_i = h_2(PID_i \| Q_i \| \nabla)$ .

*Step 3.* Check whether the following equation

$$S \cdot P = \left( \sum_{i=1}^n a_i r_i \cdot L_i \right) + Z + \left( \sum_{i=1}^n a_i n_i \right) \cdot PK_{KGC} \quad (8)$$

holds or not, if it holds, then the RSU or other entity will accept the signature and the message, then the RSU can transmit them to other entities; otherwise, it will reject the message.

**5.5. Correctness of Individual Message Verification.** The individual verification in the proposed scheme is correct. The

correctness proof is as follows:

$$\begin{aligned} S_i \cdot P &= (r_i l_i + \rho_i + \text{PPK}_i) \cdot P = (r_i l_i + \rho_i + y_i + n_i \beta) \\ &\cdot P = r_i l_i \cdot P + \rho_i \cdot P + y_i \cdot P + n_i \beta \\ &\cdot P = r_i \cdot L_i + \text{PK}_{V_i} + Q_i + n_i \text{PK}_{KGC}. \end{aligned} \quad (9)$$

**5.6. Correctness of Aggregate Message Verification.** The aggregate verification in the proposed scheme is correct. The correctness proof is as follows:

$$\begin{aligned} S \cdot P &= \sum_{i=1}^n a_i S_i \cdot P = \left( \sum_{i=1}^n a_i r_i l_i + a_i \rho_i + a_i \text{PPK}_i \right) \\ &\cdot P = \sum_{i=1}^n a_i (r_i l_i \cdot P + \rho_i \cdot P + y_i \cdot P + n_i \beta \cdot P) \\ &= \left( \sum_{i=1}^n a_i r_i \cdot L_i \right) + Z + \left( \sum_{i=1}^n a_i n_i \right) \cdot \text{PK}_{KGC}. \end{aligned} \quad (10)$$

**5.7. Security Proof of the Proposed CLS Scheme.** According to Definition 3, it is extremely hard to solve ECDLP. Therefore, we can prove that our CLS scheme is able to enforce nonforgery.

On the basis of Definition 4, assume that a probabilistic polynomial-time forger  $A_1$  can forge a signature with an advantage  $\epsilon$ . In addition,  $q_{h_i}$  denotes random oracles  $h_i$  for  $i = 2, 3$ ,  $q_{GU}$  denotes the Generate-User oracle,  $q_{PPK}$  denotes Partial-Private-Key oracle, and  $q_{SK}$  denotes the Secret-Key oracle. Then, we can know that a challenger  $C_1$  can solve ECDLP during a time scope  $T$ , where  $T \leq 120686QT/\epsilon$ , if  $\epsilon \geq 10(q_S + 1)(q_{h_2} + q_{h_3} + q_{PPK} + q_{GU} + q_{SK} + q_S)/q$ .

- (1) **Setup:**  $C_1$  chooses  $\alpha$  and calculates  $PK_{TA} = \alpha \cdot P$  which serves as its private key and master public key. Then,  $C_1$  will generate the system parameters  $\text{param} = (P, p, q, E, G, h_1, h_2, h_3, PK_{TA}, PK_{KGC})$ , and transmit it to  $A_1$ .

- (i)  **$h_2$  Hash Query:**  $C_1$  will examine whether the hash list  $L_{h_2}$  has the corresponding tuple if it receives the query with parameter  $(PID_i, Q_i)$  from  $A_1$ . If not,  $C_1$  will select a random number  $\tau_{h_2} \in \mathbb{Z}_q^*$  and put it in the list  $L_{h_2}$ . If so, it needs to transmit  $\tau_{h_2} = h_2(PID_i \| Q_i \| \nabla)$  to  $A_1$ .

- (ii)  **$h_3$  Hash Query:**  $C_1$  will examine whether the hash list  $L_{h_3}$  has the corresponding tuple  $(m_i, PID_i, PK_{V_i}, Z_i, TS, \tau_{h_3})$  if it receives the query with parameter  $\text{param} = (m_i, PID_i, PK_{V_i}, L_i, TS)$  from  $A_1$ . If not,  $C_1$  will choose a random number  $\tau_{h_3} \in \mathbb{Z}_q^*$  and put the tuple  $(m_i, PID_i, PK_{V_i}, L_i, TS, \tau_{h_3})$  in the list  $L_{h_3}$ . If so, it will transmit  $\tau_{h_3} = h_3(m_i \| PID_i \| \nabla \| PK_{V_i} \| L_i \| TS)$  to  $A_1$ . Eventually,  $C_1$  will transmit  $\tau_{h_3} = h_3(m_i \| PID_i \| \nabla \| PK_{V_i} \| L_i \| TS)$  to  $A_1$ .

- (2) **Partial-Private-Key Query:** after receiving a query about the identity  $PID_i$  from  $A_1$ ,  $C_1$  will calculate  $Q_i = y_i \cdot P$ , where  $y_i$  is randomly selected, and check whether the hash list  $L_{h_2}$  has the corresponding tuple  $(PID_i, Q_i, \tau_{h_2})$ . If so,  $C_1$  will calculate  $PPK_i = y_i + h_2(PID_i \| Q_i \| \nabla) \times \alpha \pmod p$  and transmit the pairial private key of vehicle  $V_i PPK_i$  to  $A_1$ . If not, it will halt.
- (3) **User-Generation Query:** suppose that the query is on the basis of the pseudo identity  $PID_i$
- $C_1$  will check whether  $PK_{V_i}$  exists in the list  $L$ , if the list  $L$  includes  $(PID_i, PK_{V_i}, \rho_i)$ . If not, a random number  $\rho_i \in \mathbb{Z}_q^*$  will be selected and  $C_1$  will calculate  $PK_{V_i} = \rho_i \cdot P$ . If so, it will transmit  $PK_{V_i}$  to  $A_1$ . Eventually, the chanllenger  $C_1$  will transmit  $PK_{V_i}$  to  $A_1$  and update the list
  - $C_1$  will set  $PK_{V_i} = \perp$  if the tuple  $(PID_i, PK_{V_i}, \rho_i)$  does not exist in the list  $L$ . Then, a random number  $\rho_i \in \mathbb{Z}_q^*$  will be chosen and  $PK_{V_i} = \rho_i \cdot P$  will be calculated and  $\rho_i$  will be regarded as a private key. Eventually,  $C_1$  will transmit  $PK_{V_i}$  to  $A_1$  and put the tuple  $(PID_i, PK_{V_i}, \rho_i)$  to the list  $L$
- (4) **Private-Key Query:**
- $C_1$  will check whether  $\rho_i$  exists in the list  $L$ , if the list  $L$  includes  $(PID_i, PK_{V_i}, \rho_i)$ . If not, it will access a User-Generation query to output the public key  $PK_{V_i} = \rho_i \cdot P$ . Eventually, the chanllenger  $C_1$  will transmit  $\rho_i$  to  $A_1$  and update the list
  - $C_1$  will access a User-Generation query if the tuple  $(PID_i, PK_{V_i}, \rho_i)$  does not exist int he list  $L$ . Eventually,

$C_1$  will transmit  $\rho_i$  to  $A_1$  and put the tuple  $(PID_i, PK_{V_i}, \rho_i)$  to the list  $L$

- Sign Query:** after receiving a legitimate query about the message  $m_i$  of pseudo identity  $PID_i$ ,  $C_1$  will check the tuple  $(PID_i, Q_i, \tau_{h_2})$  in the hash list  $L_{h_2}$ . Hence, it can easily get the value  $\tau_{h_2}$  from the tuple and select two random numbers  $l_i$  and  $r_i$ . Then,  $C_1$  will choose another two random numbers  $s_i$  and  $n_i$ . Furthermore,  $C_1$  will calculate  $Z_i = s_i \cdot P - n_i \cdot PK_{KGC}$  and  $S_i = s_i$ . Eventually, it will transmit  $(L_i, S_i)$  to  $A_1$  and put the tuple  $(m_i, PID_i, PK_{V_i}, L_i, TS, \tau_{h_3})$  in the list  $L_{h_3}$ .

**Theorem 7.** *According to the random oracle, when faced with an adaptive chosen message attack, our proposed scheme has the capacity of unforgeability.*

*Proof.* Assume that an ECDLP sample  $(P, Q = x \cdot P)$  is given, the elliptic curve  $E$  holds two points  $P$  and  $Q$ , and an adversary  $A_1$  is able to forge message  $(PID_i, PK_{V_i}, m_i, TS, \sigma_i)$ . Hence, we start a game between a chanllenger  $C_1$  and the adversary  $A_1$ , which can execute and manipulate  $A_1$  to solve ECDLP with a nonnegligible probability.

We know the forking lemma in Definition 4 and apply it to our proposed scheme. After using the same random elements to replay  $A_1$ ,  $C_1$  succeeds in getting two legitimate signatures  $\sigma_i = (Z_i, S_i)$  and  $\sigma'_i = (L'_i, S'_i)$  during a polynomial time period, where  $S_i = r_i \cdot L_i + Q_i + PK_{V_i} \pmod p$  and  $S'_i = t'_i \cdot L_i + Q_i + PK_{V_i} \pmod p$  by computing.

$$\frac{t'_i S_i - r_i S'_i}{t'_i - r_i} \pmod p = \frac{t'_i r_i l_i + t'_i Q_i + t'_i PK_{V_i} - r_i t'_i l_i - r_i PPK_i - r_i Q_i + r_i PK_{V_i}}{t'_i - r_i} \pmod p = Q_i + PK_{V_i}. \quad (11)$$

In conclusion, if  $\varepsilon \geq 10(q_S + 1)(q_{h_2} + q_{h_3} + q_{PPK} + q_{UG} + q_{SK} + q_S)/q$ , then  $C_1$  is able to break the ECDLP during a time period which is less than  $120686QT/\varepsilon$ . However, this conclusion is inconsistent with the difficulty of solving the ECDLP. Therefore, we can define that our proposed CLS scheme can resist a forgery attack.

**5.8. Security Proof of the Proposed CL-AS Scheme.** According to Definition 3, it is extremely hard to solve ECDLP. Therefore, we can prove that our scheme is able to enforce nonforgery. Furthermore, we will prove that our CL-AS scheme can also resist coalition attack.

- Setup:** a random number  $\alpha$  is selected as the master secret key, and the public key can also be calculated as  $PK_{TA} = \alpha \cdot P$ . Then, the oracle simulation is ready to run. In this whole game,  $C_2$  maintains a list  $L = \{PID_i, PPK_i, PK_{V_i}, \rho_i\}$  and responds to  $A_2$ 's oracle as follows.

- $h_2$  Query:** after receiving a pseudo identity  $PID_i$ ,  $C_2$  will throw a coin  $c_i \in \{0, 1\}$ , where 0 holds a probability  $\varepsilon$ , and 1 holds a probability  $1 - \varepsilon$ , then  $C_2$  will select

$w_i^1 \in \mathbb{Z}_q^*$ . If  $c_i = 1$ ,  $C_2$  will output  $Q_i = w_i^1 \cdot P$ . Otherwise, it will define  $Q_i = \omega_i^1 \cdot P$ .  $C_2$  will put the tuple (PID $_i, w_i^1, c_i, Q_i$ ) in a list  $L_{h2} = (\text{PID}_i, w_i^1, c_i, Q_i)$  to trace what the queries respond no matter what the value  $c_i$  is.

**Theorem 8.** *According to the random oracle, when faced with an adaptive chosen message attack, our proposed CL-AS scheme has the capacity of unforgeability.*

*Proof.* Suppose that our CL-AS scheme can be broken by forger  $A_2$ . We can construct a challenger  $C_2$  using forgery algorithm  $A_2$ . Challenger  $C_2$  is able to execute the following steps by interacting with  $A_2$ .

Then,  $A_2$  will transmit  $n$  vehicles with identities from the list  $L_{\text{PID}}^* = \{\text{PID}_1^*, \text{PID}_2^*, \dots, \text{PID}_n^*\}$ , public keys from the list  $L_{\text{PK}_V}^* = \{\text{PK}_{V_1}^*, \text{PK}_{V_2}^*, \dots, \text{PK}_{V_n}^*\}$ ,  $n$  messages  $L_M^* = \{m_1^*, m_2^*, \dots, m_n^*\}$ , a random list  $RL^* = \{a_1^*, a_2^*, \dots, a_n^*\}$ , and a certificateless aggregate signature  $\sigma^* = \{L^*, S^*\}$ . At the beginning,  $C_2$  will select the  $n$  tuples (PID $_i^*, w_i^1, c_i^*, Q_i^*$ ) for  $i = 1, 2, \dots, n$  in the list  $L_{h2}$  and precede only  $c_k = 1$  and  $c_j = 0$  for  $j = 1, 2, \dots, n, j \neq k$ . Note that the Sign oracle has not received the tuple (PID $_k^*, \text{PK}_{V_k}^*, m_k^*$ ). Otherwise,  $C_2$  will halt and fail. This success case signifies that  $Q_k = w_k^1 \cdot \text{PK}_{\text{TA}}$  and  $Q_j = w_j^1 \cdot P$  for  $j = 1, 2, \dots, n, j \neq k$ . In addition, the aggregate signature  $\sigma^* = (L^*, S^*)$  is supposed to satisfy the aggregate verification equation  $S \cdot P = \sum_{i=1}^n (a_i r_i \cdot L_i) + Z + (\sum_{i=1}^n a_i n_i) \cdot \text{PK}_{\text{KGC}}$ .

Accordingly,  $C_2$  checks the tuples  $(m_i^*, \text{PID}_i^*, \text{PK}_{V_i}^*, Z_i^*, w_i^2)$  in the list  $L_{h3}$  and the tuple (PID $_i^*, \text{PPK}_i^*, \text{PK}_{V_i}^*, \rho_i$ ) from  $L$ . Later, it calculates  $S_i^* = w_i^1 \cdot \alpha \bmod p$ , which will satisfy  $S_i^* \cdot P = w_i^1 \cdot \text{PK}_{\text{TA}} = Q_i^*$  for  $i = 1, 2, \dots, n, i \neq k$ . Eventually,  $C_2$  constructs  $S'^*$  as  $S'^* = S^* - \sum_{i=1, i \neq k}^n a_i S_i^*$ ,  $S'^* = \text{PPK}_k^* + \sum_{i=1}^n w_i^2 r_i^* \pmod{p}$  for  $L^* = l_i^*$  and  $l_i^* \in \mathbb{Z}_q^*$  for  $1 \leq i \leq n$ .  $C_2$  will select a random number  $h_k^* \in \mathbb{Z}_q^*$  and calculate  $Z^* = (h_k^*)^{-1} \sum_{i=1}^n w_i^2 a_i (r_i \cdot L_i + Q_i + \text{PK}_{V_i})$ .

Hence, the hash value  $h_3(m_k^*, \text{PID}_k^*, \text{PK}_{V_k}^*, Z_k^*)$  is defined as  $h_k^*$ . It will use  $h_k^*$  until it does not repeat if the list  $L_{h3}$  holds the tuple  $h_3(m_k^*, \text{PID}_k^*, \text{PK}_{V_k}^*, Z_k^*)$ . Consequently, the signature  $(L'^*, S'^*)$  is a legitimate certificateless signature on message  $m_k^*$  for the reason that the equation below:

$$\begin{aligned} Q_{V_k}^* + h_{k,0}^* + h_k^* Z'^* &= Q_{V_k}^* \\ &+ h_{k,0}^* + h_k^* (h_k^*)^{-1} \sum_{i=1}^n w_i^2 a_i (r_i \cdot L_i + Q_i + \text{PK}_{V_i}) \\ &= Q_{V_k}^* + h_{k,0}^* + \sum_{i=1}^n w_i^2 a_i (r_i \cdot L_i + Q_i + \text{PK}_{V_i}) \\ &= \text{PPK}_k^* \cdot P + \sum_{i=1}^n w_i^2 a_i (r_i \cdot L_i + Q_i + \text{PK}_{V_i}) = S'^* \cdot P. \end{aligned} \quad (12)$$

Eventually,  $S$  can get the signature  $(L'^*, S'^*)$  as a forgery of the certificateless signature scheme. However, this conclusion is inconsistent with the difficulty of solving the ECDLP. Therefore, we can define that our proposed CLS scheme can resist a forgery attack.

**Theorem 9.** *The proposed certificateless aggregate signature (CL-AS) scheme can resist coalition attacks.*

*Proof.* Assume that there are two malicious vehicles  $V_1$  and  $V_2$  with pseudonyms PID $_1$  and PID $_2$  and messages  $m_1$  and  $m_2$ , respectively, and that all other system params are published by TA and KGC. According to the description in Subsection 4.3, two vehicles  $V_1$  and  $V_2$  would like to execute similar algorithms to forge valid signatures. However, our proposed scheme can perfectly resist the coalition attacks; the detailed descriptions are as follows:

To begin with, two vehicles  $V_i$  ( $i \in \{1, 2\}$ ) pick their own private key  $\rho_i$  and calculate their corresponding public key  $\text{PK}_{V_i} = \rho_i \cdot P$ .

According to the aforementioned algorithms in Subsection 5.7, two malicious vehicles execute the algorithms in order but secretly exchange their  $r_i L_i$ , which is a part of the signature. Eventually, two vehicles transmit their messages  $m_i$ , signatures  $\sigma_i$ , timestamp  $\text{TS}_i$ , and pseudo identity PID $_i$  to the aggregator.

When the aggregator receives the above information, it will aggregate the signature as follows: firstly choose a random list  $\text{RL} = \{a_1, a_2\}$ , where  $a_i \in \mathbb{Z}_q^*$ ,  $1 \leq i \leq n$ , then calculate  $S = \sum_{i=1}^2 a_i S_i$  and  $Z = \sum_{i=1}^2 a_i (Q_i + \text{PK}_{V_i})$ . Finally, the aggregator will output the signature  $\sigma = (L, S)$  and transmits  $(M, \sigma, Z, \text{RL}, \text{PID}, Q, T)$  to the verifier.

In the last step, the verifier will check the equation  $S \cdot P = \sum_{i=1}^2 (a_i r_i \cdot L_i) + Z + (\sum_{i=1}^n a_i n_i) \cdot \text{PK}_{\text{KGC}}$  holds or not. Unfortunately, the equation is impossible as follows:

$$\begin{aligned} S \cdot P &= (a_1 r_2 L_2 + a_1 \rho_1 + a_1 \text{PPK}_1 + a_2 t_1 L_1 + a_2 \rho_2 + a_2 \text{PPK}_2) \\ &\cdot P = a_1 t_2 \cdot L_2 + a_1 \cdot \text{PK}_{V_1} + a_1 \cdot Q_1 + a_1 n_1 \cdot \text{PK}_{\text{KGC}} + a_2 t_1 \\ &\cdot L_1 + a_2 \cdot \text{PK}_{V_2} + a_2 \cdot Q_2 + a_2 n_2 \cdot \text{PK}_{\text{KGC}} = a_1 t_2 \cdot L_2 + a_2 \\ &\cdot t_1 L_1 + Z + \sum_{n=1}^2 (a_i n_i) \cdot \text{PK}_{\text{KGC}} \neq \sum_{i=1}^2 (a_i r_i \cdot L_i) + Z \\ &+ \sum_{n=1}^2 (a_i n_i) \cdot \text{PK}_{\text{KGC}}. \end{aligned} \quad (13)$$

One can find that the random list plays an important role in resisting the coalition attacks. And the 2-vehicle situation can also be developed to  $n$  vehicles simply with a fully the same method and algorithm, which can prove that our proposed certificateless aggregate signature (CL-AS) scheme can resist coalition attacks.

TABLE 2: Cryptographic operation notations and executing time.

Operation	Description	Time (ms)
$T_{bp}$	Bilinear pairing operation	4.1603
$T_{bp-m}$	Scalar multiplication in bilinear pairing operation	1.6722
$T_{bp-a}$	Addition in bilinear pairing operation	0.0069
$T_{e-m}$	Scalar multiplication in ECC operation	1.1280
$T_{e-a}$	Addition in ECC operation	0.0339
$T_h$	One-way hash function	0.0360

## 6. Performance and Security Analysis

### 6.1. Security Analysis

- (1) Traceability: in the proposed scheme, only TA has the real identity of the certain vehicle. After submitting the pseudo identity  $PID_i = (PID_i^1, PID_i^2, T_{cur})$ , TA can easily trace back to the vehicle's real identity  $RID_i$  in accordance with the equation  $PID_i^2 = RID_i \oplus h_1(\alpha PID_i^1 \| T_{cur} \| PK_{TA} \| \nabla)$ . Therefore, according to the  $RID$  list, TA can trace back to the certain vehicle  $V_i$ , even revoke it. ( $RID_i, PID_i^1$ )
- (2) Message integrity and authentication: according to Definition 3, the ECDLP problem is hard, so that no polynomial adversary can forge a valid message. Therefore, the verifier can verify the validity and integrity of the message  $(Q_i, PID_i, PK_{V_i}, m_i, TS, \sigma_i)$  by verifying whether the equation  $S_i \cdot P = r_i L_i + P K_{V_i} + Q_i + n_i \cdot PK_{KGC}$  holds or not. Therefore, our proposed scheme for VANETs provides message authentication and integrity.
- (3) Resistance to replay attacks: the proposed scheme can resist the replay attack for the reason that the tuple  $(Q_i, PID_i, PK_{V_i}, m_i, TS, \sigma_i)$  includes the timestamp  $TS$ . RSU and other vehicles will check the validity of the signature, so they are able to detect the replay of the message. Hence, our proposed scheme for VANETs can resist replay attacks.
- (4) Resistance to coalition attacks: our proposed scheme can resist the coalition attacks, because we improve the signature generation process. To be specific, we choose a random list to change the ratio in the equation  $S = \sum_{i=1}^n a_i S_i$ . Therefore, our scheme uses this method to resist the coalition attacks.
- (5) Resistance to stealing of the check table: in the proposed scheme, TA, KGC, vehicles, and RSUs do not require a check list. Therefore, an attacker cannot complete an attack by stealing any checklist. Hence, the proposed scheme can resist the attack of the checklist.

*6.2. Performance Analysis.* In this section, we will discuss the performance of the proposed scheme and related schemes and make a comparison in detail. We adopt the method of computation evaluation where the bilinear pairing on the security level of 80 bits is created as follows:  $\bar{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ , where  $\mathbb{G}_1$  is an additive group generated by a point  $\bar{P}$  with order  $\bar{q}$  on a super singular elliptic curve  $\bar{E} : y^2 = x^3 + x \pmod{\bar{p}}$  with embedding degree 2,  $\bar{p}$  is a 512-bit prime number,  $\bar{q}$  is a 160-bit prime number [25]. The ECC on the security of 80 bits is constructed as follows:  $\mathbb{G}$  is an additive group with order  $q$  that is generated on a nonsingular elliptic curve  $E : y^2 = x^3 + ax + b \pmod{p}$ , where  $p, q$  are 160-bit primes and  $a, b \in \mathbb{Z}_q^*$ . The experiment is conducted using the well-known python cryptographic library PyCryptodome on a desktop running Intel I5-9400 @ 2.90 GHz processor, with 16 GB memory running Windows 10 operating system. The notations of the cryptographic operations used in this paper and their running times are given in Table 2. Table 3 shows the summary of the computation costs in terms of signing a message, verifying a single message, and verifying  $n$  messages.

In [13, 24], their schemes choose to use bilinear pairing, which significantly increases their operation time. As a contrast, other four schemes [6, 12, 17, 23] do not use bilinear pairing, which can substantially reduce computation time.

In our scheme,  $L_i = l_i \cdot P$  uses a scalar multiplication in ECC operation and the calculation of  $r_i$  uses a one-way hash function during the individual sign process. In individual verification, we use three scalar multiplication operations for  $S_i \cdot P$ ,  $r_i \cdot L_i$ , and  $n_i \cdot PK_{KGC}$ , three addition operations, and two one-way hash function operations for the calculations of  $r_i$  and  $n_i$ . In aggregate verification process, we use  $n + 2$  scalar multiplication operations for  $\sum_{i=1}^n a_i r_i \cdot L_i$ ,  $S \cdot P$ , and  $\sum_{i=1}^n a_i n_i \cdot PK_{KGC}$ , two addition operations, and  $2n$  one-way hash function operations for each  $n_i$  and  $r_i$ . By comparison, our scheme has low time complexity and high efficiency. In addition, our scheme can resist coalition attacks, which are a special and security feature that no other scheme has.

We use the data in Table 3 to generate three figures, which can intuitively compare other related schemes with

TABLE 3: Comparison of our proposed scheme with other related schemes.

Scheme	Individual sign	Individual verify	Aggregate verify	Coalition attacks resistance	With pairing
Kamil et al. [6]	$3T_{e-m} + 2T_{e-a} + 3T_h = 3.5598ms$	$2T_{e-m} + T_{e-a} + T_h = 2.6988ms$	$2T_{e-m} + nT_{e-a} + nT_h = (0.0699n + 2.2899)ms$	No	No
Kumar et al. [12]	$4T_{e-m} + 2T_{e-a} + 3T_h = 4.6878ms$	$4T_{e-m} + 3T_{e-a} + 4T_h = 4.7577ms$	$4T_{e-m} + 3nT_{e-a} + 4nT_h = (0.2457n + 4.512)ms$	No	Yes
Yang et al. [13]	$4T_{bp-m} + 2T_{bp-a} + 3T_h = 6.9582ms$	$3T_{bp} + 3T_{bp-m} + T_{bp-a} + 4T_h = 17.9111ms$	$2nT_{bp} + 3nT_{bp-m} + nT_{bp-a} + 4nT_h = 13.7001nms$	Yes	Yes
Cui et al. [17]	$T_{e-m} + T_{e-a} + T_h = 1.1979ms$	$3T_{e-m} + 2T_{e-a} + 2T_h = 3.5238ms$	$(n+2)T_{e-m} + (n+2)T_{e-a} + 2nT_h = (1.2339n + 2.3238)ms$	No	No
Zhao et al. [23]	$T_{e-m} + 2T_h = 1.2ms$	$4T_{e-m} + 3T_{e-a} + T_h = 4.6497ms$	$(n+2)T_{e-m} + (n+3)T_{e-a} + nT_h = (1.1979n + 2.3577)ms$	No	No
Malhi et al. [24]	$4T_{bp-m} + 2T_{bp-a} + T_h = 6.8862ms$	$3T_{bp} + 3T_{bp-m} + T_{bp-a} + 2T_h = 17.8391ms$	$3T_{bp} + 3nT_{bp-m} + nT_{bp-a} + 2nT_h = (5.2061n + 12.633)ms$	No	Yes
Our scheme	$T_{e-m} + T_h = 1.164ms$	$2T_{e-m} + 3T_{e-a} + 3T_h = 3.5577ms$	$(n+1)T_{e-m} + 2T_{e-a} + 2nT_h = (1.2n + 1.1958)ms$	Yes	No



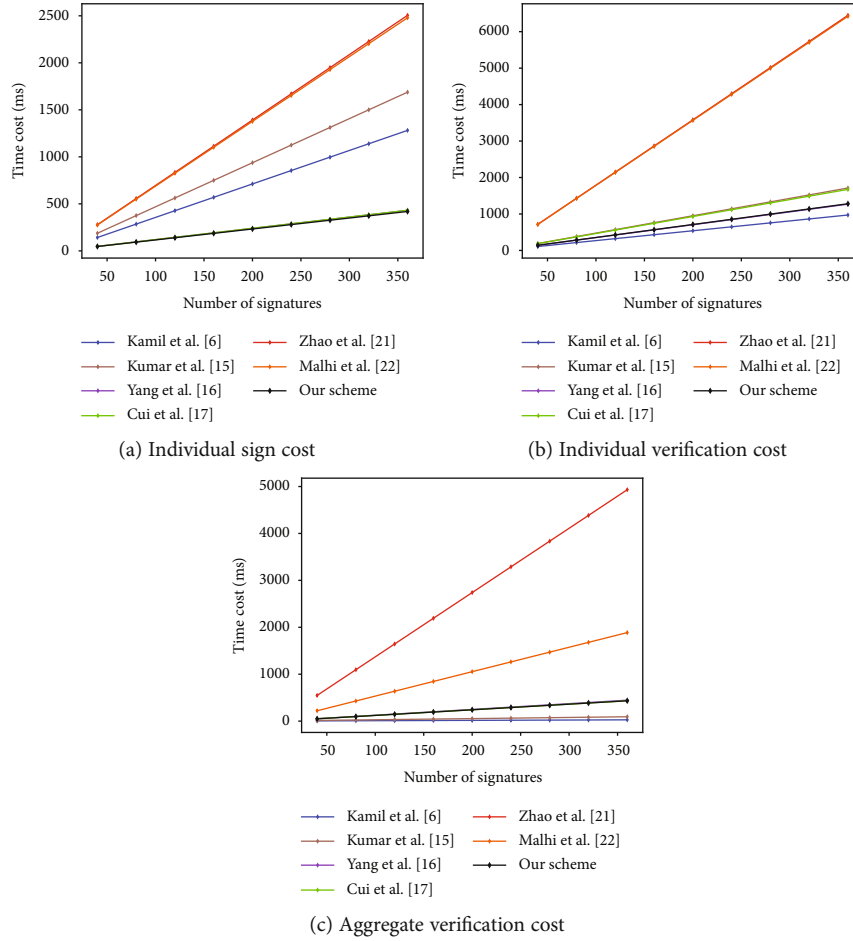


FIGURE 4: Time cost of different schemes in three cases.

our scheme. In Figures 4(a)–4(c), we can get the conclusion that our scheme has a considerably low delay in sign and verification procedure, which reveals that our scheme has a much higher efficiency.

## 7. Conclusion

Since real application scenarios of VANETs require high efficiency, an efficient certificateless-based anonymous authentication and aggregate signature scheme are proposed. The proposed CLS and its improved scheme CL-AS are appropriate for VANETs duo to analysis and testing. In addition, there is still some work to do in the future such as the low efficiency caused by the illegitimate signature in the aggregate verification process.

## Data Availability

The proposed algorithm and its comparison rely on theoretical analysis. No additional test data sets are required in this paper.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This work is supported by the Key International Cooperation Projects of the National Natural Science Foundation of China (No. 61520106007).

## References

- [1] S. Bitam, A. Mellouk, and S. Zeadally, "Vanet-cloud: a generic cloud computing model for vehicular ad hoc networks," *IEEE Wireless Communications*, vol. 22, no. 1, pp. 96–102, 2015.
- [2] C. Lin, D. He, X. Huang, N. Kumar, and K. R. Choo, "Bcpga: a blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–13, 2020.
- [3] A. Kumar, G. Thangavel, and K. Subba, "An approach to identify the Sybil attacks in vehicular ad-hoc networks using path signature," *International Journal of Scientific & Technology Research*, vol. 9, pp. 3412–3415, 2020.
- [4] Y. Jiang, S. Ge, and X. Shen, "Aaas: an anonymous authentication scheme based on group signature in vanets," *IEEE Access*, vol. 8, pp. 98986–98998, 2020.
- [5] Y. Zheng, G. Chen, and L. Guo, "An anonymous authentication scheme in vanets of smart city based on certificateless group signature," *Complexity*, vol. 2020, 7 pages, 2020.

- [6] I. A. Kamil and S. O. Ogundoyin, "An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks," *Journal of Information Security and Applications*, vol. 44, pp. 184–200, 2019.
- [7] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy*, vol. 2, no. 3, pp. 49–55, 2004.
- [8] Z. Jianhong, X. Min, and L. Liying, "On the security of a secure batch verification with group testing for vanet," *International Journal of Network Security*, vol. 16, no. 5, pp. 351–358, 2014.
- [9] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: efficient conditional privacy preservation protocol for secure vehicular communications," in *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, pp. 1229–1237, Orlando, FL, USA, 2008.
- [10] J. K. Liu, J. Baek, J. Zhou, Y. Yang, and J. W. Wong, "Efficient online/offline identity-based signature for wireless sensor network," *International Journal of Information Security*, vol. 9, no. 4, pp. 287–296, 2010.
- [11] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology - ASIACRYPT 2003*, C.-S. Lai, Ed., pp. 452–473, Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.
- [12] P. Kumar, S. Kumari, V. Sharma, X. Li, A. K. Sangaiah, and S. K. H. Islam, "Secure cls and cl-as schemes designed for vanets," *The Journal of Supercomputing*, vol. 75, no. 6, pp. 3076–3098, 2019.
- [13] X. Yang, C. Chen, T. Ma, Y. Li, and C. Wang, "An improved certificateless aggregate signature scheme for vehicular ad-hoc networks," in *2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 2018.
- [14] K. Hashimoto and W. Ogata, "Unrestricted and compact certificateless aggregate signature scheme," *Information Sciences*, vol. 487, pp. 97–114, 2019.
- [15] Y. Xie, X. Li, S. Zhang, and Y. Li, "iclas: an improved certificateless aggregate signature scheme for healthcare wireless sensor networks," *IEEE Access*, vol. 7, pp. 15170–15182, 2019.
- [16] H. Du, Q. Wen, and S. Zhang, "An efficient certificateless aggregate signature scheme without pairings for healthcare wireless sensor network," *IEEE Access*, vol. 7, pp. 42683–42693, 2019.
- [17] J. Cui, J. Zhang, H. Zhong, R. Shi, and Y. Xu, "An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks," *Information Sciences*, vol. 451-452, pp. 1–15, 2018.
- [18] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, no. 3, pp. 361–396, 2000.
- [19] S. O. Ogundoyin and S. O. Awoyemi, "Edas: efficient data aggregation scheme for internet of things," *Journal of Applied Security Research*, vol. 13, no. 3, pp. 347–375, 2018.
- [20] J. B. Kenney, "Dedicated short-range communications (dsrc) standards in the united states," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.
- [21] M. S. Kakkasageri and S. S. Manvi, "Information management in vehicular ad hoc networks: a review," *Journal of Network and Computer Applications*, vol. 39, pp. 334–350, 2014.
- [22] M. Rudack, M. Meincke, and M. Lott, "On the dynamics of ad hoc networks for inter vehicle communications (ivc)," in *proc. ICWN*, vol. 2, Citeseer, 2002.
- [23] Y. Zhao, Y. Hou, L. Wang, S. Kumari, M. K. Khan, and H. Xiong, "An efficient certificateless aggregate signature scheme for the internet of vehicles," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 5, pp. 3708–3711, 2020.
- [24] A. K. Malhi and S. Batra, "An efficient certificateless aggregate signature scheme for vehicular ad-hoc networks," *Discrete Mathematics and Theoretical Computer Science*, vol. 17, no. 1, pp. 317–338, 2015.
- [25] O. S. Oyinlola, "An autonomous lightweight conditional privacy-preserving authentication scheme with provable security for vehicular ad-hoc networks," *International Journal of Computers & Applications*, vol. 42, pp. 196–211, 2020.

## Research Article

# Dynamic Network Security Mechanism Based on Trust Management in Wireless Sensor Networks

Guiping Zheng <sup>1</sup>, Bei Gong <sup>1</sup>, and Yu Zhang <sup>2</sup>

<sup>1</sup>Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China

<sup>2</sup>School of Information Science and Technology, Zhengzhou Normal University, Henan 450044, China

Correspondence should be addressed to Yu Zhang; 20852192@qq.com

Received 7 November 2020; Revised 30 December 2020; Accepted 12 February 2021; Published 28 February 2021

Academic Editor: Zhuojun Duan

Copyright © 2021 Guiping Zheng et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Wireless sensor network is a key technology in Internet of Things. However, due to the large number of sensor nodes and limited security capability, aging nodes and malicious nodes increase. In order to detect the untrusted nodes in the network quickly and effectively and ensure the reliable operation of the network, this paper proposes a dynamic network security mechanism. Firstly, the direct trust value of the node is established based on its behavior in the regional information interaction. Then, the comprehensive trust value is calculated according to the trust recommendation value and energy evaluation value of other high-trust nodes. Finally, node reliability and management nodes are updated periodically. Malicious nodes are detected and isolated according to the credibility to ensure the dynamic, safe, and reliable operation of the network. Simulation results and analysis show that the node trust value calculated by this mechanism can reflect its credibility truly and accurately. In terms of reliable network operation, the mechanism can effectively detect malicious nodes, with higher detection rate, avoid the risk of malicious nodes as management nodes, reduce the energy consumption of nodes, and also play a defensive role in DOS attacks in wireless sensor networks.

## 1. Introduction

Internet of Things (IoT) can be regarded as the third information technology revolution following the computer and the Internet [1, 2]. It connects massive device nodes through the Internet, enabling everything to be interconnected whenever and wherever. In recent years, the widespread applications of IoT have not only changed people's lifestyles but also have a certain impact on the original cultivation patterns. Wireless Sensor Network (WSN), as a key technology in IoT, is a network system composed of microsensor nodes through wireless communication, and it is also an important source of sensing data in IoT. WSNs have been widely used in various fields, including weather monitoring, medical care, military applications, and the study phenomena in places where people cannot easily reach [3–5]. Its development and application will also have far-reaching impact on various fields, so it is very essential to ensure the safe and reliable operation of WSNs.

While WSNs play a huge role in IoT, the security problems are even more severe due to the characteristics of the sensor network itself [6–9]. On one hand, nodes in WSNs are usually deployed in unattended environments, which makes nodes have great security risks, such as vulnerable to physical attacks, being captured by attackers, private information being extracted, being transformed into malicious nodes, and launching various attacks. On the other hand, due to the mobility and effectiveness of nodes, the network topology in WSNs will change dynamically, which makes it difficult to maintain the trust relationship between nodes. In addition, sensor nodes in WSNs are characterized by limited energy, weak computing and storage capacity, low power consumption, and intensive deployment, which leads to the security protection mechanism in traditional networks cannot function effectively in WSNs, making the security problems of WSNs more prominent. Therefore, it has important significance to research into security mechanisms of WSNs.

On account of the existing problems in WSNs, this paper puts forward a dynamic network security mechanism based on trust management. This mechanism is based on trusted networking and takes trust computing as the core. Based on trust measurements, it can effectively detect malicious nodes in the network so that the network can operate dynamically and reliably. Eventually, the proposed scheme was verified by experiments.

## 2. Related Work

In WSNs, there are many researches on the safe and reliable operation mechanism of the network, which are used to detect malicious nodes attacks. Zhang et al. [10] proposed a detection scheme based on watermarking technology to detect selective forwarding attacks, which can not only detect whether the routing node discards the data packet but also detect whether the data in the packet is tampered. However, the scheme has a large delay in extracting watermarks and is not suitable for large-scale networks. Xu [11] proposed a sensor network malicious node detection scheme based on double threshold. Each sensor node maintains the trust value of its neighbors to reflect their past behavior in decision-making. Two thresholds are used to reduce the false alarm rate and enhance the accuracy event area detection; thus, under the condition of without sacrificing normal node implementation to detect malicious nodes is more accurate. However, appropriate threshold selection problem is the difficulty of scheme. An adaptive security mechanism of on-demand access control is proposed by Mauro et al. [12] for multihop energy harvesting in WSNs. In this mechanism, nodes can use base stations to release their current security measures, which helps sending nodes select appropriate recipient nodes according to their security requirements. But it is possible to cause malicious nodes to launch malicious attacks by reducing network security measures.

Trust management, as one of the methods to effectively defend against network internal attacks and identify malicious nodes, has been widely used in WSNs, and many typical models also have been proposed by scholars at domestic and foreign. Aiming at the low accuracy and malicious recommendation of the IoT trust evaluation method, Xie et al. [13] proposed a dynamic trust evaluation method for IoT nodes. First of all, this method designed the node service quality persistence factor to represent the overall behavior of the node, then used the friend acquaintance degree to filter recommended nodes, and finally calculated the comprehensive trust degree based on information entropy. The method proposed in [13] can effectively reduce the impact of malicious recommendation behavior on trust evaluation, but the implementation process is complicated and computationally intensive. Objects in the Social Internet of Things (SIoT) [14, 15] interact with each other based on their social behavior, in which any object can be either a service provider or a service consumer. Jafarian et al. [16] compared the service query context with the previous query context of other reviewers based on a data mining model, taken into account indicators such as social similarity, service importance, and the residual energy of providers, and considered this issue to a three-

dimensional space. They measured the value contribution of trust value by using a weighted method. But the definition of social boundary involved in this method is ambiguous, and it cannot accurately calculate social acquaintance, which is not applicable to IoT systems with complex social relationships. Lin et al. [17] proposed a perceptual network security connection model based on the characteristics of social networks. This model describes the inferred transfer, transmission, update, and changes in the dynamic environment of trust in the IoT from the perspective of sociology, but the model does not combine subjective and objective in the trust evaluation process, and the accuracy of node trust evaluation is deficient.

Luo et al. [18] proposed a dynamic trust management system, which uses the hash algorithm to generate the unique identifier for nodes and uses the trust evaluation model based on the  $\beta$  density function to dynamically manage the trust value of each node. It can resist both external attacks and internal compromise attacks, but the model has large memory and energy costs and computational complexity. Bao and Chen et al. [19, 20] used collaborative filtering method to screen trust recommendation nodes and proposed a trust management model of IoT based on social relations. This model can improve the reliability of recommendation trust evaluation and enhance the ability of model to resist malicious recommendation behavior. However, in the process of direct trust evaluation, only the timeliness of trust is considered, which cannot accurately reflect the node behavior. A trust-based network security connection model suggested by Nguyen et al. [21], which is based on event-driven triggering trust refresh, extends trust definition and realizes data collection and analysis from multiple data sources. However, the dynamic adaptability of the model was insufficient. Chen et al. [22] raised a distributed adaptive filtering-based sensing network security connection model based on service-oriented architecture, which integrates dynamic direct trust and indirect trust to confirm the trust of nodes. On this basis, it guarantees the reliable operation of nodes, has good environmental adaptability, and fully considers the limited computing power of sensing nodes. However, the model lacks feedback control of nodes and cannot cope with malicious attacks well. Sathish et al. [23] improved the model proposed by Priyoheswari et al. [24] by introducing the proxy nodes and proposed an intelligent Beta reputation and dynamic trust evaluation model. The node credibility of the model was only evaluated by direct communication behavior. Although the energy consumption of trust calculation was reduced, the convergence rate of the model was reduced due to the lack of indirect trust evaluation process; thus, malicious nodes cannot be quickly identified.

To sum up, all kinds of current research schemes have their own characteristics (Table 1). Comparison of advantages and disadvantages of each scheme makes a comparative analysis of relevant work. The existing WSN dynamic adaptive security mechanism research has many deficiencies, which leads to the failure of existing WSN security mechanism to meet the needs of rapid development of WSNs. This paper proposes a dynamic adaptive security mechanism suitable for WSNs based on trust management. Firstly, it

TABLE 1: Comparison of advantages and disadvantages of each scheme.

Schemes	Advantages	Disadvantages
Detection scheme based on watermarking technology [10]	Effectively detect whether the data is discarded or tampered	The time delay of watermark extraction is large
Detection scheme of sensor network malicious nodes based on double threshold [11]	Reduce the false alarm rate and improve the accuracy of event area detection	The problem of threshold selection is the difficulty of this method
Adaptive security mechanism for on-demand access control [12]	Fully consider the security requirements of each node	May cause malicious nodes to launch malicious attacks using cuts in network security measures
A dynamic trust evaluation method for Internet of Things nodes [13]	Effectively reduce the influence of malicious recommendation behavior on trust evaluation	Complex implementation process and large amount of computation
Trust evaluation scheme based on data mining model in SIoT [16]	Comprehensively measure the value contribution of trust value assessment	The definition of social boundary is vague and cannot accurately calculate social familiarity
Perceived network security connection model [17]	Describe the changes of trust in various states from a sociological perspective	Without combining subjective and objective, the accuracy of node trust assessment is deficient
Dynamic trust management system [18]	To defend against external attacks but also to defend against internal compromise attacks	High memory and energy cost, high computational complexity
Trust management model of Internet of Things based on social relations [19, 20]	Improve the reliability of recommendation trust evaluation and enhance the ability of model against malicious recommendation behavior	Cannot accurately reflect node behavior
Trust-aware network security connection model [21]	Extending the definition of trust and realizing the function of data collection and analysis from multiple data sources	Lack of dynamic adaptability
Sensory network security connection model based on distributed adaptive filtering [22]	Good environmental adaptability, fully considering the computing ability of sensing nodes	Lack of feedback control to nodes, unable to resist malicious attacks perfectly
Intelligent Beta reputation and dynamic trust evaluation model [23, 24]	Reduce the energy consumption of trust computation	The convergence rate of the model is reduced, and the malicious nodes cannot be identified quickly

calculates the trust degree of sensor nodes in WSNs based on trust management model, then removes malicious nodes and selects management nodes based on trust degree, so as to make the network run dynamically and reliably.

### 3. Network Dynamic Security Adjustment Mechanism

The network dynamic adaptive adjustment mechanism proposed in this paper takes the trust computing model as the core, dynamically monitors the change of nodes in real time according to the trust degree of each node in the domain, and updates the network topology structure in time, thus ensuring the trusted operation of WSNs. The mechanism is described from three aspects: network model, trust evaluation model, and dynamic adaptive adjustment of WSNs.

*3.1. Network Model Framework in WSNs.* As shown in Figure 1, the network model in WSNs is mainly composed of four parts: ordinary nodes, domain management nodes, monitoring nodes, and base stations.

Ordinary nodes are used for data sensing and collection, so as to conduct information interaction between nodes, and

evaluate and calculate direct and indirect local trust according to the interaction results.

Domain management nodes are high-trust nodes selected from ordinary nodes, which are mainly used to maintain the credibility of nodes within the domain, ensure that the nodes in the region are in a secure and reliable environment, calculate the comprehensive trust of each node, isolate malicious nodes in time, and communicate directly with the base station.

Monitoring nodes not only have the same function as the domain management nodes but also need to monitor the behavior of the domain management nodes. If the management nodes behave abnormally, they will directly send reports to the base stations. Each region contains two monitoring nodes, whose comprehensive trust value is second only to the domain management node in this region.

Base stations are used to select the domain management nodes and update the domain management nodes timely according to the reports from monitoring nodes. In this paper, it is assumed that the base stations are completely credible.

*3.2. Trust Evaluation Model.* The trust assessment framework proposed in this paper is shown in Figure 2. The trust degree of nodes is firstly calculated by the local trust degree between



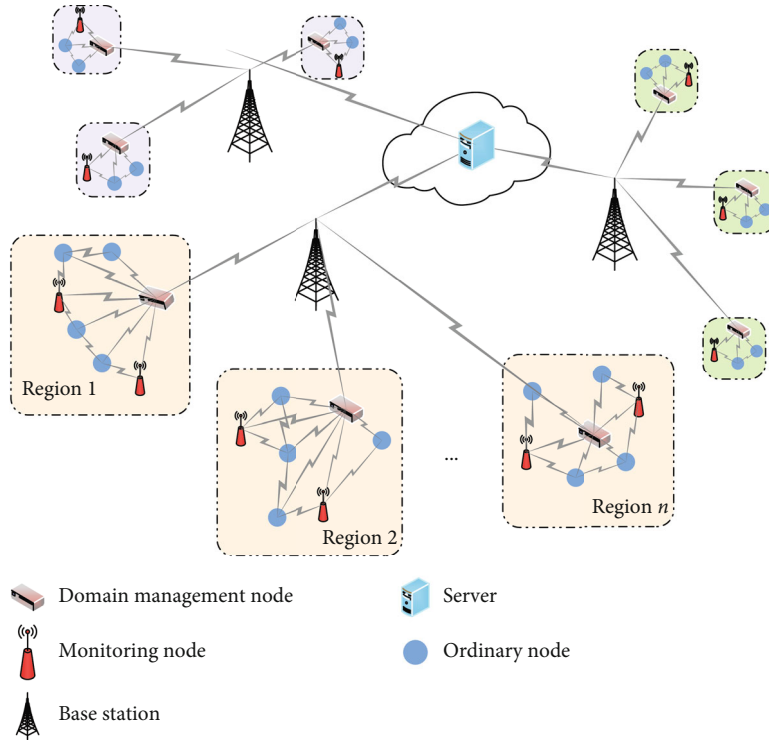


FIGURE 1: WSN node deployment architecture.

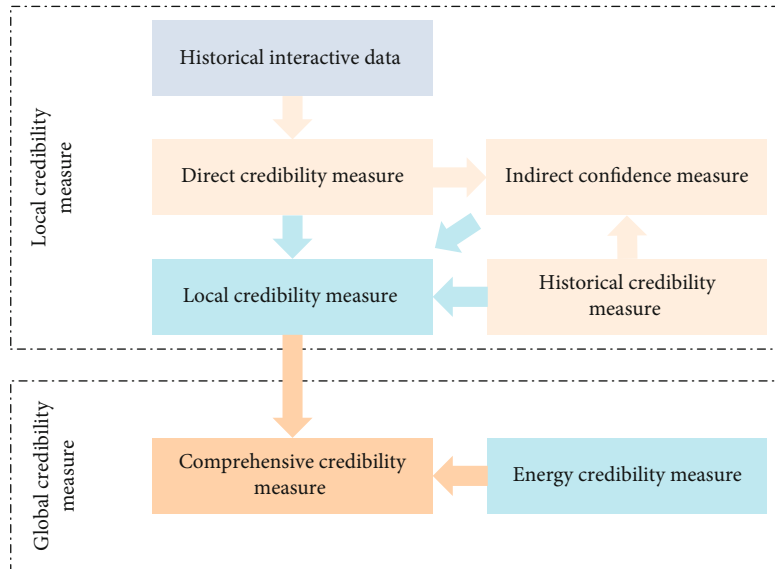


FIGURE 2: Trust assessment architecture.

the nodes in the domain, and then, the comprehensive trust degree of those nodes is calculated by domain management nodes. Improve the credibility of nodes, this paper sets the automatic update time  $\Delta T$ , so as to calculate the trust degree of nodes regularly. In the following description, only the calculation process within one detection time  $\Delta T$  is only described.

*3.2.1. Related Definitions and Initialization.* The calculation of nodes trust is the core of this mechanism. Trust is the abil-

ity to believe that a node has reliable and safe behavior in a certain context. Trust value is a quantitative representation of the trust ability of a node, and its size determines the credibility of the node. In this paper, the trust value range of node is  $[0,1]$ , where 0 means that the node belongs to a completely untrusted node, and 1 means that the node is completely trusted. In the initial stage, the trust value of all nodes is initialized in this paper, and the value is 0.5. Domain management nodes and monitoring nodes are served by nodes with strong computing power and high energy.

**3.2.2. Local Credibility Measure.** Local trust is the result of mutual evaluation between interdomain nodes, which is mainly composed of direct credibility measure and indirect credibility measure.

(1) *Direct Credibility Measure.* The direct trust value is that the evaluation nodes combine the historical direct interaction data to predict the possible behavior of the evaluated nodes in the future. Trust evaluation method based on Bayesian can effectively reduce the complexity of trust calculation and energy consumption. In this method, if the number of successful and unsuccessful interactions between nodes  $N_i$  and  $N_j$  is  $u$  and  $v$ , respectively, the interaction results between nodes  $N_i$  and  $N_j$  obey Beta distribution. Therefore, the mathematical expectation  $E(\text{beta}(p | u, v))$  of the Beta probability density function  $\text{beta}(p | u, v)$  is obtained as the direct trust value  $D_{ij}$ , which is taken by (1).

$$D_{ij} = E(\text{beta}(p | u, v)) = \frac{u + 1}{u + v + 2}. \quad (1)$$

(2) *Indirect Credibility Measure.* Although direct trust is directly detected between nodes through information interaction, if the degree of interaction between two nodes is not enough or affected by channels or malicious nodes attack, the direct trust cannot measure the credibility of nodes. Therefore, this paper uses recommendation trust to make the prediction of nodes trust more accurate.

The recommended trust value of evaluating node  $N_i$  to evaluated node  $N_j$  needs to be obtained from node  $N_k$ , where  $N_k$  belongs to  $N_j$ 's neighbor nodes set  $\text{Ne}(N_j)$ . In the IoT environment, node distribution is relatively dense, which leads to a large number of neighbor nodes. If each neighbor node makes recommendations, the network energy consumption will be accelerated, and the risk of bad-mouthing attack with higher or lower reputation may be faced. Therefore, this paper selects a set  $\text{PNe}(N_j)$ , a subset of  $\text{setNe}(N_j)$ , to calculate the recommended trust value for node  $N_j$ . The process of determining the partial neighbor node set  $\text{PNe}(N_j)$  is as follows:

- (a) The evaluation node  $N_i$  requests the domain management node to request the  $n$  nodes with the highest global trust degree in the set  $\text{Ne}(N_j)$  as the recommended nodes, and the global trust degree of these nodes must not be lower than the recommended trust threshold  $\delta_0$
- (b) After receiving the set  $\text{PNe}(N_j)$  from the domain management node, node  $N_i$  sends a trust recommendation delivery request to the nodes in  $\text{PNe}(N_j)$ . Node  $N_k$  in set  $\text{PNe}(N_j)$  receives the request and then sends  $D_{kj}$  to node  $N_i$ , where  $D_{kj}$  represents the direct trust from node  $N_k$  to  $N_j$ , according to (2) calculate the recommended trust  $\text{RT}_{ij}^k$  of the neighbor nodes  $N_k$  to  $N_j$

$$\text{RT}_{ij}^k = \text{LT}_{ik}^{\text{old}} * D_{kj}, \quad (2)$$

where  $\text{LT}_{ik}^{\text{old}}$  represents the historical local trust of nodes  $N_i$  to  $N_k$ . Therefore, node  $N_i$  calculates the final recommendation trust  $\text{RT}_{ij}$  based on the recommendation value of each node to node  $N_j$  in set  $\text{PNe}(N_j)$ . Since each neighbor node has different trust degree at node  $N_i$ , it is necessary to give certain weights to the recommendation trust value of each node. In this paper, according to (3), the weight  $w_k$  of the recommendation trust of node  $N_k$  in the indirect trust value is calculated, where  $|\text{PNe}(N_j)|$  represents the total number of nodes in the set. Then, according to (4), the recommended trust  $\text{RT}_{ij}$  from nodes  $N_i$  to  $N_j$  is calculated.

$$w_k = \frac{\text{RT}_{ij}^k}{\sum_{l=1}^{|\text{PNe}(N_j)|} \text{RT}_{ij}^l}, \quad (3)$$

$$\text{RT}_{ij} = \sum_{k=1}^{|\text{PNe}(N_j)|} w_k * \text{LT}_{ik}^{\text{old}} * D_{kj}. \quad (4)$$

(3) *Local Trust Synthesis and Update.* After the evaluation node  $N_i$  passes the above process, the direct trust degree  $D_{ij}$  and the recommended trust degree  $\text{RT}_{ij}$  for the evaluated node  $N_j$  can be obtained. The evaluation node  $N_i$  first calculates the local trust degree  $\text{LT}_{ij}^{\text{new}}$  within  $\Delta T$  according to (5), then combines the local trust degree  $\text{LT}_{ij}^{\text{old}}$  in the previous  $\Delta T$ , and finally updates the local trust degree  $\text{LT}_{ij}$  according to (6). This process needs to measure the proportion of  $D_{ij}$  and  $\text{LT}_{ij}^{\text{old}}$ , where  $\eta_0$  and  $\eta_1$  are the measuring factors, and their values are set according to the specific environment.

$$\text{LT}_{ij}^{\text{new}} = \eta_0 D_{ij} + (1 - \eta_0) \text{RT}_{ij}, \quad (5)$$

$$\text{LT}_{ij} = \eta_1 \text{LT}_{ij}^{\text{old}} + (1 - \eta_1) \text{LT}_{ij}^{\text{new}}. \quad (6)$$

**3.2.3. Global Credibility Measure.** Global credibility measurement is mainly about calculating comprehensive trust. In the calculation of comprehensive trust, the energy state of the nodes needs to be considered in order to eliminate the influence of energy changes. It is known from Section 3.1 that each region has a domain management node and two monitoring nodes. For the convenience of description, this article uses  $G_x$  to represent the domain management node of area  $x$ , and the two monitoring nodes of  $G_x$  represent by  $G_x^{M_1}$  and  $G_x^{M_2}$ .  $G_x$ ,  $G_x^{M_1}$ , and  $G_x^{M_2}$  will receive the local trust matrix  $M(x)$  as shown in (7), where  $m(m = |G_x|)$  represents the total number of nodes in the region  $x$ .

$$M(x) = \begin{bmatrix} \text{LT}_{11} & \text{LT}_{12} & \cdots & \text{LT}_{1m} \\ \text{LT}_{21} & \text{LT}_{22} & \cdots & \text{LT}_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \text{LT}_{m1} & \text{LT}_{m2} & \cdots & \text{LT}_{mm} \end{bmatrix}. \quad (7)$$

For node  $N_j$ , by searching for elements greater than zero in the  $M(x)$ 's column vector, denoted by the set  $S_j$ , then obtain the average value  $\bar{T}_j$  from (8), and obtain the energy trust  $ET_j$  of node  $N_j$  from (9); finally, calculate the comprehensive trust degree  $T_j$  of node  $N_j$  according to (10), where  $E_j^{\text{now}}$  represents the current energy value of node  $N_j$ ,  $E_j^{\text{start}}$  represents the initial energy value of node  $N_j$ , and  $\eta_2$  represents the weight factor.

$$\bar{T}_j = \frac{\mathbf{1}}{|S_j|} \sum_{LT_{ij} \in S_j} LT_{ij}, \quad (8)$$

$$ET_j = \frac{E_j^{\text{now}}}{E_j^{\text{start}}}, \quad (9)$$

$$T_j = \eta_2 \bar{T}_j + (\mathbf{1} - \eta_2) ET_j. \quad (10)$$

**3.3. Dynamic Adaptive Adjustment of WSNs.** Based on the trust calculation, the base station can clearly grasp the status of all the sensing nodes in the region, so as to better use computing resources and communication resources from a global perspective and realize the adaptive adjustment of WSNs. Next, the dynamic network security adjustment mechanism will be studied from the selection and update of domain management nodes and the isolation of malicious nodes.

**3.3.1. Domain Management Node Selection and Update.** The process of selecting and updating domain management nodes is shown in Figure 3. The specific process is as follows:

- (i) Domain management node  $G_x$  and monitoring nodes  $G_x^{M_1}$  and  $G_x^{M_2}$  obtain their respective comprehensive trust lists by calculation, which are, respectively, recorded as  $L_1$ ,  $L_2$ , and  $L_3$  and then sent them to the base station
- (ii) After receiving  $L_1$ ,  $L_2$ , and  $L_3$ , the base station selects the trust value with the highest number of occurrence as the final trust value of the node according to the three comprehensive trust values of each node
- (iii) After the base station gets the final trust list  $L$  containing each node, it needs to timely update the comprehensive trust values of  $G_x$ ,  $G_x^{M_1}$ , and  $G_x^{M_2}$ . Firstly, the similarity  $\theta_i$  between  $L$  and  $L_i$  is calculated according to (11). Then, the similarity  $\theta_i$  is judged. If it is 1, then the comprehensive trust value remains unchanged; otherwise, the comprehensive trust value will be reduced to  $(1 - \theta_i)$  times of the original

$$\theta_i = \frac{\mathbf{1}}{m} \sum_{j=1}^m (L^j == L_i^j ? \mathbf{1} : \mathbf{0}). \quad (11)$$

- (iv) The base station sets the trust threshold  $\delta_1$ . If the comprehensive trust of domain management node

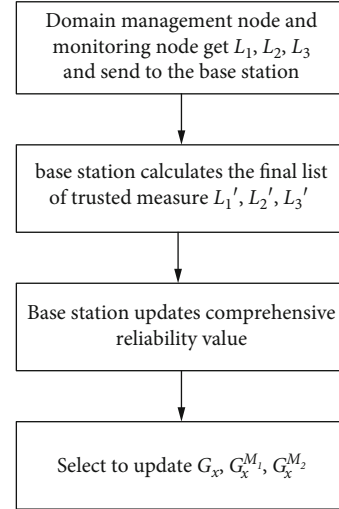


FIGURE 3: Domain management node selection and update process.

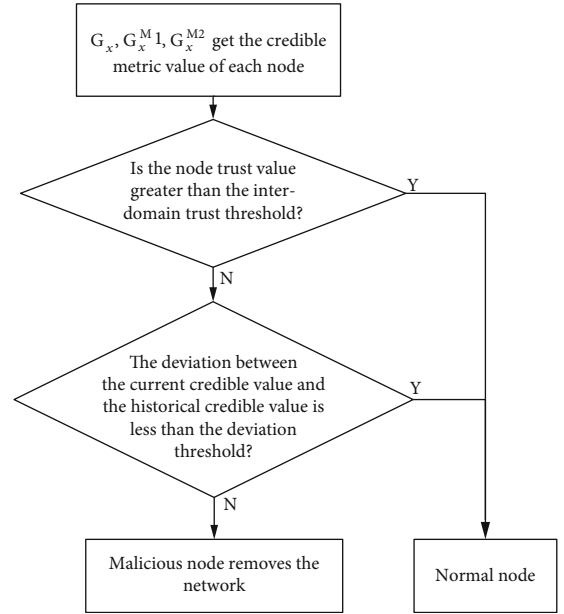


FIGURE 4: Malicious node detection process.

or monitoring node is lower than  $\delta_1$ , the three nodes with the highest trust degree in the domain need to be reselected as the new domain management node  $G_x$  and monitoring node  $G_x^{M_1}$  and  $G_x^{M_2}$ . The base station will send the final trust list  $L$  to the updated  $G_x$ ,  $G_x^{M_1}$ , and  $G_x^{M_2}$  as the comprehensive trust of each node in the domain

**3.3.2. Malicious Node Detection.** Over time, nodes may be attacked or damaged naturally, so malicious nodes need to be removed in a timely manner. Figure 4 shows the malicious node detection process.

After receiving the node information sent from the base station,  $G_x$ ,  $G_x^{M_1}$ , and  $G_x^{M_2}$  first determine whether the comprehensive trust value of each node is lower than the

TABLE 2: Some parameters of simulation experiment.

Parameter	Values
Simulation area size	100 m* 100 m
Number of nodes	100
Energy consumption for data transmission and reception	25 nJ/bit
Normal node initial energy	1 J
Manage node and monitor node initial energy	5 J
Packet size	40 bit
Wireless communication radius	15 m
Packet forwarding rate	Random number between [0.9,1]
Initial confidence	0.5

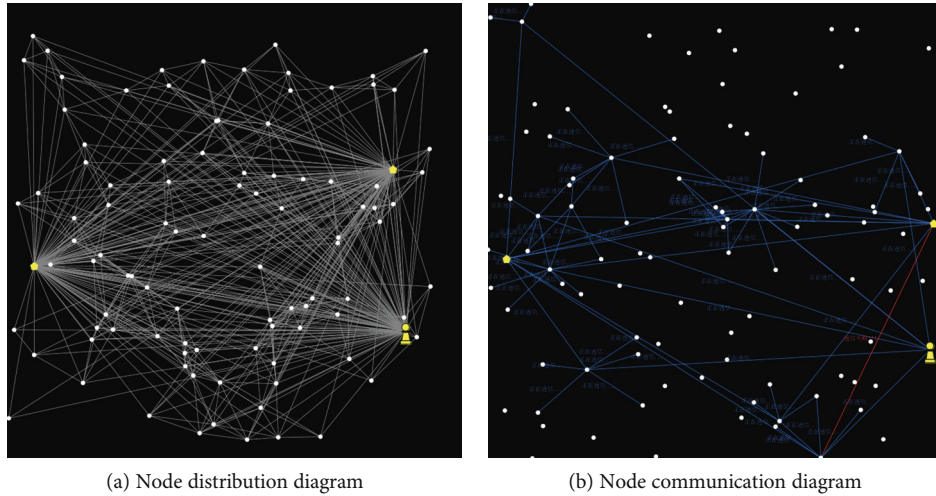


FIGURE 5: Simulation effect of the experiment.

interdomain trust threshold  $\delta_2$ . If lower than, it indicates that the node is insufficient in energy or is a malicious node. Otherwise, it is further detected whether the deviation of the current comprehensive trust value and the historical comprehensive trust value of the node are smaller than the deviation threshold  $\delta_3$ . If the deviation is less than  $\delta_3$ , it is a normal node. If it is greater than  $\delta_3$ , it can be divided into two situations: first, the current comprehensive trust value minus historical comprehensive trust value is greater than  $\delta_3$ , indicating that the trust value of the node has been greatly increased, and it can be determined that the node has disguised behavior; second, if the historical comprehensive trust value minus the current comprehensive trust value is greater than  $\delta_3$ , it indicates that the trust value of the node has been significantly reduced, and the node can be determined to be energy deficient or become a compromise node.

In addition, domain management node  $G_x$  can recognize DOS attacks when information is exchanged between nodes. According to the actual environment of region  $x$ , set the threshold  $\delta_4$  of interdomain node interaction within the detection period. If the total number of interactions between nodes  $N_i$  and  $N_j$  exceeds  $\delta_4$ , it indicates that the interactions between nodes  $N_i$  and  $N_j$  are too frequently, and it is highly likely that malicious DOS attacks will occur. Then, the behaviors of nodes  $N_i$  and  $N_j$  should be observed to further deter-

mine whether it is a malicious node and then remove them from the network.

#### 4. Simulation Experiment and Safety Analysis

*4.1. The Simulation Results.* In order to better verify the detection efficiency and energy consumption of this mechanism for malicious nodes, NetLogo is used to simulate the proposed mechanism in this paper. Since the simulation calculation process of each region is consistent, only one region is simulated. Some parameters of the simulation experiment are shown in Table 2.

Figure 5 shows the effect diagram of simulation using NetLogo. The figure on the left shows the initial network state. If the nodes can communicate with each other, they are indicated by connecting lines in the initial network state. The right figure represents the communication state at a certain moment, in which the lines represent the communication between nodes, the successful communication between nodes is represented by blue, and the failure is represented by red.

Firstly, in the trust calculation section, by analyzing the comprehensive trust value of all nodes, the comprehensive trust value curve of malicious nodes and the normal nodes in Figure 6 can be obtained. As can be seen from Figure 6,

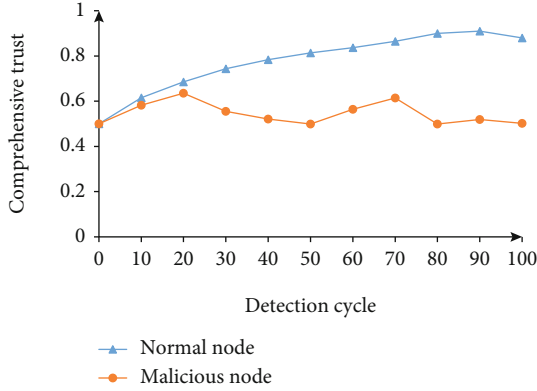


FIGURE 6: Curve of comprehensive trust change.

the normal node comprehensive trust value appears gradually rising trend, but with an increasing number of detection cycle, ordinary node comprehensive trust value will decline. This is because with the increase of detection cycle, the energy of nodes is limited, which leads to the gradual increase of the influence of the energy trust of nodes on the comprehensive trust. However, there is no regularity in the change in the overall trust of malicious nodes. Because malicious nodes do not know their comprehensive trust, it is possible to launch attacks at any time. But overall, the trust of malicious nodes will be far smaller than the normal nodes as the detection cycle changes.

Then, different proportion of malicious nodes is deployed in the network, as shown in Figure 7, and the detection rate changes of malicious nodes in 10, 20, and 40 cycles are compared, respectively. It can be seen from the horizontal direction that the detection rate will decrease as the number of malicious nodes increases, because the increase in malicious nodes will affect the accuracy of trust value and thus affect the judgment of nodes to some extent. Vertically, the longer the detection cycle, the higher the detection rate will be. This is because as the detection cycle increases, the malicious nodes will gradually be isolated, and the comprehensive trust generated by the interaction will become more and more accurate, which is conducive to the detection of malicious nodes. Overall, when malicious nodes are lower than 20%, the average detection rate of this paper is higher than 75%. This mechanism can detect and isolate malicious nodes quickly and effectively.

Finally, since sensor nodes are resource-constrained, it is necessary to analyze the energy consumption of nodes. Figure 8 shows that as the number of malicious nodes increases, the total energy consumption in the network increases gradually. At the same time, it can be seen that compared with [13], the scheme in this paper reduces the network energy consumption and the aging rate of nodes.

**4.2. Security Analysis.** In this paper, the recommendation trust value of all neighbor nodes is not used in the calculation of recommendation trust, but the set of high-trust neighbor nodes is screened out. This method can effectively exclude the malicious recommendation behavior of neighbor nodes and avoid bad-mouthing attack.

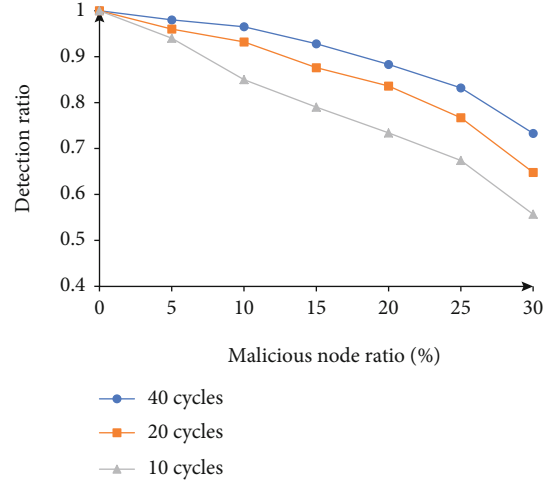


FIGURE 7: Detection rate of malicious nodes.

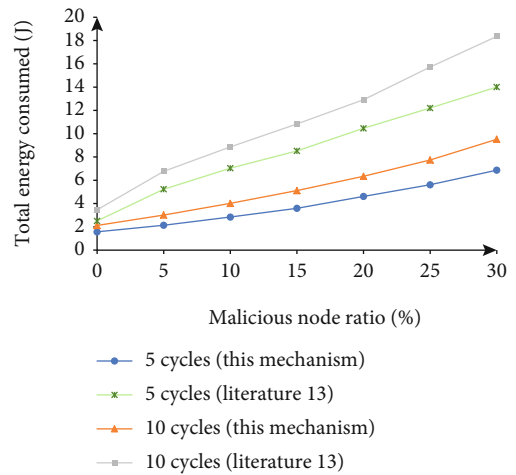


FIGURE 8: Total network energy consumption.

Domain management nodes play a role in managing other common nodes in the region. If a domain management node is attacked as a compromise node to launch a malicious attack, the trust value of all nodes cannot be measured, and the region falls into an extremely insecure situation. In this paper, monitoring nodes are set up to observe the behavior of the domain management node at any time and report it to the base station in time. The base station will verify the reported content. If true, the credibility of domain management node will be reduced, and the domain management node will be replaced with a node with higher trust. In addition, monitoring nodes have the same computing tasks as domain management nodes. If the base station detects that their behavior is abnormal, the domain management node and the monitoring node are replaced with new nodes in time. This method can effectively deal with the risk of domain management node being attacked.

In the traditional trust management mechanism, there is a risk of disguised attack, that is, when malicious nodes find their trust value is lower than other nodes, they will suspend the attack behavior, improve their trust value in a short term



through good performance, or change the identity and rejoin the network. In this paper, the comprehensive trust degree of nodes is only stored in the management node, the monitoring nodes, and the base station. Malicious nodes are not clear about themselves trust degree, so the masking behavior of malicious nodes is effectively avoided.

## 5. Conclusion

The key of network dynamic trusted operation is to identify and isolate malicious nodes to ensure their trusted operation. This paper proposes a network security mechanism based on trust management to deal with the threats faced by WSNs. Based on the trusted access of nodes, this mechanism firstly calculates the local trust degree of nodes according to existing interaction behavior and further obtains the comprehensive trust degree of nodes that can reflect the trust degree of nodes. In network management, the selection and updating of domain management nodes and detection of malicious nodes are carried out according to the comprehensive trust degree of nodes. Through simulation experiment analysis, the node's comprehensive trust can accurately reflect their behavior, detect and isolate malicious nodes in time, and effectively guarantee the trusted and reliable operation of WSNs.

## Data Availability

No data were used to support this study.

## Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

## Acknowledgments

This research was supported by the National Key R&D Program of China (2019YFB2102303), the National Natural Science Foundation of China (61971014), and the 2020 Henan Key Research and Development Project (202102310522).

## References

- [1] S. B. Shen and C. Lin, "Opportunities and challenges in study of Internet of Things," *Journal of Software*, vol. 8, pp. 1621–1624, 2014.
- [2] H. Kaur and R. Kumar, "A survey on Internet of Things (IoT): layer-specific, domain-specific and industry-defined architectures," *Advances in Computational Intelligence and Communication Technology*, vol. 1086, pp. 265–275, 2021.
- [3] R. Krishnan, "Mobile application for emergency navigation during disaster using wireless sensor network," *Advances in Wireless Communications and Networks*, vol. 4, no. 1, p. 1, 2018.
- [4] N. Brinis and L. A. Saidane, "Context aware wireless sensor network suitable for precision agriculture," *Wireless Sensor Network*, vol. 8, no. 1, pp. 1–12, 2016.
- [5] G. Ramesh and R. Nivedha, "Micro climate monitoring-web application using wireless sensor network," *International Journal of Science and Research (IJSR)*, vol. 5, no. 4, pp. 104–106, 2016.
- [6] J. Furtak, Z. Zielinski, and J. Chudzikiewicz, "Security techniques for the WSN link layer within military IoT," in *IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pp. 233–238, Reston, VA, USA, 2016.
- [7] D. Pandita, R. K. Malik, and Department of ECE, Geeta Engineering College, Panipat Kurukshetra University, Kurukshetra, Haryana, India, "A survey on clustered and energy efficient routing protocols for wireless sensor networks," *International Journal of Trend in Scientific Research and Development*, vol. Volume-2, no. Issue-6, pp. 1026–1030, 2018.
- [8] W. L. Wu, N. X. Xiong, and C. X. Wu, "Improved clustering algorithm based on energy consumption in wireless sensor networks," *The Institution of Engineering and Technology*, vol. 6, no. 3, pp. 47–53, 2017.
- [9] J.-Y. Yu, E. Lee, S.-R. Oh, Y.-D. Seo, and Y.-G. Kim, "A survey on security requirements for WSNs: focusing on the characteristics related to security," *IEEE Access*, vol. 8, pp. 45304–45324, 2020.
- [10] D. Y. Zhang, C. Xu, and S. Lin, "Detecting selective forwarding attacks in WSNs using watermark," *International Conference on Wireless Communications and Signal Processing (WCSP)*, vol. 2011, pp. 1–4, 2011.
- [11] C. J. Xu, *Research on detection scheme of malicious nodes and abnormal data in wireless sensor network [Ph.D. thesis]*, Nanjing University of Posts and Telecommunications, 2020.
- [12] A. D. Mauro, X. Fafoutis, and N. Dragoni, "Adaptive security in ODMAC for multihop energy harvesting wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 3, 2015.
- [13] L. X. Xie and R. X. Wei, "Dynamic trust evaluation method for IoT nodes," *Journal of Computer Applications*, vol. 39, no. 9, pp. 2597–2603, 2019.
- [14] A. U. Rehman, R. A. Naqvi, A. Rehman, A. Paul, M. T. Sadiq, and D. Hussain, "A trustworthy SIoT aware mechanism as an enabler for citizen services in smart cities," *Electronics*, vol. 9, no. 6, p. 918, 2020.
- [15] K. C. Chung and S. W.-J. Liang, "An empirical study of social network activities via social Internet of Things (SIoT)," *IEEE Access*, vol. 8, pp. 48652–48659, 2020.
- [16] B. Jafarian, N. Yazdani, and M. S. Haghghi, "Discrimination-aware trust management for Social Internet of Things," *Computer Networks*, vol. 178, p. 107254, 2020.
- [17] Z. T. Lin and L. Dong, "Clarifying trust in Social Internet of Things," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 2, pp. 234–248, 2018.
- [18] W. Luo, W. Ma, and Q. Gao, "A dynamic trust management system for wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 7, pp. 613–621, 2016.
- [19] F. Y. Bao and R. Chen, "Trust management for the Internet of Things and its application to service composition," *World of Wireless, Mobile & Multimedia Networks IEEE*, 2012.
- [20] I. R. Chen, F. Bao, and J. Guo, "Trust-based service management for Social Internet of Things systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 6, pp. 684–696, 2016.
- [21] H. L. Nguyen, O. J. Lee, J. E. Jung, J. Park, T. W. Um, and H. W. Lee, "Event-driven trust refreshment on ambient services," *IEEE Access*, vol. 5, pp. 4664–4670, 2017.

- [22] I. R. Chen, J. Guo, and F. Bao, "Trust management for SOA-based IoT and its application to service composition," *IEEE Transactions on Services Computing*, vol. 9, no. 3, pp. 482–495, 2017.
- [23] S. Sathish, A. Ayyasamy, and M. Archana, "An intelligent beta reputation and dynamic trust model for secure communication in wireless networks," *Industry Interactive Innovations in Science, Engineering and Technology (I3SET)*, vol. 11, pp. 395–402, 2017.
- [24] B. Priyoheswari, K. Kulothungan, and A. Kannan, "Beta reputation and direct trust model for secure communication in wireless sensor networks," in *Proceedings of the International Conference on Informatics and Analytics*, New York, NY, USA, 2016.

## Research Article

# BSSPD: A Blockchain-Based Security Sharing Scheme for Personal Data with Fine-Grained Access Control

Hongmin Gao <sup>1</sup>, Zhaofeng Ma <sup>1</sup>, Shoushan Luo <sup>1</sup>, Yanping Xu <sup>2</sup>, and Zheng Wu <sup>3</sup>

<sup>1</sup>Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China

<sup>2</sup>School of Cyberspace Security, Hangzhou Dianzi University, Hangzhou, Zhejiang Province 310018, China

<sup>3</sup>School of Electronics and Information Engineering, Hunan University of Science and Engineering, China

Correspondence should be addressed to Zheng Wu; 18153361706@189.cn

Received 25 November 2020; Revised 31 December 2020; Accepted 29 January 2021; Published 20 February 2021

Academic Editor: Zhuojun Duan

Copyright © 2021 Hongmin Gao et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Privacy protection and open sharing are the core of data governance in the AI-driven era. A common data-sharing management platform is indispensable in the existing data-sharing solutions, and users upload their data to the cloud server for storage and dissemination. However, from the moment users upload the data to the server, they will lose absolute ownership of their data, and security and privacy will become a critical issue. Although data encryption and access control are considered up-and-coming technologies in protecting personal data security on the cloud server, they alleviate this problem to a certain extent. However, it still depends too much on a third-party organization's credibility, the Cloud Service Provider (CSP). In this paper, we combined blockchain, ciphertext-policy attribute-based encryption (CP-ABE), and InterPlanetary File System (IPFS) to address this problem to propose a blockchain-based security sharing scheme for personal data named BSSPD. In this user-centric scheme, the data owner encrypts the sharing data and stores it on IPFS, which maximizes the scheme's decentralization. The address and the decryption key of the shared data will be encrypted with CP-ABE according to the specific access policy, and the data owner uses blockchain to publish his data-related information and distribute keys for data users. Only the data user whose attributes meet the access policy can download and decrypt the data. The data owner has fine-grained access control over his data, and BSSPD supports an attribute-level revocation of a specific data user without affecting others. To further protect the data user's privacy, the ciphertext keyword search is used when retrieving data. We analyzed the security of the BSSPD and simulated our scheme on the EOS blockchain, which proved that our scheme is feasible. Meanwhile, we provided a thorough analysis of the storage and computing overhead, which proved that BSSPD has a good performance.

## 1. Introduction

The development of 5G and Internet of Things technology provides a large amount of training data for the rapid implementation of artificial intelligence (AI). At the same time, data security and privacy protection have become the most interesting topics in data governance and sharing. Powerful data mining and analysis have brought potential threats to personal privacy protection. Traditionally, most people choose to outsource their data to cloud servers for sharing and dissemination. However, most of the data stored in the cloud is very sensitive, especially those data generated by IoT devices that are closely related to human life. These data have their particularities and may contain personal-related

information such as life, work, and healthcare; once personal data is stolen or leaked illegally and linked to the data owner's real identity, it may bring great trouble to an individual. Therefore, integrating data and generating value while ensuring data security and privacy have become a significant challenge for all contemporary companies that use big data and AI.

At present, researchers have proposed many secure sharing schemes in the cloud environment [1–9]. These schemes seem to solve the security and privacy issues during data sharing. Nevertheless, these schemes all have a standard feature: they are overly dependent on the Cloud Service Provider (CSP). They believe that the CSP is a trusted third-party organization, and their security models assume that

the CSP is semitrustable, which means that the CSP will be curious about the data but will not destroy it. It means that the following situations are always inevitable:

- (1) The CSP itself may make profits from the user's private data, or its insiders may do evil and cause the user's privacy disclosure. Although some methods, such as attribute-based encryption algorithms, can achieve user-defined access policies that seem user-centric, these methods still require a trusted third party to generate and manage user keys. It is impossible to exclude the possibility of collusion between these trusted centers. All these will lead to the fact that once the data owners upload their data to the cloud server, they will no longer have their data's absolute possession
- (2) The data is centrally stored on cloud servers and managed by the CSP. An inevitable single point of failure may lead that users cannot obtain their data generally by using the cloud service. The CSP can improve data security and service stability by utilizing disaster recovery backup. However, some irresistible factors will prevent users from using cloud services to obtain their data, such as political factors
- (3) To provide better service, the CSP needs to spend more money to buy servers, hire better employees, rent the data center venues, and so on. These costs are increasing gradually, and the CSP cost is also increasing and the construction of the management platform. Users ultimately pay the operating costs of the CSP

From the above point of view, to better protect data security and personal privacy, it is very urgent to design a whole user-centric data-sharing scheme to solve the above problems. In this scheme, we do not need to rely on any trusted third party to store and disseminate data, nor do we worry that the data will be inaccessible. Fortunately, with the emergence and development of Bitcoin [10], as a decentralized and self-organized cryptocurrency, its underlying technology blockchain can elegantly help us realize such a data security sharing scheme [11–14]. In this paper, we proposed a data-sharing scheme based on blockchain. The main contributions of this paper are as follows:

- (1) A user-centric data security sharing scheme named BSSPD is proposed, which combines blockchain, CP-ABE, and IPFS. The data owner encrypts his sharing data and stores it on IPFS to maximize decentralization, and BSSPD allows the data owners to have fine-grained access control over their data. Moreover, it supports revoking permissions of a specific data user at an attribute level without affecting others
- (2) In BSSPD, the data owner publishes data-related information and distributes decryption keys for data users through the blockchain. To avoid denial of service attacks, data users need to complete a proof of

work (PoW) before registering, which is similar to the mining process of Bitcoin, and the data owner can adjust the target of PoW according to the number of data users in the system

- (3) BSSPD sets ciphertext keyword indices for each data-related data user. Combined with CP-ABE, it further prevents the privacy disclosure that data labels may cause to the data owner and protects the data user's privacy during retrieval
- (4) We experimented with our scheme on the EOS blockchain and provided the detailed implementation of algorithms and Smart Contracts. Together with the security analysis, it proved that our scheme is feasible
- (5) We used five MacBooks to build an EOS private chain in the laboratory environment and simulated our scheme. Analysis of storage and computing overhead proved that BSSPD has a good performance

The rest of this paper is organized as follows. Section 2 consists of related works. Section 3 reviews some preliminary knowledge used throughout this paper. In Section 4, we have an overview of our scheme. Specific implementation details are described in Section 5. Security and performance analysis are discussed in Section 6. Finally, the conclusion and future direction are presented.

## 2. Related Work

As early as 2015, Swan pointed out that there was not yet an acceptable "health data common" model [15] with appropriate privacy and reward systems for public sharing of personal health data and quantified self-tracking data. Simultaneously, the author believes that blockchain can precisely provide such a structure for creating a secure, remunerated, and owner-controlled health data sharing. Zyskind et al. described a distributed personal data management system [16] that ensures users own and control their data. The system encrypts the data collected from the user's mobile phone and stores it off-chain and only stores the data's hash value on the blockchain. Meanwhile, two acceptable transaction types named *Taccess* and *Tdata* are defined, in which *Taccess* is used to implement access control management, and *Tdata* is used for data storage and retrieval. Azaria et al. proposed MedRec system [17], a blockchain-based decentralized record management system for electronic medical records (EMRs). MedRec provides patients with a comprehensive and immutable log, and the patients can access their medical information at any time across providers and locations. However, the system implements permissionless blockchain with PoW consensus, lacking data security, data privacy, and throughput. Xia et al. proposed MeDShare [18], a system that solves the problem of sharing medical data in a trustless environment by custodians of medical big data. Dubovitskaya et al. have proposed a framework for managing and sharing EMR data for cancer patient care [19]. It uses a permission chain to maintain metadata and access control

policies and uses cloud services to store the encrypted data. Patients can define their access control policies to ensure data security and availability. The above-mentioned data-sharing schemes based on blockchain give an ideal blueprint, but most of them only describe the scheme's outline and do not provide the implementation details of the required protocol.

In the following years, many researchers have designed and implemented more robust access control protocols on blockchain to protect data privacy and security during sharing. Liang et al. used the consortium chain Hyperledger Fabric to realize a user-centric health data-sharing model [20] in which the cloud storage is used as a data warehouse and the blockchain ledger is constructed to store operations such as query and update. At the same time, it uses the member management service provided by Hyperledger Fabric to strengthen the users' identity authentication and the channel model to protect users' privacy. Fan et al. focused their attention on mobile network data sharing and privacy protection in the 5G era and proposed an efficient sharing scheme based on blockchain [21]. The main idea is to define a transaction format on blockchain to represent an access strategy. The strategy includes access requestor, content provider, visitor, and the beginning and ending time of access allowed, which is a role-based access control model. Zhang et al. proposed a blockchain-based data-sharing scheme for AI-powered network operations [22]. The scheme sets up two different types of chain, in which DataChain is used as access control tools for data, and BehaviorChain is used to store access records and ensure they cannot be tampered with. They divide access permissions into four levels. Zhou et al. proposed a blockchain-based file-sharing system [23] to address inefficient file sharing during the review of academic papers. The scheme uses Access Control Language (ALC) to exercise access control over the information stored on-chain. It needs to define an access policy on the blockchain for each pair of users and resource. Patel proposed a crossdomain image-sharing framework based on blockchain [24], which uses blockchain as data storage and allows patients to define an access policy. They pointed out that this approach can protect the data from unrelated parties, but no research has been conducted on privacy and security. Tan et al. have proposed a blockchain-based access control scheme for Cyber-Physical Social System (CPSS) big data [25], called BacCPSS. BacCPSS uses an address of blockchain as the user's identity and maintains a user access matrix on the Smart Contract, ensuring that only operations authorized in the access matrix can be performed. The access control methods implemented in the above data-sharing schemes either need to maintain large numbers of access rules on the chain or cannot achieve fine-grained access control. Neither the access control matrix nor the RBAC is suitable for distributed environments like blockchain.

ABE is considered the most appropriate technology to solve data security and privacy protection problems in a distributed environment. Therefore, recently, researchers have used ABE to achieve fine-grained access control over data on the blockchain. Jemel and Serhrouchni proposed a decentralized access control mechanism [26]. For the first time, researchers used blockchain nodes to execute a CP-ABE

algorithm to verify user access rights' legitimacy. The scheme designs two types of transactions: *SetPolicy* and *GetAccess*. But it does not use Smart Contracts, and it is obvious that the scheme is unable to achieve more complex requirements. Sun et al. constructed a model of secure storage and effective sharing for electronic medical data based on ABE and blockchain [27], which provides better access control. Doctors use ABE to encrypt patients' medical data and store it on IPFS. However, it also does not use Smart Contracts. It only broadcasts some ABE parameters stored in transactions, which cannot achieve more complex business functions. Wang et al. proposed a sharing scheme [28] in which users distribute secret keys. It realizes that the data owner has a fine-grained access control on his data. At the same time, the Ethereum Smart Contract is used to realize the retrieval of ciphertext keywords. However, it requires multiple off-chain communication between users, and more importantly, it does not implement the permit revocation. Pournaghi et al. proposed a secure and efficient sharing scheme based on blockchain and ABE entitled MedSBA to record and store medical data [29]. It implements the update and revocation of permissions by broadcasting a new strategy to cover the previous transaction, but this will lead to users who do not want to be revoked to update their keys.

### 3. Preliminary

**3.1. Bilinear Groups of Composite Order.** Let  $n = p_1 p_2$  ( $p_1$  and  $p_2$  are distinct primes),  $G_1$  and  $G_2$  be cyclic groups of order  $n$ , and  $g$  be a generator of  $G_1$ . We call  $e : G_1 \times G_1 \rightarrow G_2$  as a bilinear pairing, if it is a map with the following properties:

- (1) Bilinear:  $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$  for all  $g_1, g_2 \in G_1$  and  $a, b \in \mathbb{Z}$
- (2) Nondegenerate: there exists  $g_1, g_2 \in G_1$ , such that  $e(g_1, g_2) \neq 1$
- (3) Computable: There is an efficient algorithm to compute  $e(g_1, g_2) \neq 1$  for all  $g_1, g_2 \in G_1$

Let  $G_{p_1}$  and  $G_{p_2}$  denote the subgroups of  $G_1$  with order  $p_1$  and  $p_2$ . Then,  $G_1 = G_{p_1} \times G_{p_2}$ ;  $g^{p_2}$  and  $g^{p_1}$  are the generators of  $G_{p_1}$  and  $G_{p_2}$ . Let  $g_1$  and  $g_2$  denote the generators of  $G_{p_1}$  and  $G_{p_2}$ . For all random elements  $h_1 \in G_{p_1}$  and  $h_2 \in G_{p_2}$ , then we have  $e(h_1, h_2) = 1$ ; because of that,  $e(h_1, h_2) = e(g_1^a, g_2^b) = e(g^{ap_2}, g^{bp_1}) = e(g, g)^{abp_1 p_2}$ .

**3.2. Linear Secret-Sharing Scheme (LSSS).** Let  $P = \{P_1, \dots, P_n\}$  be a set of parties, and  $(A, \rho)$  denote an access structure in which  $A$  is an  $l \times k$  access matrix with  $\rho$  mapping its rows. A linear secret-sharing scheme (LSSS) consists of two polynomial-time algorithms:

- (1) *Share*( $A, \rho$ ): to share a secret value  $s$ , it randomly chooses  $v_1, v_2, \dots, v_{k-1} \in \mathbb{Z}$  and let  $\mathbf{v} = (s, v_1, \dots, v_{k-1})^T$ . Let  $A_i$  denote the vector as the  $i$ th



row in matrix  $A$ , and then, the share  $\sigma_i = A_i \mathbf{v}$  belongs to party  $\rho(i)$

- (2)  $\text{Re } \text{con}(A, \rho)$ : the algorithm takes  $\omega \in A$  as input; let  $L \in \{i \mid \rho(i) \in \omega\}$ . Then, a set of recovery coefficients can be calculated effectively according to  $\{\mu_i\}_{i \in L}$ , so that  $\sum_{i \in L} \mu_i \sigma_i = s$ . Research has shown that the monotonic access structure is equivalent to the LSSS. Let  $(A, \rho)$  be an access structure and  $\omega$  be a set of authorization; then  $\exists \{\mu_i\}_{i \in L}$  makes that  $\sum_{i \in L} \mu_i \sigma_i = s$ . For unauthorized sets, such constants do not exist

**3.3. Ciphertext-Policy Attribute-Based Encryption (CP-ABE).** The CP-ABE mechanism was proposed by Bethencourt et al. [30]. It is a public key encryption scheme, but unlike RSA and ECC, CP-ABE is a one-to-many encryption scheme. In CP-ABE, the user's attributes correspond to the private key, and the access policy is embedded in the ciphertext [31]. Only when the decryption user's attributes satisfy the access policy can the data be decrypted. CP-ABE is mostly used for fine-grained access control. CP-ABE consists of four phases: initialization, key generation, encryption, and decryption, corresponding to the following four algorithms:

- (1)  $\text{Setup}(\lambda, S) \rightarrow (PSK, MSK)$

Initialization algorithm is a randomization algorithm, which is generally executed on a trusted key distribution center. The algorithm inputs a secure parameter  $\lambda$  and the attributes are set  $S$ , to generate the system public key  $PSK$  and the system master key  $MSK$ .

- (2)  $\text{KeyGen}(PSK, MSK, \omega) \rightarrow USK$

Key generation algorithm generates a private key  $USK$  for the data user according to the system public key  $PSK$ , the system master key  $MSK$ , and the data user's attributes  $\omega$ .

- (3)  $\text{Encrypt}(PSK, M, A) \rightarrow CM$

Encryption algorithm is executed by the data owner. The algorithm inputs the system public key  $PSK$ , the message  $M$  to be encrypted, and the access control structure  $A$  associated with the access policy and outputs the ciphertext  $CM$ .

- (4)  $\text{Decrypt}(PSK, CM, USK) \rightarrow M$

Decryption algorithm is executed by the data user. The inputs of the algorithm are the system public key  $PSK$ , the user's private key  $USK$ , and the ciphertext  $CM$ . If the data user's attribute set  $\omega$  satisfies the access policy, he will decrypt the ciphertext and obtain the corresponding plaintext  $M$ .

**3.4. Blockchain.** A blockchain concept originated from Nakamoto's Bitcoin paper [10], and it is based on cryptography and P2P network. The data on the blockchain is organized into blocks, which are chained in a particular chronological order. Cryptography and consensus mechanisms ensure the security and nonforgery of data. In short, as the underlying technology of cryptocurrencies like Bitcoin, blockchain is a distributed trusted ledger that cannot be tampered with.

**3.4.1. Smart Contract.** At the early stage of blockchain development, only cryptocurrencies like BTC and LTC were more successful applications. In 2013, Buterin introduced the concept of Smart Contract in his Ethereum white paper [32], demonstrating the first public blockchain with a built-in Turing complete language. Smart Contract [33] was defined as "a computerized transaction protocol that executes the terms of the contract." In the blockchain, Smart Contract is a code that relies on blockchain's trusted environment to automatically execute while enabling the blockchain to realize a more complex business. The smart contract operation mechanism based on blockchain is shown in Figure 1.

From a higher point of view, blockchain can be considered a state machine triggered by transactions, and its public ledger is a world state starting from the Genesis Block. Users can build a transaction and broadcast it from any node in the blockchain network. All block producers will perform the corresponding operation after receiving the transaction. Because of the consensus mechanism, all nodes will eventually get a consistent result and update the world state. The action triggered by a transaction can be to deploy a new Smart Contract or to invoke a Smart Contract from blockchain and execute it in a sandbox environment. Blockchain provides Smart Contract with the following capabilities:

*Public state:* everyone can see the Smart Contract's execution and its current global status on the public ledger, which cannot be tampered with.

*Trusted propagation channel:* after encrypting the message by the receiver's public key, the sender can broadcast the message through the blockchain. The receiver will receive the message, and it will be recorded on the blockchain securely and undeniably.

**3.4.2. Transaction of EOS.** In the EOS blockchain, there are three essential components named address, account, and transaction. Each user has his account in EOS, and each account corresponds to multiple ECDSA key pairs denoted by  $(pk, sk)$ . The public key calculates an address of EOS through a hash function and base58 coding. The private key and the public key are used to sign and verify the transaction, respectively. If a user wants to invoke a Smart Contract on-chain, he needs to prepare such a transaction  $Tx$  [34]:

$$Tx = (\text{Ref}_{\text{block}}, t, \text{Sig}_u(\text{Chain\_ID}, Tx), \text{Action}(\text{Code}, \text{Name}, \text{Auth}_u, \text{Data})). \quad (1)$$

$\text{Ref}_{\text{block}}$  denotes the reference to the block number and header of a block which generated recently to prevent transactions from appearing on a forked chain.  $\text{Sig}_u(\text{Chain\_ID}, Tx)$  denotes the user's signature information on the transaction which is used to verify the identity of the user who initiated the transaction by his public key.  $\text{Action}$  represents the operation to be performed, where  $\text{Code}$  is the name of the Smart Contract to be invoked,  $\text{Name}$  is a method in Smart Contract to be called,  $\text{Auth}_u$  is used to verify whether the user who initiated the transaction has the permission, and  $\text{Data}$  is the parameters to be passed into the contract.

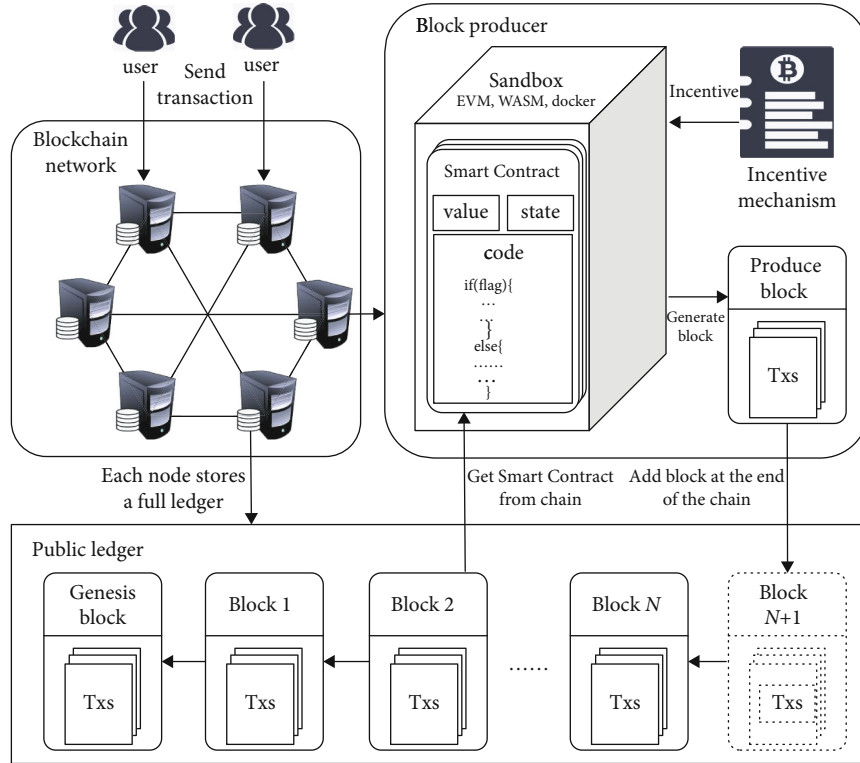


FIGURE 1: The operation mechanism of smart contract on blockchain.

3.4.3. *Data Persistence of EOS.* After the Smart Contract is executed, the occupied memory will be released, and all variable data in the program will be lost, so it is necessary to persist the data in Smart Contract. In the Smart Contract of Ethereum, data can only be stored in key-value pairs, which is difficult to meet more complex requirements. In EOS, it imitates Multiindex Containers in Boost library and develops a C++ class: *eosio::multi\_index* (hereinafter referred to as *multi\_index*). Each *multi\_index* can be regarded as a table in the traditional database. Each row of the table can store an object, and the object's attributes can be any C++ data type. Therefore, the table constructed by *multi\_index* in EOS is no less flexible than traditional databases. A significant feature of *multi\_index* is that a primary key can be set as the main index and 16 secondary indices. Users can obtain any of these indices and use the *emplace*, *erase*, *modify*, and *find* functions of the index to insert, delete, update, and select data.

3.5. *IPFS (InterPlanetary File System).* The InterPlanetary File System is a globally oriented, point-to-point distributed version of the File System, dedicated to creating persistent and distributed storage and shared file network transmission protocols. By integrating existing technologies such as BitTorrent, DHT, Git, and SFS (self-certifying File System), IPFS provides a high-throughput content block storage model that contains content addressing hyperlinks. Simultaneously, it does not have a single point of failure, and the nodes in the system do not need to trust each other. Any resource, such as text, images, sound, video, and website code, once added to the IPFS network, computes the content

to a uniquely encrypted hash value unique to the address. This address can be understood as a URL (Uniform Resource Locator) on the Web. If the user wants to use the file, they just need to go to this address to get them.

#### 4. Overview of Our Scheme

This section will give an overview of the system model and the design of our proposed scheme. Table 1 shows some symbols and abbreviations involved in this paper.

4.1. *System Model of BSSPD.* Our proposed scheme BSSPD consists of four components: IPFS, blockchain, data owner, and data user. The *DO* encrypts his data and uploads it to IPFS, then invokes the Smart Contract on blockchain to save the returned address along with the decryption key. CP-ABE is used to realize a fine-grained access control of data. The *DO* distributes the private keys for *DUs* through blockchain, and only those who satisfy the access policy can download and decrypt the shared data. The whole process is entirely decentralized. The data is encrypted and stored in the IPFS to ensure the security of data and accessibility. The traces of the *DO* and *DUs* are stored on the blockchain, which cannot be tampered with or denied. The specific functions and responsibilities of these four parts are as follows:

- (1) IPFS: provide a secure and reliable storage service. The incentive mechanism ensures that the data on IPFS will never be unavailable
- (2) Blockchain: stores the public information and operational records in the whole scheme. Meanwhile, it can

TABLE 1: The symbols and abbreviations involved in this paper.

No.	Symbol	Description
1	$DO$	The data owner
2	$DU$	The data user
3	$MSK$	System master key
4	$PK$	System public parameters
5	$S$	All general attributes set
6	$\omega$	The attributes set of a specific $DU$
7	$\mathcal{P}$	Access policy
8	$uid$	A user ID which is unique
9	$SK_{uid,\omega}$	The attribute private key of $DU$ whose ID is $uid$
10	$SK_{search}$	The secret key of $DU$ for search
11	$E = (E.Enc, E.Dec)$	An asymmetric encryption algorithm like ECC
12	$(SK_{com}, PK_{com})$	A pair of keys for algorithm $E$
13	$\varepsilon = (\varepsilon.Enc, \varepsilon.Dec)$	A symmetric encryption algorithm like AES
14	$F$	Data that the $DO$ intends to share
15	$CF$	Ciphertext of the data $F$
16	$href_{location}$	The address where the data is stored on IPFS
17	$kw$	Keyword
18	$t_{kw}$	Search token of $kw$

be used as a reliable broadcast channel for transferring messages from the  $DO$  to  $DU$ . Without any trusted third party, it is the cornerstone of trust for the scheme. There are two Smart Contracts in BSSPD.  $UMContract$  is used to manage data users and  $DSContract$  is used to share data

- (3) Data owner: responsible for creating and deploying the Smart Contract in the scheme. The  $DO$  can publish his sharing data and set an access policy for it. Meanwhile, the  $DO$  can grant and revoke a  $DU$ 's access rights
- (4) Data user: the  $DU$  is the person who wants to access the shared data. When  $DU$ 's attributes meet the policy embedded in the ciphertext, he will decrypt the address and key to obtain the shared data

The system model of the proposed scheme is shown in Figure 2.

The CP-ABE algorithm we adopted was mainly inspired by [35] and extended to use the user's ID as an attribute to support permission revocation. The keyword ciphertext search in BSSPD was learned from [36]. The corresponding description of each step number in Figure 2 is shown as follows:

- (i) The  $DO$  creates and deploys Smart Contracts. There are two Smart Contracts in our scheme.  $UMContract$  includes the functions of user registration, attribute management, identity management, and authentication.  $DSContract$  includes publishing sharing data, updating access policy, permission revocation, and data retrieval

- (ii) The  $DO$  generates the system master key and system public key locally and stores the system public key in  $DSContract$
- (iii) The  $DU$  invokes  $UMContract$  to apply for registration, and he needs to provide his account of EOS and a public key. The public key is used to communicate with the  $DO$ , and the  $DO$  uses it to encrypt the message and broadcasts the ciphertext to the blockchain. Only the corresponding  $DU$  can decrypt the ciphertext and obtain the message
- (iv) The  $DO$  assigns a unique  $uid$  to each  $DU$  who applies for, and generates a private attribute key and a secret search key for the  $DU$ . After encrypting these two keys with the  $DU$ 's communication public key, the  $DO$  will save them in the Smart Contract together with the  $uid$
- (v) The  $DU$  obtains the ciphertext information of the keys and decrypts them with his private communication key
- (vi) The  $DO$  randomly selects a key of the symmetric encryption algorithm, uses it to encrypt the sharing data, then uploads the ciphertext to the IPFS network, and IPFS returns an address
- (vii) The  $DO$  sets an access policy for sharing data and sets a revocation list for each attribute in the policy, then encrypts the address along with the decryption key of shared data. The  $DUs$  in the revocation list do not have corresponding attributes when accessing the data

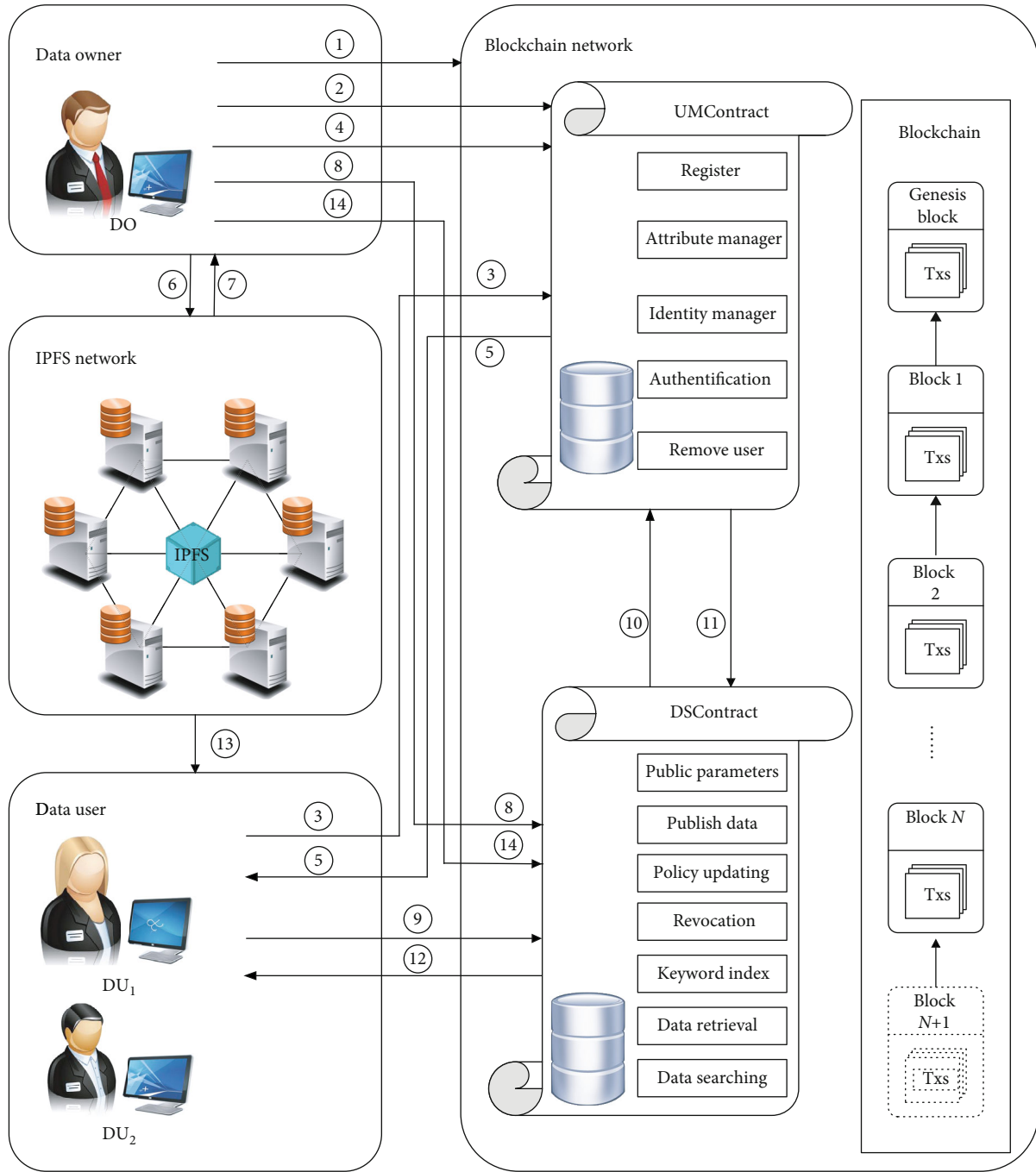


FIGURE 2: The system model of BSSPD.

- (viii) The *DO* selects keywords to generate ciphertext indices for data-related *DUs* and then invokes the *DSContract* to store the indices and data-related information
- (ix) The *DU* selects a keyword of the data to be retrieved and uses the trapdoor function to generate a search token
- (x) The *DU* invokes *DSContract* to start searching for the desired data. *DSContract* will call *UMContract* to authenticate the *DU* and check whether the *DU* is legal
- (xi) *UMContract* returns the authentication result to *DSContract*. If the *DU* is legal, the search function will continue to be executed
- (xii) The *DU* obtains the search results from *DSContract*
- (xiii) The *DU* uses his attribute private key to decrypt the acquired data-related information. If the *DU*'s unrevoked attributes still satisfy the access policy, he will get the address where the ciphertext data is stored on IPFS and the corresponding decryption key. The *DU* can download the ciphertext of the shared data from IPFS and decrypt it



- (xiv) If the *DO* wants to revoke a *DU*'s attribute *A* to a certain shared data, he can add this *DU*'s *uid* to the revocation list of attribute *A*. Then, the *DO* will generate a new ciphertext and invoke *DSContract* to update the data-related information

**4.2. Detail Design of BSSPD.** The scheme we proposed is mainly composed of the following phases: initialization phase, apply and register phase, encryption and uploading phase, search phase, decryption and downloading phase, and permission revocation phase. This section will describe the detailed design of each phase and the corresponding relationship with the process steps in the previous section.

**4.2.1. Initialization Phase.** The primary function of the initialization phase is that the *DO* deploys Smart Contracts, then generates the system master key and the public parameters in the scheme, and stores them in the Smart Contract. The core algorithm of this phase is  $Setup(1^\lambda) \rightarrow (MSK, PK)$ , which was executed by the *DO*. The algorithm's input is a security parameter  $1^\lambda$ , and the outputs are the system master key *MSK* and public system parameters *PK*. *MSK* will be kept secret by the *DO*, and *PK* will be stored in *UMContract* by the *DO* initiating a transaction. The corresponding steps in the system flowchart are (i) and (ii).

**4.2.2. Apply and Register Phase.** The apply and register phase's primary function is that the *DU* invokes to apply for registration, and an asymmetric encryption algorithm public key is required when applying. After that, the *DO* assigns a unique *uid* and distributes private keys for the *DU*. The core algorithm is  $KeyGen(MSK, PK, uid, \omega) \rightarrow (SK_{data}, SK_{search})$  which is run by the *DO*. The inputs of the algorithm are the system master key *MSK*, the public parameters *PK*, the *uid* of the *DU*, and the general attribute set  $\omega$  of the *DU*. It outputs the private attribute key  $SK_{data}$  and the search key  $SK_{search}$  of the *DU*. The *DO* executes  $SK_{uid, \omega} = Enc_{PK_{com}}(SK_{data} | SK_{search})$  and invokes *UMContract* to store  $SK_{uid, \omega}$  in the Smart Contract. In this way, the *DU* can obtain his private keys securely and reliably. The corresponding steps in the system flowchart are (iii)–(v).

**4.2.3. Encryption and Uploading Phase.** The encryption and uploading phase's main function is that the *DO* encrypts sharing data and uploads it to IPFS. After that, the address and decryption key are encrypted and uploaded to *DSContract*, and the ciphertext keyword indices are established for the relevant *DUs*. The core algorithm is  $Encrypt(F, (A_{pk}, \rho), \{R_{\rho(x)}\}_{x \in \{1, \dots, l\}}, PK)$  and executed by the *DO*. It consists of the following three substeps:

**Step 1.  $EncryptFile(F) \rightarrow (K_F, href_{location})$ .**

The input of the data encryption algorithm is the sharing data *F*, and outputs are the key  $K_F$  of a symmetric encryption algorithm and an IPFS address  $href_{location}$ . The whole process is to randomly select a private key  $K_F$  and encrypt *F* to get the ciphertext *CF* and then upload *CF* to IPFS to get the

address  $href_{location}$ . The corresponding step in the system flowchart is (vi).

**Step 2.  $EncryptKey(K_F, href_{location}, \mathcal{P}, \{R_i\}_{i \in \mathcal{P}}, PK)_{(K_F | href_{location})}$ .**

The algorithm is used to encrypt the address, and the key whose inputs are the decryption key  $K_F$ , the IPFS address  $href_{location}$ , the access policy  $\mathcal{P}$ , a revocation list  $R_i$  for each attribute in  $\mathcal{P}$ , and system public parameters *PK*. Its output is the ciphertext of  $K_F$  and encrypted with CP-ABE. The corresponding step in the system flowchart is (vii).

**Step 3.  $IndexGen(kw, K_{search}) \rightarrow t_{kw}$ .**

In the algorithm that generates the ciphertext keyword index, the *DO* selects a keyword *kw* of data *F*, which is used as inputs together with the search secret key  $K_{search}$  of a relevant *DU*. The output is a search token  $t_{kw}$  and the corresponding step in the system flowchart is (viii).

**4.2.4. Search Phase.** The main function of the search phase is that a *DU* uses the trapdoor function to generate the corresponding search token according to the keyword of the shared data which he wants. After that, the *DU* invokes the contract *DSContract* for retrieval. This phase can be divided into two steps, as follows:

**Step 1.  $Trpdr(kw', SK_{search}) \rightarrow t'_{kw}$ .**

Generate search token algorithm, which is executed by the *DU*. The *DU* selects the keyword related to the shared data he wants to search, together with his  $SK_{search}$  as inputs, and the output is the search token  $t'_{kw}$  corresponding to the keyword. This corresponds to step (ix) in the system flowchart.

**Step 2.  $Search(t'_{kw}) \rightarrow CT_{(K_F | href_{location})}$ .**

The search algorithm is executed by *DSContract*, which uses the search token  $t'_{kw}$  generated by the *DU* in the previous step as input. If such data exists, the algorithm returns data-related information successfully. In this algorithm, the *DU* sends a transaction to *DSContract* to trigger the execution, corresponding to steps (x)–(xii).

**4.2.5. Decryption and Downloading Phase.** The main function of the decryption and downloading phase is that *DUs* use their attribute private keys to decrypt the data-related information to obtain the address where the shared data stored on IPFS and the decryption key. The core algorithm is  $Decrypt(SK_{uid, \omega}, CT_{(K_F | href_{location})}, PK) \rightarrow (K_F, href_{location})$  which was executed by the *DU*. The inputs of the algorithm are the private attribute key  $SK_{uid, \omega}$  of the *DU*, the data-related information  $CT_{(K_F | href_{location})}$ , and the public system parameters *PK*. It outputs the decryption key  $K_F$  and the address  $href_{location}$ . Because the access policy  $\mathcal{P}$  and the revocation



list  $R_i$  of each attribute are embedded in the ciphertext, if the attribute set of the  $DU$  that have not been revoked still satisfies access policy  $\mathcal{P}$ , he will decrypt and obtain  $K_F$  and  $href_{location}$  successfully. In this way, the  $DU$  could download  $CT_F$  from IPFS and decrypt it to obtain the data  $F$ . This corresponds to step (xiii) in the system flowchart.

**4.2.6. Permission Revocation Phase.** The main function of the permission revocation phase is that the  $DO$  performs an attribute-level fine-grained permission revocation to a  $DU$  on a certain ciphertext. At the same time, it does not need to update the keys of other  $DUs$  related to the ciphertext. The core algorithm of this phase is  $Revoke(K_F, href_{location}, \mathcal{P}, \{R_i\}_{i \in \mathcal{P}}, PK, i, uid) \rightarrow CT'_{(K_F|href_{location})}$  which is run by the  $DO$ . This is similar to the encryption algorithm, but a  $DU$ 's  $uid$  and the attribute  $i$  to be revoked are added to the parameters. The algorithm will add  $uid$  to the revocation list  $R_i$  and output a new ciphertext. The  $DO$  sends a transaction to  $DSContract$  to update the data-related information. In this way, if the remaining attribute set of the  $DU$  cannot satisfy the policy  $P$ , he can no longer decrypt the data after obtaining the ciphertext, while other  $DUs$  are not affected. This corresponds to step (xiv) in the system flowchart.

## 5. Implementation Details of Our Scheme

In order to achieve our goal, we will construct a CP-ABE which supports permission revocation and combine it with the EOS blockchain to implement our scheme. This section will elaborate on the details of our Smart Contracts deployed on EOS blockchain and concrete construction of BSSPD.

**5.1. Smart Contract Design.** To make the logic clearer, we divide the Smart Contract in the scheme into two parts:  $UMContract$  and  $DSContract$ .  $UMContract$  is used to manage  $DUs$ ' identity, while  $DSContract$  is used to handle business operations related to data sharing. In the contract, we will use  $_self$  to represent the account of the  $DO$  who created the contract. We will describe the detailed design of these two contracts.

**5.1.1. User Management Contract ( $UMContract$ ).** The  $UMContract$  is composed of five function interfaces:  $SetTarget$ ,  $GetUserByUid$ ,  $Apply$ ,  $Register$ , and  $Authenticate$ . We initialize  $UMContract$  as follows.

Let three-tuple  $(A, uid, Pk_{com})$  denote a  $DU$ , and create a multi\_index named  $table\_user$  for it in which  $A$  is an EOS account of the  $DU$ ,  $uid$  is the unique ID assigned by the  $DO$ , and  $Pk_{com}$  is a public key of the  $DU$  used for communication with the  $DO$ . Let  $A$  be the primary key of  $table\_user$  whose corresponding index is  $account\_idx$ . Let  $uid\_idx$  be a secondary index corresponding to  $uid$ . Let  $target$  be the target value of PoW.

- (1) **SetTarget:** when  $UMContract$  receives action ( $UMContract$ , SetTarget, Auth, ( $newTarget$ )), this function interface will be triggered to execute. It can only be invoked by the  $DO$  who created the contract to adjust the difficulty of PoW. When there are too

```

Input: newTarget
Output: bool
1 if msg.sender is not _self then
2   throw;
3 else
4   target = newTarget;
5   return true;
6 end

```

ALGORITHM 1: SetTarget.

many users in the system, the  $DO$  can increase the difficulty of PoW

- (2) **GetUserUid:** when  $UMContract$  receives action ( $UMContract$ , GetUserByUid, Auth, ( $account$ )), this function interface will be triggered to execute. It is used to get all the information of a  $DU$  according to his  $uid$  and can only be invoked by the  $DO$  who created the contract
- (3) **Apply:** when  $UMContract$  receives action ( $UMContract$ , Apply, Auth, ( $from, pk, nonce$ )), this function interface will be triggered to execute. It is invoked by the  $DU$  to apply for registration in the system
- (4) **Register:** when  $UMContract$  receives action ( $UMContract$ , Register, Auth, ( $account, id$ )), this function interface will be triggered to execute. It is used to complete the registration of a  $DU$  and can only be invoked by the creator of the contract
- (5) **Authenticate:** when  $UMContract$  receives action ( $UMContract$ , Authenticate, Auth, ( $from, method, account, id, args$ )), this function interface will be triggered to execute. It is used to authenticate the identity of a  $DU$ , which is invoked by another contract and returns the result to the invoker

**5.1.2. Data Sharing Contract ( $DSContract$ ).** The  $DSContract$  is composed of six function interfaces:  $SetPK$ ,  $SetSK$ ,  $AddData$ ,  $PolicyUpdate$ ,  $Search$  and  $EndSearch$ , and  $Remove$ . We initialize  $DSContract$  as follows.

Let  $PK$  denote the system public parameters. Let two-tuple  $(A, SK)$  be the corresponding relationship between the  $DU$ 's account and his attribute private key, and the multi\_index  $table\_sk$  is created for it. Let  $A$  be the primary key of  $table\_sk$  whose corresponding index is  $ua\_idx$ . Let two-tuple  $(fid, cf)$  denote the shared data in which  $fid$  is the id of shared data and  $cf$  is the data-related information. Then, create a multi\_index  $data\_table$  for it, where  $fid$  is the primary key and  $fid\_idx$  is the corresponding index. Let four-tuple  $(id, A, t, fid)$  be an index of  $DU$  related to shared data in which  $A$  is the EOS account of  $DU$ ,  $t$  is the search token, and  $fid$  is the id of shared data in  $data\_table$ , then create a multi\_index  $search\_table$  for it. Let  $sa\_idx$ ,  $t\_idx$ ,  $sf\_idx$  be the secondary indices of  $search\_table$ , corresponding to  $A$ ,  $t$ , and  $fid$ , respectively.

```

Input: uid
Output: all information of DU
1 if msg.sender is not _self then
2   throw;
3 else
4   user_row = uid_idx.find(uid);
5   return user_row;
6 end

```

ALGORITHM 2: GetUserByUid.

```

Input: from, pk, nonce
Output: bool
1 u = account_idx.find(from)
2 if u != null then
3   u.Pkcom = pk;
   account_idx.modify(u);
4   return true;
5 else
6   pow = SHA256(SHA256(from | pk | nonce));
7   if pow > target then
8     return false;
9   else
10    u.A = from;
11    u.Pkcom = pk;
12    account_idx.emplace(u);
13    return true;
14  end
15 end

```

ALGORITHM 3: Apply.

```

Input: account, id
Output: bool
1 if msg.sender is not _self then
2   throw;
3 else
4   u = account_idx.find(account);
5   if u == null then
6     return false;
7   else
8     u.uid = id;
9     account_idx.modify(u);
10    return true;
11  end
12 end
13 end

```

ALGORITHM 4: Register.

- (1) *SetPK*: when *DSContract* receives action (*DSContract*, *SetPK*, *Auth*, (*newPk*)), this function interface will be triggered to execute. It can only be invoked by the *DO* to set and update the system public parameters
- (2) *SetSK*: when *DSContract* receives action (*DSContract*, *SetSK*, *Auth*, (*account, sk*)), this function interface will be triggered to execute. It can only be invoked

```

Input: from, method, account, id, args
Output: null
u = account_idx.find(account)
1 if u != null then
2   if u.id == id then
3     send action (from, method, (_self, true, args));
4   else
5     send action (from, method, (_self, false, args));
6   end
7 else
8   send action (from, method, (_self, false, args));
9 end

```

ALGORITHM 5: Authenticate.

by the *DO* to set and update the private keys of the *DU*

- (3) *AddData*: when *DSContract* receives action (*DSContract*, *AddData*, *Auth*, (*account, t<sub>kw</sub>, CT<sub>(K<sub>F</sub>|href<sub>location</sub>)</sub>*)), this function interface will be triggered to execute. It is used to publish the sharing data and add the indices for the relevant *DUs*. There can be multiple index relationships. For clarity, we only add an index for one *DU* here. It can only be invoked by the *DO*
- (4) *PolicyUpdate*: when *DSContract* receives action (*DSContract*, *PolicyUpdate*, *Auth*, (*fid, CT<sub>(K<sub>F</sub>|href<sub>location</sub>)</sub>*)), this function interface will be triggered to execute. It can only be invoked by the *DO* and used to update the access policy for a certain shared data. In this way, the *DO* can revoke the access permission of a *DU* to this shared data
- (5) *Search* and *EndSearch*: when *DSContract* receives action (*DSContract*, *Search*, *Auth*, (*from, uid, t<sub>kw</sub>*)), this function interface will be triggered to execute. These two function interfaces work together to complete the retrieval of shared data. Because we have divided BSSPD into two contracts, it needs to invoke *UMContract* to verify the identity of the *DU* during the retrieval
- (6) *Remove*: when *DSContract* receives action (*DSContract*, *Remove*, *Auth*, (*fid*)), this function interface will be triggered to execute. It is used to remove a shared data and the search indices related to this data. It can only be invoked by the *DO*

5.2. *Concrete Construction of BSSPD*. In this section, we will show the concrete construction of our scheme, including the algorithms that the *DO* and *DUs* need to execute at each phase and their interactions with the EOS blockchain. Our initialization is as follows.

Let  $N = p_1 p_2$  ( $p_1$  and  $p_2$  are distinct primes)  $G_1$  and  $G_2$  be cyclic groups of order  $N$ . Let  $G_{p_1}$  and  $G_{p_2}$  denote the subgroups of  $G_1$  with order  $g$  and  $Y$ . Let  $e : G_1 \times G_1 \rightarrow G_2$  be a

bilinear pairing and  $I = \{1, \dots, m\}$  be the set of all attributes. Let  $F$  be a pseudorandom function, where  $F : \{0, 1\}^k \times \{0, 1\}^* \rightarrow \{0, 1\}^k$ , and  $U = \{uid_1, \dots, uid_n\}$  be the  $uid$  set of all  $DU$ s obtained from  $UMContract$ .

(1)  $setup(1^\lambda, I)$

For each attribute  $\{i \mid i \in I\}$ , the algorithm first randomly picks two elements  $t_i, \gamma_i \in Z_{p_1}$  and computes  $T_i = g^{t_i}, h_i \in g^{\gamma_i}$ . Next, it picks  $\alpha, a \in Z_{p_1}$  randomly, then computes  $e(g, g)$ .

The public key is  $PK$ :

$$PK = (N, e(g, g)^\alpha, g, u = g^a, \{T_i = g^{t_i}, h_i \in g^{\gamma_i}\}_{i \in I}). \quad (2)$$

The system master key is  $MSK$ :

$$MSK = (\alpha, a, \{t_i\}_{i \in I}, Y). \quad (3)$$

Among them,  $t_i$  and  $T_i$  are used for calculations related to attributes,  $\gamma_i$  and  $h_i$  are used for calculations related to attribute revocation,  $u$  is used for calculations related to  $DU$ 's identity, and  $Y$  is used for randomization of  $DU$ 's private key.

Then, send the following transaction to EOS blockchain and store the public key in the  $DSContract$ :

$$Tx = (\text{Re } f_{block}, t, \text{Sig}(\text{chain\_id}, Tx), \text{Action}(DSContract, SetPK, Auth_{DO}, (PK))). \quad (4)$$

(2)  $KeyGen(uid, \omega, MSK, PK)$

Firstly, send the following transaction to EOS blockchain to obtain the  $DU$ 's information including  $A, Pk_{com}$ , and  $uid$  from  $UMContract$ :

$$Tx = (\text{Re } f_{block}, t, \text{Sig}_{DO}(\text{chain\_id}, Tx), \text{Action}(UMContract, GetUserByUid, Auth_{DO}, (uid))). \quad (5)$$

After that, the algorithm randomly chooses  $r \in Z_{p_1}$  and computes  $K_0 = g^{a+ar}$ . For each attribute  $i \in \omega$ , randomly pick  $r_i \in Z_{p_1}$  and  $Y_{i,1}, Y_{i,2}, Y_{i,3} \in G_{p_2}$ , then compute the following:

$$\begin{aligned} K_{i,1} &= g^{ar+t_i+r_i+ar_i} Y_{i,1}, \\ K_{i,2} &= g^{r_i} Y_{i,2}, \\ K_{i,3} &= (u^{uid} h_i)^{r_i} Y_{i,3}. \end{aligned} \quad (6)$$

Let  $K_i = \{K_{i,1}, K_{i,2}, K_{i,3}\}$ , then  $DU$ 's attribute private key will be  $SK_{uid,\omega} = (K_0, \{K_i\}_{i \in \omega})$ . As can be seen, the attribute-related part of the private key is embedded with the  $DU$ 's identity.

Then, the algorithm randomly picks a secret key  $SK_{search}$  for search where  $SK_{search} = SK_i \leftarrow \{0, 1\}^\lambda$ . Let  $SK_{uid} = E$ .

```

Input: newPk
Output: bool
1 if msg.sender is not _self then
2   throw;
3 else
4   PK = newPk;
5   return true;
6 end

```

ALGORITHM 6: SetPK.

$Enc_{Pk_{com}}(SK_{uid,\omega} \mid SK_{search})$ , and send the following transaction to set and update the  $DU$ 's private keys:

$$Tx = (\text{Re } f_{block}, t, \text{Sig}_{DO}(\text{chain\_id}, Tx), \text{Action}(DSContract, SetSK, Auth_{DO}, (A, SK_{uid}))). \quad (7)$$

(3)  $Encrypt(F, (A_{l \times k}, \rho), \{R_{\rho(x)}\}_{x \in 1, \dots, l}, PK)$

The algorithm randomly chooses a private key  $K_F$  of  $\varepsilon$ , and encrypts the sharing data  $CF = \varepsilon.Enc_{K_F}(F)$ , then uploads the  $CF$  to the IPFS network, and the returned address is  $href_{location}$ , set  $M = (K_F \mid href_{location})$ .

The algorithm first randomly picks  $s, v_2, \dots, v_k \in Z_{p_1}$  and lets  $\mathbf{v} = (s, v_2, \dots, v_k)^T$ . For  $i = 1$  to  $l$ , it calculates  $\lambda_x = \mathbf{A}_x \cdot \mathbf{v}$  where  $\mathbf{A}_x$  is the vector corresponding to the  $x$ th row of  $\mathbf{A}_{l \times k}$ . Assume that  $R_{\rho(x)} = \{uid_1, \dots, uid_{l_{\rho(x)}}\}$  in which the number of revocable users  $l_{\rho(x)}$  is variable. For each  $uid_j \in R_{\rho(x)}$ , it randomly chooses a  $\eta_{x,j} \in Z_{p_1}$ , where  $j = \{1, 2, \dots, l_{\rho(x)}\}$  and  $\sum_{j=1}^{l_{\rho(x)}} \eta_{x,j}$ , and then computes

$$\begin{aligned} C_0 &= M \cdot e(g, g)^{\alpha s}, \\ C_1 &= g^s. \end{aligned} \quad (8)$$

For each attribute  $\rho(x)$ , it computes that

$$\begin{aligned} C_{x,0} &= g^{\lambda_x}, \\ C_{x,1} &= T_{\rho(x)}^{\lambda_x}. \end{aligned} \quad (9)$$

When  $R_{\rho(x)} \neq \emptyset$ , it computes for each revoked  $uid_j \in R_{\rho(x)}$  as follows:

$$\begin{aligned} C_{x,j,1} &= g^{\eta_{x,j}}, \\ C_{x,j,2} &= (u^{uid_j} h_{\rho(x)})^{\eta_{x,j}}. \end{aligned} \quad (10)$$

```

Input: account, sk
Output: bool
1 if msg.sender is not _self then
2   throw;
3 else
4   u = ua_idx.find(account);
5   if u != null then
6     u.SK = sk;
7     ua_idx.modify(u);
8     return true;
9   else
10    u.A = account;
11    u.SK = sk;
12    ua_idx.emplace(u);
13    return true;
14  end
15 end

```

ALGORITHM 7: SetSK.

```

Input: account, tkw, CT(KF|hreflocation)
Output: bool
1 if msg.sender is not _self then
2   throw;
3 else
4   data_row.cf = CT(KF|hreflocation);
5   data_table.emplace(data_row);
6   search_row.A = account;
7   search_row.t = tkw;
8   search_row.fid = data_row.fid;
9   search_table.emplace(search_row);
10  return true;
11 end

```

ALGORITHM 8: AddData.

```

Input: fid, CT(KF|hreflocation)
Output: bool
1 if msg.sender is not _self then
2   throw;
3 else
4   data_row = data_table.find(fid);
5   if data_row == null then
6     return false;
7   else
8     data_row.cf = CT(KF|hreflocation);
9     data_table.modify(data_row);
10    return true;
11  end
12 end

```

ALGORITHM 9: PolicyUpdate.

The ciphertext  $CF$  is set to

$$CT_{(K_F|href_{location})} = \left( C_0, C_1, \left\{ C_{x,0}, C_{x,1}, \{ C_{x,j,1}, C_{x,j,2} \}_{j=\{1,\dots,l_p(x)\}} \right\}_{x \in \{1,\dots,l\}} \right). \quad (11)$$

$$(4) \text{ IndexGen}(A, kw, K_{search}, CT_{(K_F|href_{location})})$$

The algorithm calculates a search token for a keyword  $kw$  of the sharing data.

$$t_{kw} = F(K_{search}, kw). \quad (12)$$

After that, it will send the following transaction to EOS blockchain to publish the data-related information and add the indices for the relevant DUs:

$$Tx = (\text{Re } f_{block}, t, \text{Sig}_{DO}(\text{chain\_id}, Tx), \text{Action}(DSContract, AddData, Auth_{DO}, (A, t_{kw}, CT_{(K_F|href_{location})}))) \quad (13)$$

$$(5) \text{ Trpdr}(kw', SK_{search})$$

The DU obtains  $SK_{uid}$  from the  $DSContract$  and decrypts it with his own private key.

$$(SK_{uid,\omega} | K_{search}) = E.Dec_{SK_{com}}(SK_{uid}). \quad (14)$$

Then, it calculates the search token corresponding to  $kw'$

$$t'_{kw} = F(K_{search}, kw'). \quad (15)$$

$$(6) \text{ Search}(t'_{kw})$$

Send the following transaction to EOS blockchain:

$$Tx = (\text{Re } f_{block}, t, \text{Sig}_{DU}(\text{chain\_id}, Tx),$$

$$\text{Action}(DSContract, Search, Auth_{DU}, (t'_{kw}))) \quad (16)$$

If the search is successful, the DU will obtain the data-related information  $CT_{(K_F|href_{location})}$ .

$$(7) \text{ Decrypt}(SK_{uid}, CT_{(K_F|href_{location})}, PK)$$

```

Input: from, uid, tkw
Output: data_rows
1 send action (UMContract,Authenticate,Auth,(_self,Search,from,id, tkw))
2 if get false then
3   throw;
4 else
5   t_itr=t_idx.find(tkw);
6   while t_itr != search_table.end() and t_itr.t == tkw and t_itr.A == from
7     data_row=search_table.find(t_itr.fid);
8     data_rows.add(data_row);
9     t_idx++;
10 end
11 return data_rows;
12 end

```

ALGORITHM 10: Search and EndSearch.

```

Input: fid
Output: bool
1 if msg.sender is not _self then
2   return false;
3 else
4   s_itr = sf_idx.find(fid);
5   while s_itr != sf_idx.end() and s_itr.fid == fid
6     sf_idx.erase(s_itr);
7   end
8   data_row = fid_idx.find(fid)
9   fid_idx.erase(data_row)
10 return true;
11 end

```

ALGORITHM 11: Remove.

Let  $L = \{x \mid \rho(x) \in \omega, uid \notin R_{\rho(x)}\}$ , then  $\omega' = \{\rho(x)\}_{x \in L}$  denote the attribute set of the *DU* that has not been revoked. Assume that  $\omega'$  still satisfies the access policy  $(A_{l \times k}, \rho)$ ; for any  $x$  from 1 to  $l$ , it will calculate  $D_{x,1}$  and  $D_{x,2}$ .

$$D_{x,1} = \prod_{j=1}^{l_{\rho(x)}} \left( \frac{e(K_{\rho(x),2}, C_{x,j,2})}{e(K_{\rho(x),3}, C_{x,j,1})} \right)^{1/uid-uid_j}, \quad (17)$$

$$D_{x,2} = \frac{e(K_{\rho(x),1}, C_{x,0})}{e(K_{\rho(x),2}, C_{x,1})}.$$

Let  $\mu_x$  be the restitution coefficient corresponding to the  $x$ th row in  $A_{l \times k}$ , and finally obtain the plaintext.

$$M = (K_F \mid href_{location}) = C_0 \cdot \frac{1}{e(K_0, C_1)} \cdot \prod_{x \in L} (D_{x,1}, D_{x,2})^{\mu_x}. \quad (18)$$

The *DU* can download *CF* from IPFS according to  $href_{location}$  and then use  $K_F$  to decrypt *CF* and obtain the shared data *F*.

$$F = \varepsilon.Dec_{K_F}(CF). \quad (19)$$

$$(8) \text{ Revoke}(M, (A_{l \times k}, \rho), \{R_{\rho(x)}\}_{x \in 1, \dots, l}, PK, uid, i)$$

Take the revoking of the attribute  $i$  of a *DU* to the sharing data *F* as an example; the *DO* needs to add the *uid* of the *DU* to the revocation list corresponding to the attribute  $i$  and execute the CP-ABE part of *Encrypt* to encrypt the data-related information *M*. Then, the *DO* sends a transaction as following to the EOS blockchain.

$$Tx = (\text{Re } f_{block}, t, \text{Sig}_{DO}(\text{chain.id}, Tx),$$

$$\text{Action}(\text{DSContract}, \text{PocikyUpdate}, \text{Auth}_{DO}, (fid, CT'_{(K_F \mid href_{location})}))) \quad (20)$$

## 6. Security and Performance Analysis of the Proposed Scheme

### 6.1. Security and Privacy Analysis of BPSSD

**6.1.1. Correctness.** Let  $L = \{x \mid \rho(x) \in \omega, uid \notin R_{\rho(x)}\}$ , then  $\omega' = \{\rho(x)\}_{x \in L}$  denote the attributes set of the *DU* that has not been revoked. Assume that  $\omega'$  still satisfies the access policy  $(A_{l \times k}, \rho)$ ; for any  $x$  from 1 to  $l$ , then

$$D_{x,1} = \prod_{j=1}^{l_{\rho(x)}} \left( \frac{e(g^{r_{\rho(x)}} Y_{\rho(x),2}, (u^{uid_j} h_{\rho(x)})^{\eta_{x,j}})}{e((u^{uid} h_{\rho(x)})^{r_{\rho(x)}} Y_{\rho(x),3}, g^{\eta_{x,j}})} \right)^{1/uid-uid_j}$$

$$= e(g, u)^{-r_{\rho(x)} \sum_{j=1}^{l_{\rho(x)}} \eta_{x,j}} = e(g, g)^{-ar_{\rho(x)} \lambda_x},$$



$$\begin{aligned}
D_{x,2} &= \frac{e\left(g^{ar+t_{\rho(x)}r_{\rho(x)}+ar_{\rho(x)}} Y_{\rho(x),1}, g^{\lambda_x}\right)}{e\left(g^{r_{\rho(x)}} Y_{\rho(x),2}, T_{\rho(x)}^{\lambda_x}\right)} \\
&= e(g, g)^{(ar+t_{\rho(x)}r_{\rho(x)}+ar_{\rho(x)})\lambda_x - t_{\rho(x)}r_{\rho(x)}\lambda_x} \\
&= e(g, g)^{(ar+ar_{\rho(x)})\lambda_x}, \\
M' &= (K_F | href_{location}) = C_0 \cdot \frac{1}{e(K_0, C_1)} \cdot \prod_{x \in L} (D_{x,1} D_{x,2})^{\mu_x} \\
&= Me(g, g)^{as} \cdot \frac{1}{e(g^{\alpha+ar}, g^s)} \cdot e(g, g)^{ar \sum_{x \in L} \lambda_x \mu_x} \\
&= Me(g, g)^{as} \cdot \frac{1}{e(g^{\alpha+ar}, g^s)} \cdot e(g, g)^{ars} = M.
\end{aligned} \tag{21}$$

After the proof, the data-related information  $M$  can be decrypted by the  $DU$ .

**6.1.2. Security Analysis.** The CP-ABE algorithm used in this paper is based on the scheme [37], referring to the revocation idea in [35] that introduces a revocation list for each attribute. The scheme [37] has proved to be completely secure. The detailed proof process can refer to the security analysis in [37], which is based on the standard model, and the security depends on three static assumptions.

This paper focuses on security data sharing based on blockchain. The security of CP-ABE is not within the main scope of this article. We will conduct a brief analysis of the security after adding an attribute revocation mechanism to the scheme [37].

If an adversary  $\mathcal{A}$  can win the game with a nonnegligible advantage in the security model in [37], he must be able to calculate  $e(g, g)^{as}$ . To obtain such a pairing, the adversary needs to utilize  $K_0 = g^{a+r\alpha}$  in the private key and  $C_1 = g^s$  in the ciphertext, both of which can get  $e(g, g)^{as} e(g, g)^{ars}$ . This means that  $\mathcal{A}$  needs to get  $e(g, g)^{ars}$ . Then,  $\mathcal{A}$  needs to get  $D_{x,1}$  and  $D_{x,2}$  corresponding to each attribute and get  $e(g, g)^{ar\lambda_x}$  by calculation. If  $\mathcal{A}$  does not satisfy the challenge attributes, he cannot obtain the correct attribute keys to calculate  $e(g, g)^{ar\lambda_x}$  conforming to the access policy and recover  $e(g, g)^{ars}$ .

For collusion attacks, when generating private keys for each  $DU$ , a random element  $r$  is contained in  $K_0$  and random elements  $r_i$  and  $Y_{i,1}, Y_{i,2}, Y_{i,3}$  are added to the attributes, so that different  $DUs$  cannot combine their private keys to launch attacks.

The attribute private key  $K_{i,3} = (u^{uid} h_i)^{r_i} Y_{i,3}$  which is related to the revocation contains the  $DU$ 's identity information  $uid$ . When  $R_{\rho(x)} \neq \emptyset$ , each  $uid_j \in R_{\rho(x)}$  in the revocation list contains  $C_{x,j,1} = g^{r_{x,j}}$  and  $C_{x,j,2} = (u^{uid_j} h_{\rho(x)})^{r_{x,j}}$ , which need to be eliminated when decrypting.  $1/(uid - uid_j)$  is used when eliminating. If  $uid$  is in the revocation list,  $1/(uid -$

$uid_j)$  will not be calculated to achieve the purpose of revoking the attribute  $j$  of  $uid$ .

### 6.1.3. Other Security Problem

(1) *Data Security.* Data security includes the confidentiality, integrity, and availability of the shared data. In our scheme, the large-capacity sharing data of the  $DO$  is encrypted using an efficient asymmetric encryption algorithm such as AES and uploaded to IPFS. The IPFS will split the encrypted data and store them on different IPFS nodes in a distributed manner. The access will be routed through the dynamic hash table maintained by each node, and a certain redundancy mechanism will ensure fault tolerance. Besides, IPFS also provides version control like Git. Thus, data encryption and storage in blocks ensure the confidentiality of the shared data. The integrity is guaranteed by dynamic hash table routing, and the tampered data blocks will not be available. The redundant storage and incentive mechanisms of IPFS ensure that users can access their data at any time. As long as IPFS is secure, then the data stored on it in our scheme is secure.

(2) *Privacy Analysis.* In a data-sharing system, privacy includes the content of the  $DO$ 's shared data and the traces of the  $DU$  when using the data. In our scheme, the  $DO$  will encrypt the address of the shared data and the corresponding decryption key with CP-ABE according to the established access policy. Then, the ciphertext is stored on the blockchain, and only the  $DUs$  whose attribute set satisfies the access policy can obtain the data. The content of the data will not be leaked. For the traces generated by  $DUs$ , we encrypt the keywords corresponding to the sharing data. The  $DU$  invoked the trapdoor function to calculate the search token for the keyword that he needs to retrieve and then uses the search token for retrieving on the blockchain without revealing any information he wants. More importantly, the user's identity is represented in the form of an address on the blockchain, and the real information of the user will not be exposed.

(3) *Fine-Grained Access Control.* In our scheme, the fine-grained access control of shared data is realized by CP-ABE. The  $DO$  can make different access policies through LSSS and assign different attributes to  $DUs$ . Meanwhile, fine-grained access control should also include fine-grained revocation. The proposed scheme draws on the identity-based broadcast encryption scheme, in which the  $DO$  assigns a unique  $uid$  for each  $DU$ , and the  $uid$  will be used as a user attribute, embedded in the ciphertext together with the general attributes. Each general attribute in the ciphertext carries a revocation list, and the  $DU$  whose  $uid$  in this list no longer has the corresponding attribute, so that it achieves the purpose of directly revoking a  $DU$ 's attribute.

(4) *Avoid a Single Point of Failure.* Compared with traditional cloud storage solutions, there is no centralized third party in our proposed scheme. Blockchain and IPFS used in BSSPD are all distributed technologies. Even if some of the nodes fail, the availability of the whole scheme will not be affected. More importantly, the BitTorrent protocol adopted by IPFS can enjoy

a high throughput only by requiring paying a small number of fees to incentive storage nodes. Simultaneously, the EOS blockchain is free to users, only the *DO* needs to mortgage some system tokens in exchange for storage and CPU resources, and these tokens can also be redeemed.

(5) *User-Centric*. In our proposed scheme, the *DO* can generate public parameters and the system master key and generate and distribute the private keys for *DUs* according to their attributes. Moreover, the *DO* can formulate access policies arbitrarily to assign and revoke the permission of *DUs*. All of these are controlled by the *DO* without any trusted third party. In this manner, the *DO* has complete control over his shared data.

(6) *Identity Authentication*. The user generates his identity in the blockchain through an asymmetric encryption algorithm with generating key pairs, whose cost is too low. In our proposed scheme, since the *uid* is embedded in the ciphertext of CP-ABE as an attribute, the *DUs* may register a large number of *uids* and use different *uids* to search and decrypt the shared data, which increases the burden of the *DO*. In order to prevent such attacks, BSSPD requires identity authentication. Before applying for registration, the *DU* needs to perform a PoW, which is similar to Bitcoin mining. The *DO* can adjust the difficulty of PoW according to the total number of *DUs* in the system. User management and identity authentication are carried out on the blockchain, and only authenticated users can perform operations. These are all executed in Smart Contract ensuring transparency and security.

## 6.2. Experiments and Performance Analysis of BPSSD

6.2.1. *Functional Comparison*. We compared the scheme proposed in this article with the recent blockchain-based data-sharing models from the following aspects, including security and privacy, identity management, fine-grained access control, immediate access revocation, and ciphertext keyword retrieval, as shown in Table 2.

From the comparison in the table, it can be concluded that due to the blockchain's decentralized and trustless nature, the data-sharing models based on blockchain allow *DOs* to formulate access control policies for their data on-chain, so they all can guarantee security and privacy. Early schemes like Ref. [18] mostly only described the model's outline without the specific implementation details. Generally, they only describe how blockchain can benefit security and privacy during the sharing, so the function is relatively simple. Reference [21] implemented a role-based access control model on the blockchain, but it turns out that RBAC is not suitable for implementing fine-grained access control and revocation in a distributed environment. Reference [28] utilized CP-ABE to achieve fine-grained access control, but it does not achieve permission revocation. However, in the access control scheme based on CP-ABE, an immediate access revocation is indispensable.

In our proposed scheme, we utilized CP-ABE to achieve fine-grained access control and realized the identity management of *DUs*. The *DO* assigns and manages unique *uids* and

TABLE 2: Functional comparison between BSSPD and other blockchain-based data-sharing scheme.

No.	BSSPD	Ref. [18]	Ref. [21]	Ref. [28]
Security and privacy	√	√	√	√
Identity management	√	×	×	×
Fine-grained access control	√	×	×	√
Immediate access revocation	√	×	×	×
Keyword ciphertext retrieval	√	×	×	√

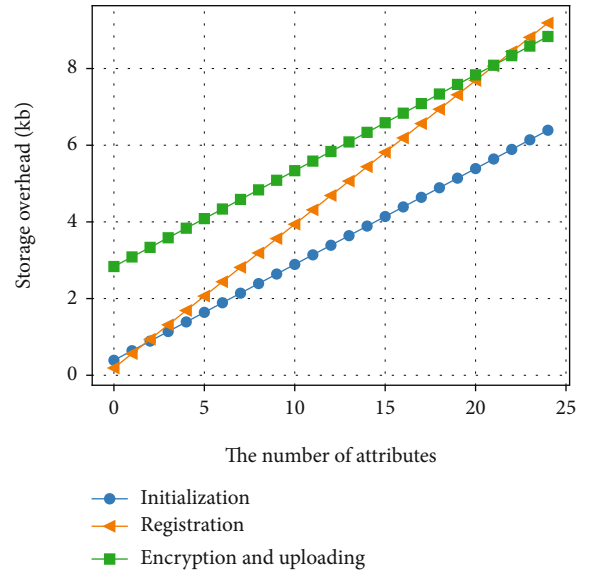


FIGURE 3: Storage overhead of BSSPD at each phase varies with the number of attributes.

attributes for registered *DUs*. Maintaining a revocation list for each attribute in the ciphertext can directly revoke a particular attribute of a *DU* without updating others' keys. BSSPD uses ciphertext keyword search to protect the privacy of *DUs* on-chain. Therefore, our proposed scheme has better applicability and usability.

6.2.2. *Storage Analysis*. BSSPD is a user-centric data-sharing scheme based on the EOS blockchain, and it stores the public system parameters, user information, and data-related information in the persistent database of Smart Contract. Because the storage resource on-chain is valuable and the acquisition of RAM in the EOS blockchain requires mortgaging system tokens, so it is necessary to analyze the size of the data stored in the Smart Contract.

We first define some symbols; we set  $|G_1|$ ,  $|G_2|$ ,  $|G_{p_1}|$ ,  $|G_{p_2}|$  to represent the bit length of an element in group  $G_1$ ,  $G_2$ ,  $G_{p_1}$ , and  $G_{p_2}$ , respectively. Let  $|Z_N|$  be the bit length of an element in filed  $Z_N$ ,  $|K_{AES}|$  be the bit length of a key of AES algorithm, and  $|Sk_{com}|$  and  $|Pk_{com}|$  be the bit length of private key and public key of ECC, respectively;  $|S|$  denote the number of attributes in system, and  $K_{search}$  denote the bit length of a secret key of pseudorandom function  $F$ .

According to the experiment simulation in our scheme, we set  $|G_1| = |G_2| = |G_{p_1}| = |G_{p_2}| = 1024\text{bits}$ ;  $|Z_N| = 128\text{bits}$ ;  $|K_{AES}| = 256\text{bits}$ ;  $|Sk_{com}| = 256\text{bits}$ ;  $|Pk_{com}| = 272\text{bits}$ ;  $|K_{search}| = 128\text{bits}$ ; the bit length of *account*, *uid*, *fid*, and search token  $t_{kw}$  to be 64; and the bit length of an IPFS address to be 256. The storage overhead of BSSPD at each phase varies with the number of attributes which is shown in Figure 3.

In our proposed scheme, there are three operations that interact with the blockchain to store data in the Smart Contract, which are as follows:

### (1) Initialization

The *DO* uploads the system public parameters to the Smart Contract; the storage overhead is

$$|Z_N| + |G_1| + 2|G_{p_1}| + |S|(2|G_{p_1}|) = (3200 + 2048|S|)\text{bits}. \quad (22)$$

### (2) Registration

The *DU* uploads information to the Smart Contract when applying for registration, and the *DO* assigns a unique *uid* and private keys for the *DU*. The storage overhead is

$$|account| + |uid| + |Pk_{com}| + |K_{search}| + |G_{p_1}| + 3|G_{p_1}||S| = (1552 + 3072|S|)\text{bits}.$$

### (3) Encryption and uploading

The *DO* uploads data-related information and the private keys of the *DU* to the Smart Contract, as well as the indices for the *DU*. The storage overhead is

$$|K_{AES}| + |address| + 2|G_{p_1}| + 2|G_{p_1}||S| + 2|G_{p_1}||R| + |fid| + |t_{kw}| + |fid| + |account| = 2752 + 2048|S| + 2048|R|. \quad (24)$$

For simplicity, the figure shows that the storage overhead varies with the number of attributes when there are 10 *DUs* in the revocation list. As the number of *DUs* in the revocation list and the relevant *DUs* increases, the storage overhead will also increase to a certain extent.

The RAM in the EOS blockchain is obtained by collateralizing system tokens, and the current price is 0.05 EOS/KB. The *DO* can purchase RAM according to the scale of his system. Unlike Ethereum transactions that need to consume ETH as gas, the tokens mortgaged when acquiring RAM in EOS can still be redeemed at the original price. Above all, the proposed scheme is feasible and practical.

**6.2.3. Performance Analysis.** As we all know, the computing resource on the blockchain is also precious, and the computational efficiency of the existing blockchains is often criticized. For example, Bitcoin takes 10 minutes to produce a block. Ethereum has dramatically improved the block generation time, but it also takes about 15 seconds. In this section, we will conduct experiments on our proposed scheme and evaluate the scheme's performance and user scale.

We used 5 nodes to build an EOS private chain in a laboratory environment. The 5 nodes we chose were all MacBook Pro (2017) with Intel (R) Core (TM) i5 CPU that clocks at 3.1 GHz and has 16.0 GB of RAM. The version of the EOS blockchain we chose is v2.0.6. The code of the indices of the two tables related to the sharing data in our Smart Contract is as follows:

In our scheme's initialization phase, the operation on-chain is to set and update the public system parameters. The previous section shows that the storage overhead will continue to expand as the attributes increase. However, it can be seen from Figure 4 that as the attributes increase, the computing overhead will not be significantly affected in this phase.

In the encryption and uploading phase of our scheme, the operations that need to be performed on-chain are uploading the data-related information to Smart Contract and establishing the keyword indices for the data-related *DUs*. As shown in Figure 5, the increase in the number of attributes will not have too much influence on the computing overhead of *AddData*. In the case of a different number of attributes, the computing overhead of *AddData* is generally stable. What impacts the computing overhead of *AddData* is the scale of *DUs*, especially the number of *DUs* related to the sharing data. It can be seen from Figure 5 that the computing overhead of 500 *DUs* is obviously higher than that of 100 *DUs*, and the time cost is mainly spent on establishing search indices for the relevant *DUs*.

Since BSSPD sets the search token as a secondary index of the *search\_table* in the Smart Contract, no matter how many pieces of index data exist in the system, the time complexity of retrieving according to the search token is  $O(1)$ . As shown in Figure 6, when there are 10 billion pieces of index data, the search time is not much different from that of 1 million, and the search time is in milliseconds.

The deletion of a certain data in our scheme is to remove the data-related information and the indices to the data. As shown in Figure 7, as the number of data-related *DUs* continues to expand, the computing overhead of deletion will increase too. The main time cost is spent on deleting the search indices to the data.

Since only the ciphertext data needs to be updated according to the shared data's primary key id when revoking a *DU*'s attribute of a specific shared data, there is no need to operate on the relevant indices, and its computing overhead is similar to set and update the public system parameters in the initialization phase, which is stable.

In summary, in our proposed scheme, the total number of attributes will not impact much on the computing overhead on-chain. According to experience, it only affects

```

typedef eosio::multi_index<"sharedatas"_n, my_data> data_table;
typedef eosio::multi_index<"searchindexxs"_n, s_index, indexed_by<"username"_n,
const_mem_fun<s_index, uint64_t, &s_index::by_secondary>>, indexed_by <"searchtoken "_n, const_mem_fun<s_index, check-
sum256, &s_index::by_thirdary>>, indexed_by<"fid"_
n, const_mem_fun<s_index, uint64_t, &s_index::by_forthary>>> search_table;
    
```

CODE 1: The code of the tables in Smart Contract.

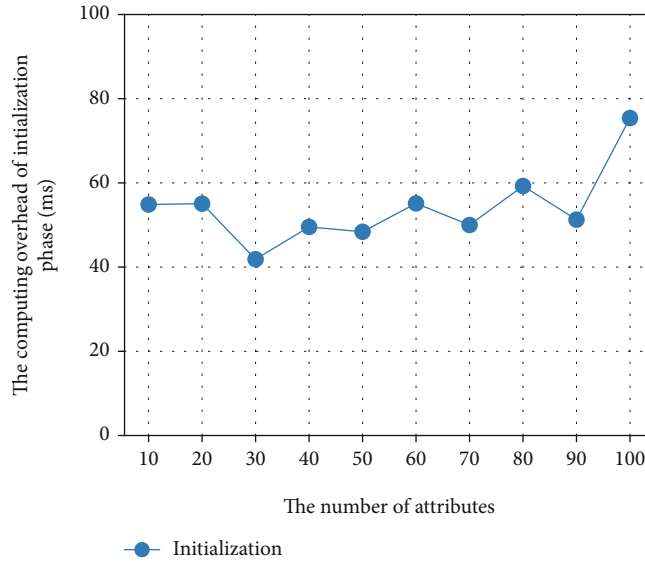


FIGURE 4: Computing overhead of the initialization phase varies with the number of attributes.

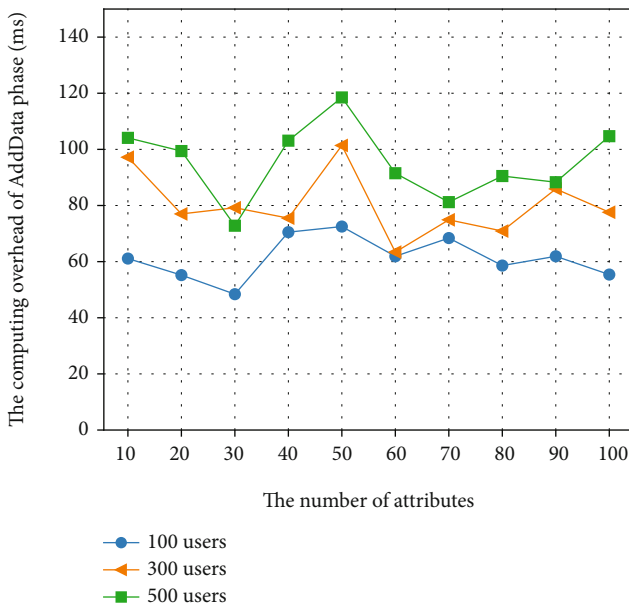


FIGURE 5: Computing overhead of the AddData varies with the number of attributes.

operations off-chain, such as key generation, encryption, and decryption. However, the expansion of the user scale will increase the time cost of some operations. Specifically, it is increased with the number of *DUs* related to certain shared

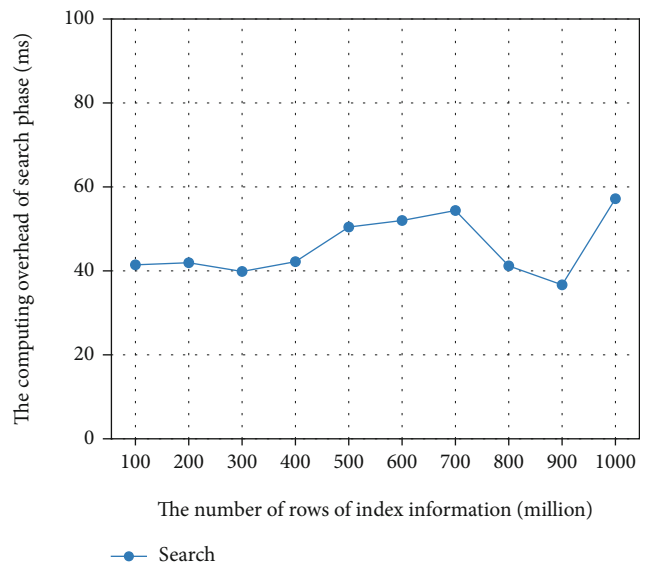


FIGURE 6: Computing overhead of the search phase varies with the number of rows of index information.

data because search indices will be established. When the related search indices of a specific data increase to 500, the computing overhead is still in milliseconds. For all operations on-chain in our scheme, the computing overhead is less than 100 milliseconds. The configuration of the EOS main network’s block producer is much better than the laptop we



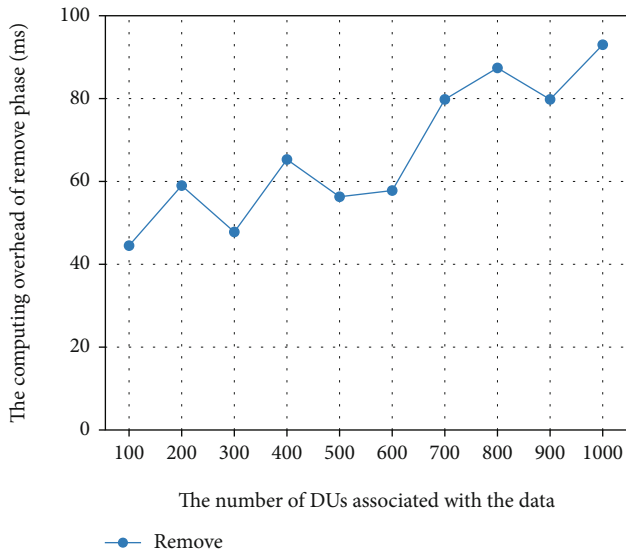


FIGURE 7: Computing overhead of the remove varies with the number of DUs associated with the shared data.

use, so when the contract is deployed on the main network of EOS, the computing overhead will be much lower than that of our simulation. Now, since EOS takes 0.5 seconds to generate a block, our scheme's operation will be confirmed soon after execution. Therefore, the experiment has proved that our scheme has a good performance.

## 7. Conclusion

In the AI-driven era, a user-centered sharing model is proposed to open data while ensuring data privacy. We combined blockchain, CP-ABE, and IPFS to propose a blockchain-based security data-sharing scheme with fine-grained access control and permission revocation. In our proposed scheme, the *DO* encrypts his data and uploads it to IPFS, then encrypts the returned address and decryption key by CP-ABE. Only *DUs* whose attributes satisfy the access policy can decrypt and obtain the data. There is no centralized node in the scheme, and the *DO* has complete control over his shared data, which promises privacy and security. To achieve the goal, we have implemented our scheme on the EOS blockchain. The security and performance analysis proves that our scheme is feasible and practical and has a good performance. We can also add a cryptocurrency to introduce an economic system for data sharing and further enrich our scheme's functions. At the same time, there are many shortcomings in our scheme. For example, the CP-ABE we designed with permission revocable does not have the best performance. There are also many types of research on CP-ABE [38–42]. We can use a CP-ABE with better performance to improve our scheme. Besides, for the searchable encryption algorithm used in our scheme, the *DO* needs to distribute a secret key for each *DU* and store it on-chain. It also needs to maintain large amounts of indices for each shared data, which can be further optimized. At present, some researchers have proposed using blockchain to solve the fairness problem in searchable encryption algorithm

[43–47]. In the future, we will study and discuss the endowment of a better ciphertext searchable algorithm to further optimize our scheme. Simultaneously, to make our scheme more practical, we can combine some studies [48–52] with ours and put forward a data governance scheme that is more in line with the practical application.

## Data Availability

The data that support the findings of this study are available from the corresponding author, upon reasonable request.

## Conflicts of Interest

The author(s) declare(s) that they have no conflicts of interest.

## Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant 61272519, 61170297, 61472258, and 61802094 and National Natural Science Foundation of Zhejiang Province under Grant LY20F020012.

## References

- [1] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Computers & Security*, vol. 72, pp. 1–12, 2018.
- [2] S. Sundareswaran, A. Squicciarini, and D. Lin, "Ensuring distributed accountability for data sharing in the cloud," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 4, pp. 556–568, 2012.
- [3] Cheng-Kang Chu, S. S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 468–477, 2014.
- [4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *2010 Proceedings IEEE INFOCOM*, pp. 1–9, San Diego, CA, 2010.
- [5] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.
- [6] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 1–590, 2018.
- [7] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.
- [8] X. Zhou, W. Liang, K. Wang, R. Huang, and Q. Jin, "Academic influence aware and multidimensional network analysis for research collaboration navigation based on scholarly big data," *IEEE Transactions on Emerging Topics in Computing*, no. 1, 2018.
- [9] Z. Cai, X. Zheng, and J. Yu, "A differential-private framework for urban traffic flows estimation via taxi companies," *IEEE*



- Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6492–6499, 2019.
- [10] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system,” 2008, <https://bitcoin.org/bitcoin.pdf>.
  - [11] Y. Xu, C. Zhang, G. Wang, Z. Qin, and Q. Zeng, “A blockchain-enabled deduplicatable data auditing mechanism for network storage services,” *IEEE Transactions on Emerging Topics in Computing*, 2020.
  - [12] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, “Blockchain empowered arbitrable data auditing scheme for network storage as a service,” *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 289–300, 2020.
  - [13] Y. Xu, C. Zhang, Q. Zeng, G. Wang, J. Ren, and Y. Zhang, “Blockchain-enabled accountability mechanism against information leakage in vertical industry services,” *IEEE Transactions on Network Science and Engineering*, 2020.
  - [14] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, “A blockchain-based nonrepudiation network computing service scheme for industrial IoT,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3632–3641, 2019.
  - [15] M. Swan, “Blockchain thinking: the brain as a decentralized autonomous corporation [commentary],” *IEEE Technology and Society Magazine*, vol. 34, no. 4, pp. 41–52, 2015.
  - [16] G. Zyskind, O. Nathan, and A. Pentland, “Decentralizing privacy: using blockchain to protect personal data,” in *2015 IEEE Security and Privacy Workshops*, pp. 180–184, San Jose, CA, 2015.
  - [17] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “Medrec: using blockchain for medical data access and permission management,” in *2016 2nd International Conference on Open and Big Data (OBD)*, pp. 25–30, Vienna, 2016.
  - [18] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, “Medshare: trust-less medical data sharing among cloud service providers via blockchain,” *IEEE Access*, vol. 5, pp. 14757–14767, 2017.
  - [19] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, “Secure and trustable electronic medical records sharing using blockchain,” *AMIA Annual Symposium Proceedings*, vol. 2017, pp. 650–659, 2017.
  - [20] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, “Integrating blockchain for data sharing and collaboration in mobile healthcare applications,” in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–5, Montreal, QC, 2017.
  - [21] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, “Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5g,” *IET Communications*, vol. 12, no. 5, pp. 527–532, 2017.
  - [22] G. Zhang, T. Li, Y. Li, P. Hui, and D. Jin, “Blockchain-based data sharing system for AI-powered network operations,” *Journal of Communications and Information Networks*, vol. 3, no. 3, pp. 1–8, 2018.
  - [23] I. Zhou, I. Makhdoom, M. Abolhasan, J. Lipman, and N. Shariati, “A blockchain-based file-sharing system for academic paper review,” in *2019 13th International Conference on Signal Processing and Communication Systems (ICSPCS)*, pp. 1–10, Gold Coast, Australia, 2019.
  - [24] V. Patel, “A framework for secure and decentralized sharing of medical imaging data via blockchain consensus,” *Health informatics journal*, vol. 25, no. 4, pp. 1398–1411, 2018.
  - [25] L. Tan, N. Shi, C. Yang, and K. Yu, “A blockchain-based access control framework for cyber-physical-social system big data,” *IEEE Access*, vol. 8, pp. 77215–77226, 2020.
  - [26] M. Jemel and A. Serhrouchni, “Decentralized access control mechanism with temporal dimension based on blockchain,” in *2017 IEEE 14th International Conference on e-Business Engineering (ICEBE)*, pp. 177–182, Shanghai, 2017.
  - [27] X. Sun, S. Yao, S. Wang, and Y. Wu, “Blockchain-based secure storage and access scheme for electronic medical records in ipfs,” *IEEE Access*, vol. 8, pp. 59389–59401, 2020.
  - [28] S. Wang, Y. Zhang, and Y. Zhang, “A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems,” *IEEE Access*, vol. 6, pp. 38437–38450, 2018.
  - [29] S. M. Pournaghi, M. Bayat, and Y. Farjami, “MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 11, pp. 4613–4641, 2020.
  - [30] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in *2007 IEEE Symposium on Security and Privacy (SP ’07)*, pp. 321–334, Berkeley, CA, 2007.
  - [31] B. Waters, “Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization,” in *Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography Conference on Public Key Cryptography, PKC’11*, pp. 53–70, Berlin, Heidelberg, 2011.
  - [32] V. Buterin, “Ethereum: a next-generation smart contract and decentralized application platform,” 2013, <https://github.com/ethereum/wiki/wiki/White-Paper>.
  - [33] N. Szabo, “Smart contracts,” 1994, <https://szabo.best.vwh.net/smart.contracts.html>.
  - [34] H. Gao, Z. Ma, S. Luo, and Z. Wang, “Bfr-mpc: a blockchain-based fair and robust multi-party computation scheme,” *IEEE Access*, vol. 7, pp. 110439–110450, 2019.
  - [35] N. Attrapadung and H. Imai, “Conjunctive broadcast and attribute-based encryption,” in *Proceedings of the 3rd International Conference Palo Alto on Pairing-Based Cryptography, pairing ’09*, pp. 248–265, Berlin, Heidelberg, 2009.
  - [36] H. Li, F. Zhang, J. He, and H. Tian, “A searchable symmetric encryption scheme using blockchain,” 2017, <https://arxiv.org/abs/1711.01030>.
  - [37] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, “Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption,” in *Proceedings of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques, EUROCRYPT’10*, pp. 62–91, Berlin, Heidelberg, 2010.
  - [38] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, “User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage,” *IEEE Systems Journal*, vol. 12, no. 2, pp. 1767–1777, 2018.
  - [39] Y. Xu, Q. Zeng, G. Wang, C. Zhang, J. Ren, and Y. Zhang, “An efficient privacy-enhanced attribute-based access control mechanism,” *Concurrency and Computation: Practice and Experience*, vol. 32, no. 5, article e5556, 2020.
  - [40] X. Yan, Y. Xu, X. Xing, B. Cui, Z. Guo, and T. Guo, “Trustworthy network anomaly detection based on an adaptive learning rate and momentum in IIoT,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6182–6192, 2020.

- [41] Z. Cai and Z. He, "Trading private range counting over big IoT data," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 144–153, Dallas, TX, USA, 2019.
- [42] G. Yu, X. Zha, X. Wang et al., "Enabling attribute revocation for fine-grained access control in blockchain-IoT systems," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1213–1230, 2020.
- [43] L. Chen, W. K. Lee, C. C. Chang, K. K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Generation Computer Systems*, vol. 95, pp. 420–429, 2019.
- [44] Y. Xu, G. Wang, J. Yang, J. Ren, Y. Zhang, and C. Zhang, "Towards secure network computing services for lightweight clients using blockchain," *Wireless Communications and Mobile Computing*, vol. 2018, 12 pages, 2018.
- [45] X. Zhou, W. Liang, K. I. Wang, H. Wang, L. T. Yang, and Q. Jin, "Deep-learning-enhanced human activity recognition for Internet of healthcare things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6429–6438, 2020.
- [46] X. Yan, Y. Xu, B. Cui, S. Zhang, T. Guo, and C. Li, "Learning URL embedding for malicious website detection," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6673–6681, 2020.
- [47] S. Hu, C. Cai, Q. Wang, C. Wang, X. Luo, and K. Ren, "Searching an encrypted cloud meets blockchain: a decentralized, reliable and fair realization," in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, pp. 792–800, Honolulu, HI, 2018.
- [48] X. Zhou, Y. Hu, W. Liang, J. Ma, and Q. Jin, "Variational LSTM enhanced anomaly detection for industrial big data," *IEEE Transactions on Industrial Informatics*, 2020.
- [49] X. Zhou, Y. Li, and W. Liang, "CNN-RNN based intelligent recommendation for online medical pre-diagnosis support," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 2020.
- [50] X. Zhou, W. Liang, K. I. Wang, and L. T. Yang, "Deep correlation mining based on hierarchical hybrid networks for heterogeneous big data recommendations," *IEEE Transactions on Computational Social Systems*, vol. 8, no. 1, pp. 171–178, 2021.
- [51] Y. Liang, Z. Cai, J. Yu, Q. Han, and Y. Li, "Deep learning based inference of private information using embedded sensors in smart devices," *IEEE Network*, vol. 32, no. 4, pp. 8–14, 2018.
- [52] X. Yan, B. Cui, Y. Xu, P. Shi, and Z. Wang, "A method of information protection for collaborative deep learning under GAN model attack," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 2019.

## Research Article

# Trustworthy Jammer Selection with Truth-Telling for Wireless Cooperative Systems

Yingkun Wen , Tao Jing , and Qinghe Gao 

School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing, China

Correspondence should be addressed to Yingkun Wen; 16111024@bjtu.edu.cn

Received 9 November 2020; Revised 23 December 2020; Accepted 9 January 2021; Published 8 February 2021

Academic Editor: Zhuojun Duan

Copyright © 2021 Yingkun Wen et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In this paper, we propose a trustworthy friendly jammer selection scheme with truth-telling for wireless cooperative systems. We first utilize the reverse auction scheme to enforce truth-telling as the dominant strategy for each candidate friendly jammer. Specifically, we consider two auction cases: (1) constant power (CP) case and (2) the utility of the BS maximization (UBM) case. In both cases, the reverse auction scheme enforces truth-telling as the dominant strategy. Next, we introduce the *trust category* and *trust degree* to evaluate the trustworthiness of each Helper transmitter (Helper-Tx). Specifically, an edge controller calculates the reputation value of each Helper-Tx periodically using an additive-increase multiplicative-decrease algorithm by observing its jamming behavior. With the historical reputation values, the edge controller (EC) classifies a Helper-Tx into one of four trust categories and calculates its trust degree. Then, the EC selects the best Helper-Tx based on the trust category and trust degree. Lastly, we present numerical results to demonstrate the performance of our proposed jammer selection scheme.

## 1. Introduction

Cooperative jamming enables two wireless nodes to exchange secret messages in the presence of an eavesdropper without encryption [1, 2]. It is an information-theoretic security approach that exploits the physical characteristics of the wireless channel, which does not depend on the assumption of computational hardness. In cooperative jamming, a selected friendly jammer sends out artificial noise (i.e., jamming signal) at the same time when a sender transmits a message to a receiver [3, 4]. The artificial noise is aimed at creating intentional interference at the eavesdropper. If the channel condition between the sender-receiver is better than that of the channel between the sender-eavesdropper, the sender and receiver can exchange secure messages at a certain rate.

Friendly jammer selection plays a fundamental role in maximizing the secure message exchange rate (i.e., secrecy rate) in cooperative jamming [5, 6]. In general, there are two phases in a jammer selection scheme. In the first phase, each candidate jammer reports its private information (e.g., battery

state) to the sender (also known as the source node or mechanism designer) through a common control channel [7, 8]. According to the reported private information, the sender selects a suitable candidate as the jammer. In the second phase, the selected jammer sends out sufficient jamming signals to create desired interference at the eavesdropper (Eve).

There are challenges that need to address in both phases. In the first phase, since each candidate wants to be selected to get payment, it may not be telling the truth in reporting its private information so as to increase the chance of being selected. A candidate without truth-telling can cause unfairness and degrade the secrecy performance of the entire network. Therefore, it is necessary to develop a mechanism to ensure truth-telling for each candidate. In the second phase, a selected jammer may transmit a partial (or even none) jamming signal due to various reasons. We call it an *untrusted* friendly jammer. An untrusted jammer can also lead to unfairness and a decrease in the secrecy rate. Hence, it is important to avoid untrusted jammers.

To address the aforementioned challenges, we propose a trustworthy friendly jammer selection scheme with truth-

telling for a wireless cooperative system (WCS). Firstly, we utilize the reverse auction scheme to enforce truth-telling under two cases: (1) constant power (CP) case and (2) utility of the BS maximization (UBM) case. In these two cases, we enforce truth-telling as the dominant strategy of each candidate jammer. In the auction scheme, helper transmitters (Helper-Txs) are edge devices that function as candidate jammers. Spectrum resources of a base station (BS) are revenues for Helper-Txs. In the CP case, the BS assigns a fixed transmission power to the jammer. In the UBM case, the utility of the BS is approximately maximized.

Secondly, we introduce *trust categories* and *trust degree* to evaluate the trustworthiness of each Helper-Tx. Specifically, an edge controller (EC) is introduced to calculate the reputation value of each Helper-Tx periodically using an additive-increase multiplicative-decrease (AIMD) algorithm by observing its jamming behavior. Subsequently, the EC classifies each Helper-Tx into one of four trust categories based on its historical reputation values. The trust degree of each Helper-Tx is obtained by averaging its reputation values over time. If a Helper-Tx belongs to a certain trust category and meets the trust degree requirement, it can be regarded as a trustworthy jammer.

The main contributions of this paper are summarized as follows:

- (i) We prove that the BS can achieve the highest secrecy rate by selecting a one best Helper-Tx as the jammer. More than one jammer can lead to a decreased secrecy performance
- (ii) We utilize the reverse auction scheme to stimulate truth-telling of Helper-Txs. In the reverse auction scheme, we consider two cases: (1) CP case and (2) UBM case. In both cases, the reverse auction scheme can guarantee incentive compatible (IC) and individual rationality (IR). In both cases, we show numerical results that the reverse auction scheme outperforms the widely used Vickrey auction scheme
- (iii) We propose two metrics (i.e., trust category and degree) to measure the trustworthiness of a selected jammer. We adopt the AIMD algorithm to promote trustworthy behavior and penalize selfish conducts

The rest of the paper is organized as follows. Related work is given in Section 2. In Section 3, an overview of the network model and some preliminaries are presented. In Section 4, we give out the auction scheme and related solutions. In Section 5, the trust management process and the jammer selection scheme are described. Numerical results are given in Section 6, and conclusions are drawn in Section 7.

*Notations:*  $(\cdot)^H$  and  $|\cdot|$  denote the Hermitian transpose and the absolute value, respectively.  $\text{Tr}(\cdot)$  denotes the trace operator.  $\mathbf{I}_N$  is the  $N \times 1$  vector of all ones. The normal distribution with the mean  $\mu$  and the variance  $\sigma^2$  is denoted as  $\mathcal{N}(\mu, \sigma^2)$ .  $[x]^+ = \max\{x, 0\}$ .  $\mathbf{A} \pm 0$  ( $\mathbf{A} > 0$ ) means that  $\mathbf{A}$  is a Hermitian positive semidefinite (definite) matrix.

## 2. Related Work

Conventional cryptographic-based methods at the upper layer are of high complexity due to the expensive operations such as the encryption and decryption [9–11]. Physical layer security approaches with the advantages of low complexity and resource savings have been explored both as an alternative and a complementary to conventional cryptographic-based methods [12–14]. Physical layer security approaches with the cooperation of helping nodes (cooperative relaying and jamming) have been extensively investigated [15–18]. Recently, some new physical layer security technologies have been proposed for secure communication, e.g., unmanned aerial vehicle- (UAV-) aided jamming [19], intelligent reflecting surfaces- (IRS-) assisted jamming [20], and learning-aided cooperative relays [21, 22].

Considering that the helping nodes consume energy during cooperation, it is necessary to investigate how to incentivize users to cooperate for security enhancement [23–25]. Therefore, game theory is employed in physical layer security to study the interactions between the source and helping nodes, where helping nodes would gain some payoffs [26, 27]. However, in most of the current cooperative networks, the helping nodes are assumed honest and ready to disclose their true private information, which is usually not realistic [28, 29]. In practice, helping nodes may exaggerate their private information to maximize their payoffs, which is a key issue in cooperative networks.

To address this issue, a mechanism designer aims to motivate the helping nodes to disclose their private information by designing the payoff structure [30–33]. Authors of [31] designed different “transfer payment” functions to the payoff of each relay and proved that each relay gains its maximum payoff when it truthfully reports its private information. In [33], the author proposed a truth-telling based mechanism, where the selected relays’ energy harvesting requirements would be fulfilled if they tell the truth. Otherwise, the relays are penalized by the transfer payment.

Besides cooperative relays, cooperative jammers are also important helping nodes for physical layer security in cooperative networks [6, 34, 35]. In [6], the authors investigated the physical layer security of amplify-and-forward (AF) relaying networks with the aid of the joint relay and jammer selection. Authors in [34] proposed three categories of relay and jammer selection for a two-way cooperative communication scenario. In [35], the authors proposed a joint relay and jammer selection scheme and derived a closed-form suboptimal solution to maximize the secrecy rate.

In addition, untrusted jammers were investigated in [5, 36]. Specifically, the authors of [36] investigated a social-tie-based jammer selection scheme, allocating power appropriately to the source node and the cooperative jammer node to maximize the worst-case ergodic secrecy rate. In [5], the authors investigated how to select jammers for device to device users to thwart eavesdroppers by exploiting social relationship with the help of full CSI and partial CSI, respectively.

In the above literatures, the jammers are assumed honest, and the private information are perfectly known at the source



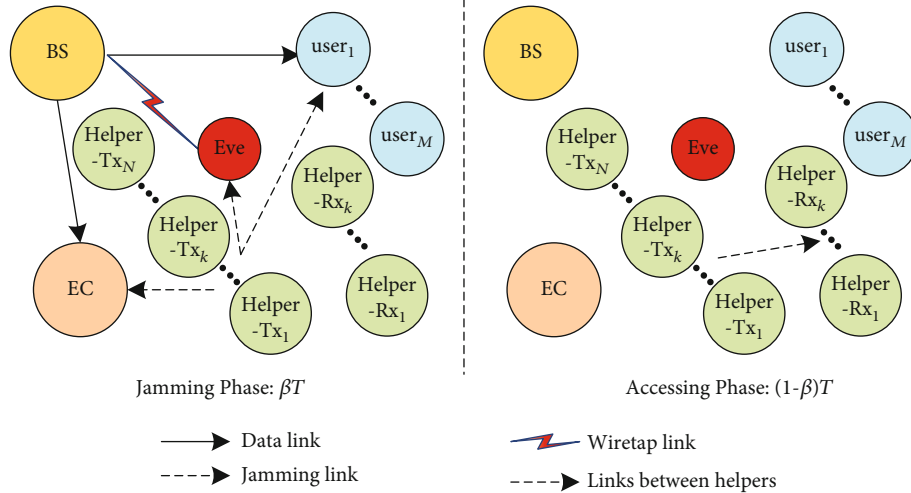


FIGURE 1: Network components.

node. However, the optimal solutions in these works would not hold if the jammers report their private information untruthfully. In addition, the trust degree of a jammer was only considered to be one of the parameters to analyze the secrecy performance. To the best of our knowledge, how to incentive cooperative jammers to report their private information and do trustworthiness analysis for a jammer has never been investigated, which motivates the study of this paper.

### 3. An Overview

In this paper, we consider a WCS that consists of a BS,  $M$  users, an Eve, an EC, and  $N$  pairs of Helper-Tx/Rx as shown in Figure 1. The BS is a type of edge device that functions as a user data entry point to the primary network. Helper-Tx/Rxs are another type of edge device that protects user data from being intercepted by Eve. Both types of edge devices are managed by the EC that is a controller that can be configured to match multiple specific requirements.

**3.1. Transmission Phases.** In the WCS, from the perspective of the jammer, there are two transmission phases (the jamming phase and the accessing phase) with a duration of length  $T$ .

**3.1.1. Jamming Phase.** In the jamming phase of length  $\beta T$ , the BS wants to send a message to a user (e.g., user<sub>1</sub>) on the data link. Meanwhile, there is an Eve that wants to intercept and decode the message on the wiretap link. To protect the transmitted message from being eavesdropped, the BS selects  $K \leq N$  Helper-Txs as friendly jammers to interfere with Eve on the jamming link.

In the WCS, the selected Helper-Tx (the jammer) is an edge device of user<sub>1</sub>; thus, it is assumed that the jamming signal cannot be known previously by user<sub>1</sub>. It means that user<sub>1</sub> cannot remove the jamming signal from the received signal. Instead, the beamforming vector of the jammer ( $\mathbf{w}_j$ ) needs to be designed to ensure that the interference imposed at user<sub>1</sub> is lower than a temperature limit. In the WCS, we

would first analyze the secrecy performance of the BS through cooperative jamming and then select the appropriate Helper-Txs. In what follows, we would calculate the secrecy rate to measure the secrecy performance of the BS.

It is assumed that the BS is able to acquire the CSI of the data link through pilot sequences [37]. Each Helper-Tx measures its CSI between itself and user<sub>1</sub>, i.e.,  $\mathbf{h}_{j_n,u}$ , and reports the CSI to the EC. The EC would share the CSI of Helper-Txs with the BS via a secure channel, such as a common control channel [38]. Finally, the CSI of users and Helper-Txs are both available at the BS. Thus, we assume that the perfect CSI of the data link is available. For the CSI of wiretap link, there are two cases:

- (i) *Perfect CSI Case.* In some special cases, one of the legitimate users (e.g., untrusted relays) may be considered to be a potential Eve [39]. In other words, Eve is one of the legitimate users; thus, we can obtain the perfect CSI of the wiretap link. Specifically, the instantaneous CSI of  $\mathbf{h}_{b,e}$  and  $\mathbf{h}_{j_k,e}$  is known.
- (ii) *Statistical CSI Case.* In most cases, accurate CSI for passive Eve cannot be acquired. However, the statistical CSI for wiretap links can be obtained by some measurement methods. Therefore, it is assumed that we can obtain the statistical CSI of the wiretap link. Specifically, the covariance matrices of  $\mathbf{h}_{b,e}$  and  $\mathbf{h}_{j_k,e}$  are known, i.e.,  $\mathbf{h}_{b,e} \sim \mathcal{CN}(0, \sigma_{b,e}^2 \mathbf{I}_{N_b})$  and  $\mathbf{h}_{j_k,e} \sim \mathcal{CN}(0, \sigma_{j_k,e}^2 \mathbf{I}_{N_j})$ .

In this paper, we only consider the perfect CSI case. In the case with statistical CSI, the design and analysis for reverse auction and trust management can be treated similarly in our previous work [40], which is omitted for brevity.

In the WCS, the BS is equipped with  $N_b$  antennas, and Helper-Txs are equipped with  $N_j$  antennas. All users, Eve, the EC, and Helper-Rxs are all equipped with a single antenna. The transmit beamforming vectors of the BS ( $\mathbf{w}_b$ ) and Helper-Tx <sub>$k$</sub>  ( $\mathbf{w}_{j_k}$ ) are both designed at the BS. Next, the



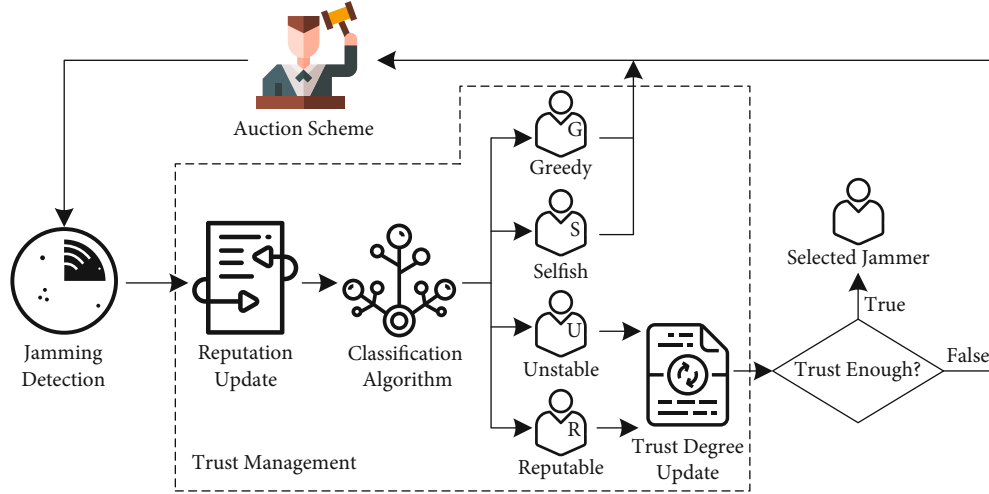


FIGURE 2: A framework for trustworthy jammer selection with truth-telling.

BS delivers the related beamforming vector ( $\mathbf{w}_{j_k}$ ) to the EC, and the EC applies the beamforming vector ( $\mathbf{w}_{j_k}$ ) to Helper-Tx $_k$ .

With the CSI and beamforming vectors, the received signals at user $_1$ , the EC, and Eve at time index  $t$  can be expressed as

$$y_q(t) = \mathbf{h}_{b,q}^H \mathbf{w}_b x_b(t) + \sum_{k=1}^K \mathbf{h}_{j_k,q}^H \mathbf{w}_{j_k} x_{j_k}(t) + n_q(t), \quad (1)$$

respectively, where  $\mathbf{h}_{p,q}$ ,  $p \in \{b, j_k\}$ ,  $q \in \{u, c, e\}$  are the links from the transmitters (the BS, Helper-Tx $_k$ ) to the receivers (user $_1$ , the EC, and Eve).  $\mathbf{h}_{p,q} = \bar{\mathbf{h}}_{p,q} \sqrt{\theta_{p,q}}$  with  $\bar{\mathbf{h}}_{p,q}$  and  $\theta_{p,q}$  denoting the  $N_b(N_j) \times 1$  complex link vectors and the corresponding path loss from  $p$  to  $q$  link, respectively. The path loss can be expressed as  $10 \log_{10}(\theta_{p,q}) = -34.5 - 38 \log_{10}(d_{p,q}[\text{m}])$ , where  $d_{p,q}$  is the distances between transmitters and receivers.  $\mathbf{w}_b \in \mathbb{C}^{N_b \times 1}$  and  $\mathbf{w}_{j_k} \in \mathbb{C}^{N_j \times 1}$  are beamforming vectors of the BS and Helper-Tx $_k$ , respectively.  $x_b$  is the message signal transmitted from the BS.  $x_{j_k}$  is the jamming signal transmitted from Helper-Tx $_k$ , where  $x_{j_k} \sim \mathcal{N}(0, 1)$ .  $n_q$  is the additive white Gaussian noise (AWGN) with two-sided power spectral density  $N_{02}$ . It is assumed that  $n_q \sim \mathcal{N}(0, \delta_q^2)$ , where  $\delta_q^2 = 2N_{02}B$  and  $B$  is the link bandwidth. All links are assumed to be subject to independent Rayleigh fading.

**3.1.2. Accessing Phase.** In the accessing phase of length  $(1 - \beta)T$ , the selected Helper-Txs are allowed to access the data link when the data link is idle so that they can transmit their messages to intended Helper-Rxs.

**3.2. Trustworthy and Truth-Telling Challenges.** In the WCS, note that the secrecy rate is provided by a Helper-Tx; the selection of an appropriate Helper-Tx as the cooperative jammer plays a critical role in improving the secrecy rate. Specifically, the selection of an appropriate Helper-Tx faces two challenges as follows:

- (i) *Truth-Telling Challenge.* Since the selected Helper-Txs may have greater opportunity to access the data link, all the Helper-Txs will be naturally interested in participating in the WCS. However, there is no guarantee that they would report its private information (the battery state) to the BS honestly. In practice, the issue is that Helper-Txs may exaggerate their private information to enhance their chance to be selected, hoping to maximize their transmission time in the data link.
- (ii) *Trustworthy Challenge.* A selected jammer may transmit a partial (or even none) jamming signal due to various reasons. We call it an *untrusted friendly jammer*. An untrusted jammer cannot improve the secrecy performance of the WCS. In addition, an untrusted jammer can obtain underserved utility, leading to unfairness to other trustworthy jammers.

To address these challenges, we propose a framework as shown in Figure 2, consisting of *Auction Scheme*, *Jamming Detection*, and *Trust Management*. The auction scheme is introduced in Section 4 to prevent Helper-Txs from cheating so that Helper-Txs are self-enforced to reveal the truth. Jamming detection is investigated in our previous work [40], where the EC is adopted to detect whether the artificial noise is absent or present by using an energy detection method. In Section 5, we adopt trust management to evaluate the trustworthiness of Helper-Tx and select a trustworthy jammer.

## 4. Auction Scheme

In this section, we utilize the reverse auction scheme to incentivize Helper-Txs to report their private information truthfully. In the reverse auction scheme, the number of jammers ( $K$ ) is a critical parameter for the jammer selection. Therefore, we first investigate the optimal number of  $K$  so that the BS can select an appropriate number of Helper-Txs as jammers. Next, we consider the utility design of the reverse

auction scheme in the CP case and UBM case. In both two cases, we prove that the reverse auction scheme satisfies IC and IR.

**4.1. Optimal Number of Jammers.** In this paper, it is assumed that Helper-Txs are independent and competing with each other. Therefore, we do not consider that there is cooperation between  $K$  jammers. Furthermore, if there is cooperation between multiple Helper-Txs, then we consider these cooperative Helper-Txs as a more powerful Helper-Tx that is competing with other Helper-Txs. It can be obtained that different  $K$  can lead to different results in the total secrecy rate. In this paper, we only investigate the optimal number of jammers in the case with perfect CSI, provided that the result is no difference from the case with statistical CSI. Specifically, in the case with perfect CSI, we can obtain the achieved SINRs of Helper-Tx <sub>$n$</sub>  at user<sub>1</sub> and Eve as

$$\begin{aligned}\gamma_{u,n} &= \frac{\text{Tr}(\mathbf{W}_b \mathbf{H}_{b,u})}{\text{Tr}(\mathbf{W}_{j_n} \mathbf{H}_{j_n,u}) + \delta_u^2}, \\ \gamma_{e,n} &= \frac{\text{Tr}(\mathbf{W}_b \mathbf{H}_{b,e})}{\text{Tr}(\mathbf{W}_{j_n} \mathbf{H}_{j_n,e}) + \delta_e^2},\end{aligned}\quad (2)$$

where  $\mathbf{H}_{b,u} = \mathbf{h}_{b,u} \mathbf{h}_{b,u}^H$ ,  $\mathbf{H}_{b,e} = \mathbf{h}_{b,e} \mathbf{h}_{b,e}^H$ ,  $\mathbf{H}_{j_n,u} = \mathbf{h}_{j_n,u} \mathbf{h}_{j_n,u}^H$ ,  $\mathbf{H}_{j_n,e} = \mathbf{h}_{j_n,e} \mathbf{h}_{j_n,e}^H$ ,  $\mathbf{W}_b = \mathbf{w}_b \mathbf{w}_b^H$ , and  $\mathbf{W}_{j_n} = \mathbf{w}_{j_n} \mathbf{w}_{j_n}^H$ .

The achievable secrecy rate is defined as the transmission rate at which Eve is unable to decode the transmitted message [41]. It is equal to the capacity difference between the data link and the wiretap link. Thus, the secrecy rate achieved by Helper-Tx <sub>$n$</sub>  can be calculated as

$$R_{s,n} = [\log_2(1 + \gamma_{u,n}) - \log_2(1 + \gamma_{e,n})]^+. \quad (3)$$

Let  $q_n = \gamma_{u,n}/\gamma_{e,n}$ . Sort  $q_n$  in a descending order, and get  $q_1 \geq q_2 \cdots \geq q_N$ ,  $q_n \in \{q_1, q_2, \dots, q_N\}$ . Based on (3), we can obtain that the Helper-Tx which has a larger  $q_n$  also has a larger  $R_{s,n}$ . It is assumed that Helper-Tx<sub>1</sub> is the best jammer which has the largest secrecy rate, Helper-Tx<sub>2</sub> is the second best, and so forth. Thus, the jammer selection scheme is designed as follows:

*Step 1.* Select Helper-Tx<sub>1</sub> as a jammer. Let  $n = 1$  and calculate  $\Psi_1 = (1 + \gamma_{u,1})/(1 + \gamma_{e,1})$ .

*Step 2.* For  $1 \leq n \leq N - 1$ , calculate  $\Psi_{n+1} = (1 + \gamma_{u,\{1,2,\dots,n+1\}})/(1 + \gamma_{e,\{1,2,\dots,n+1\}})$ , where

$$\begin{aligned}\gamma_{u,\{1,2,\dots,n+1\}} &= \frac{\text{Tr}(\mathbf{W}_b \mathbf{H}_{b,u})}{\sum_{k=1}^{n+1} \text{Tr}(\mathbf{W}_{j_k} \mathbf{H}_{j_k,u}) + \delta_u^2}, \\ \gamma_{e,\{1,2,\dots,n+1\}} &= \frac{\text{Tr}(\mathbf{W}_b \mathbf{H}_{b,e})}{\sum_{k=1}^{n+1} \text{Tr}(\mathbf{W}_{j_k} \mathbf{H}_{j_k,e}) + \delta_e^2}.\end{aligned}\quad (4)$$

If  $\Psi_n < \Psi_{n+1}$ , proceed to Step 3, and if  $\Psi_n \geq \Psi_{n+1}$ , skip to Step 4.

*Step 3.* Select Helper-Tx <sub>$n+1$</sub>  as jammer, then let  $n = n + 1$  and go back to Step 2.

*Step 4.* Let  $K = n$  and stop.

**Proposition 1.** *The optimal secrecy rate can be achieved by selecting  $K = 1$  Helper-Tx as jammer, where  $K = 1$  is decided by the process above.*

*Proof.* See the appendix.

From the Proposition 1, we can obtain that the BS may only select a single best Helper-Tx as jammer. More than one jammer would lead to a reduction in the secrecy rate of the WCS.

#### 4.2. Utility Design and Objective

**4.2.1. Utility of the BS with Perfect CSI.** For each Helper-Tx <sub>$n$</sub> , the utility of the BS can be characterized as:

$$U_{B,n} = aR_{s,n} - \pi_n R_{s,n} - C_n(P_{j_n}), \quad (5)$$

where  $a$  is the revenue per unit secrecy rate obtained by the BS from a user.  $\pi_n$  is the payment per unit secrecy rate for the jammer.  $C_k(P_{j_n})$  is the monetary cost incurred due to the interference caused by the jammer.

**4.2.2. Utility of the BS with Statistical CSI.** In this section, we focus on the utility design in the case with statistical CSI. As we only know statistical CSI of the wiretap link, the beamforming vectors of the BS and the jammer are both designed as homogeneous isotropic. The CSI of Helper-Tx <sub>$n$</sub>  is denoted as  $g_n = \{\mathbf{h}_{j_n,u}, \delta_{j_n,e}^2\}$ . Specifically, it means that  $\mathbf{h}_{j_n,e}$  have the covariance matrices  $\delta_{j_n,e}^2 \mathbf{I}_{N_j}$  i.e.,  $\mathbf{h}_{j_n,e} \sim \mathcal{CN}(0, \delta_{j_n,e}^2 \mathbf{I}_{N_j})$ .  $\mathbf{h}_{b,e}$  have the covariance matrices  $\delta_{b,e}^2 \mathbf{I}_{N_b}$ , i.e.,  $\mathbf{h}_{b,e} \sim \mathcal{CN}(0, \delta_{b,e}^2 \mathbf{I}_{N_b})$ . In this case, the accurate secrecy rate cannot be calculated. Instead, we calculate the probabilities of the transmission and secrecy outage events. On the basis of the probabilities, the utility of the BS is defined as efficient transmission throughput (ETT), which can be found in our previous work [40].

When Helper-Tx <sub>$n$</sub>  is selected as a jammer, the instantaneous output SINRs at user<sub>1</sub> and Eve are calculated as follows

$$\begin{aligned}\zeta_{u,n} &= \frac{P_b \|\mathbf{h}_{b,u}\|^2}{P_{j_n} \|\mathbf{h}_{j_n,u}\|^2 + \delta_u^2} = \frac{\psi_{b,u}}{\psi_{j_n,u} + 1}, \\ \zeta_{e,n} &= \frac{P_b \|\mathbf{h}_{b,e}\|^2}{P_{j_n} \|\mathbf{h}_{j_n,e}\|^2 + \delta_e^2} = \frac{\psi_{b,e}}{\psi_{j_n,e} + 1},\end{aligned}\quad (6)$$

where

$$\psi_{p,q} = \frac{P_b \|\mathbf{h}_{p,q}\|^2}{\delta_q^2}, p \in \{b, j_n\}, q \in \{u, e\}. \quad (7)$$

In (7),  $P_p = \mathbf{w}_p^H \mathbf{w}_p$  are the transmit powers of the BS and the jammer.  $\psi_{p,q}$  represents the instantaneous signal to noise ratios (SNRs) from node  $p$  to node  $q$ . As the CSI  $\{\mathbf{h}_{b,u}, \mathbf{h}_{j_n,u}\}$  are perfectly known, we can calculate the transmission rate of BS as  $R_{u,n} = \log_2(1 + \zeta_{u,n})$ . For the statistical CSI  $\{\mathbf{h}_{b,e}, \mathbf{h}_{j_n,e}\}$ , according to equation (26) in our previous work [40], we can obtain the probability density function of  $\zeta_{e,n}$  expressed as  $f_{\zeta_{e,n}}(w)$ .

To evaluate the secrecy performance, we adopt Wyner's encoding scheme with the target transmission rate  $\bar{R}_u$  and the target secrecy rate  $\bar{R}_s$  [42]. The difference between  $\bar{R}_u$  and  $\bar{R}_s$  is used as a redundancy rate against eavesdropping. Therefore, the user can decode the received signal with arbitrarily low error rate only if the instantaneous capacity of the user is larger than the transmission rate, i.e.,  $R_{u,n} > \bar{R}_u$ ; otherwise, a transmission outage event occurs. Besides, secrecy outage may occur when the instantaneous capacity of Eve is larger than the redundancy rate, i.e.,  $R_{e,n} = \log_2(1 + \zeta_{e,n}) > \bar{R}_u - \bar{R}_s$ . The probabilities of the transmission and secrecy outage events provided by Helper-Tx <sub>$n$</sub>  are denoted as  $P_{st}^n$  and  $P_{out}^n$ , respectively. We can obtain the probability of transmission event as

$$P_{st}^n = \Pr(R_{u,n} > \bar{R}_u) = \begin{cases} 1, & R_{u,n} > \bar{R}_u, \\ 0, & R_{u,n} \leq \bar{R}_u. \end{cases} \quad (8)$$

The secrecy outage probability can be derived as

$$P_{out}^n = \Pr(\zeta_{e,n} > \xi_e) = \int_{\xi_e}^{+\infty} f_{\zeta_{e,n}}(w) dw, \quad (9)$$

where  $\xi_e = 2^{\bar{R}_u - \bar{R}_s} - 1$ . Thus, the ETT that Helper-Tx <sub>$n$</sub>  can provide is expressed as

$$T_n = R_{u,n} P_{st}^n (1 - P_{out}^n) = \begin{cases} R_{u,n} (1 - P_{out}^n), & R_{u,n} > \bar{R}_u, \\ 0, & R_{u,n} \leq \bar{R}_u. \end{cases} \quad (10)$$

**4.2.3. Utility of the Jammer.** In the perfect CSI case, when Helper-Tx <sub>$n$</sub>  is selected as a jammer, its utility is given by:

$$U_{b_n,n} = \pi_n R_{s,n} - E_n, \quad (11)$$

where  $\pi_n R_{s,n}$  is the payment made by the BS to the jammer.  $E_n$  is the energy cost incurred by the jammer. In the statistical CSI case, the only difference in the utility of jammer is to replace the secrecy rate with ETT. Let  $P_{j_n}$  denotes the transmission power of Helper-Tx <sub>$n$</sub> ; we assume that the energy cost is a linear function of  $P_{j_n}$  and is expressed as:

$$U_{b_n,n} = \pi_n R_{s,n} - b_n P_{j_n}, \quad (12)$$

where  $b_n$  is the cost per unit power, i.e., the valuation that Helper-Tx <sub>$n$</sub>  has for its power. In general, Helper-Tx <sub>$n$</sub>  with a lower battery power would value its power highly and assign a higher  $b_n$ .

**4.2.4. Objective.** In this subsection, our objective is to design reverse auctions for the BS to select a jammer. Specifically, the auction has to satisfy IR and IC. IR means that each Helper-Tx gets a positive utility under any outcome of the auction. An auction satisfies IC if revealing its true valuation ( $b_n$ ) is the dominant strategy for each Helper-Tx. To design reverse auctions that satisfy IC and IR, we consider two cases:

- (a) *CP Case.* In this case, the BS assigns a fixed transmission power ( $P_j^c$ ) to each Helper-Tx. In general, the BS needs to do secrecy rate maximization to design an optimal transmission power of a selected jammer. Although the optimal transmission power design leads to a higher secrecy performance, there is higher computational complexity when the number of Helper-Tx increases. In the process of auction scheme, it is necessary to evaluate the secrecy performance that each Helper-Tx can achieve and selects a suitable one as candidate. In fact, the optimal transmission power design needs to be completed on all Helper-Txs. Therefore, for the optimal power allocation design, there is higher computational complexity when the number of Helper-Tx increases. For the constant power case, we can allocate a fixed power to each Helper-Tx and evaluate the secrecy performance of all Helper-Txs. As an alternative, the constant power allocation with lower computational complexity is easier to implement, and the loss in performance is acceptable.
- (b) *UBM Case.* In this case, we aim to design a reverse auction scheme to approximately maximize the utility of the BS.

**4.3. Auction Scheme.** In this section, we present the reverse auction scheme for the CP case and UBM case.

**4.3.1. CP Case.** In the CP case, the Vickrey auction selects a Helper-Tx with the lowest price  $b_n P_{j_n}^c$ . However, the Vickrey auction has several limitations shown as follows:

*Secrecy performance:* the Vickrey auction scheme ignores the secrecy performance achieved by a jammer.

*Utility:* from (5), the utility of the BS is an increasing function of the secrecy rate, which means that the Vickrey auction scheme also ignores the utility of the BS.

*Interference:* the Vickrey scheme does not consider the interference cost to the BS.

To avoid the above limitations, we utilize the reverse auction scheme in the CP case to select a Helper-Tx as a jammer.

**Lemma 2.** *The utility of the auction winner Helper-Tx<sub>i</sub> can be given by:*

$$U_{b_i,i} = W_{w_{\min}}^{\lambda_i} R_{s,i}^c - b_i P_j^c, \quad (13)$$

*Proof.* The utility of a selected Helper-Tx<sub>n</sub> is expressed as:

$$U_{b_n,n} = \pi_n R_{s,n} - b_n P_j^c. \quad (14)$$

Each Helper-Tx reports its valuation  $b_n$ , and we calculate the weight of each Helper-Tx as:

$$W_n = \frac{b_n P_j^c}{R_{s,n}^c}, \quad (15)$$

where  $R_{s,n}^c$  is calculated for each Helper-Tx with a fixed transmission power  $P_j^c$ . We denote that

$$w_{\min} = \arg \min_{n \in N} W_n, \quad (16)$$

we select Helper-Tx<sub>w<sub>min</sub></sub> as the auction winner that is functioned as a jammer. For a Helper-Tx<sub>i</sub>, it is assumed that

$$w_{\min}^{\lambda_i} = \arg \min_{n \in N, n \neq i} W_n, \quad (17)$$

where  $w_{\min}^{\lambda_i}$  represents the auction winner when Helper-Tx<sub>i</sub> does not participate in the auction. We define that for the auction winner Helper-Tx<sub>i</sub>, the payment is given by:

$$p_i = W_{w_{\min}}^{\lambda_i} R_{s,i}^c, \quad (18)$$

thus the utility of the auction winner Helper-Tx<sub>i</sub> is calculated as:

$$U_{b_i,i} = W_{w_{\min}}^{\lambda_i} R_{s,i}^c - b_i P_j^c. \quad (19)$$

**Proposition 3.** *The reverse auction in the CP case satisfies IR and IC.*

*Proof.* When Helper-Tx<sub>i</sub> is the auction winner, from (19), we can obtain that

$$U_{b_i,i} = W_{w_{\min}}^{\lambda_i} R_{s,i}^c - b_i P_j^c \geq W_{w_{\min}}^{\lambda_i} R_{s,i}^c - b_i P_j^c = W_i R_{s,i}^c - b_i P_j^c = 0. \quad (20)$$

We can obtain that  $U_{b_n,n} \geq 0$  for Helper-Tx<sub>n</sub> so that participating in the reverse auction is the optimal choice for each Helper-Tx<sub>n</sub>. Thus, the reverse auction in the constant case satisfies IR.

If Helper-Tx<sub>i</sub> is the auction winner whether reporting true valuation  $b_i$  or false valuation  $\hat{b}_i < b_i$ , we can obtain from (19) that Helper-Tx<sub>i</sub> cannot change its utility. In addition, let us consider the case that Helper-Tx<sub>i</sub> is not the auction winner when it reports its true valuation  $b_i$ . We assume that Helper-

Tx<sub>i</sub> is the auction winner when it reports a false valuation  $\hat{b}_i < b_i$ . In this case, we can obtain that

$$\hat{W}_{w_{\min}} < W_{w_{\min}} = W_{w_{\min}}^{\lambda_i}, \quad (21)$$

then, the utility of Helper-Tx<sub>i</sub> is calculated as

$$\hat{U}_{b_i,i} = W_{w_{\min}}^{\lambda_i} R_{s,i}^c - b_i P_j^c = W_{w_{\min}} R_{s,i}^c - b_i P_j^c < 0. \quad (22)$$

Therefore, reporting the true valuation  $\hat{b}_n = b_n$  is the dominant strategy for each Helper-Tx<sub>n</sub>, which means that the reverse auction satisfies IC in the CP case.

In this paper, the utility of the jammer is converted into spectrum resources, i.e., the transmission time in the primary channel. Therefore, we can obtain that

$$\nu U_{b_i,i} = (1 - \beta_i) T, \quad (23)$$

where  $\nu$  is the transmission time per utility of the jammer. Therefore, we can obtain the transmission time fraction of Helper-Tx<sub>i</sub> expressed as:

$$\beta_i = 1 - \frac{\nu U_{b_i,i}}{T} = 1 - \frac{\nu (W_{w_{\min}}^{\lambda_i} R_{s,i}^c - b_i P_j^c)}{T}. \quad (24)$$

**4.3.2. UBM Case.** In the UBM case, we aim to approximately maximize the BS's utility. As the Vickrey auction does not specify how the transmit power of the jammer, it is not applicable in this case. Therefore, in this subsection, we utilize the reverse auction scheme in the case that BS requests a jammer to transmit at a power that approximately maximize the BS's utility.

Let  $P_{j_n}$  denote the power at which the BS requires Helper-Tx<sub>n</sub> to transmit. The utility of Helper-Tx<sub>n</sub> can be expressed as:

$$U_{b_n,n} = \pi_n R_{s,n} - b_n P_{j_n}. \quad (25)$$

The utility of the BS can be calculated as:

$$U_{B,n} = (a - \pi_n) R_{s,n} - C_n (P_{j_n}). \quad (26)$$

As the reverse auction satisfies IR, we can obtain that  $U_{b_n,n} \geq 0$ , i.e.,  $\pi_n R_{s,n} \geq b_n P_{j_n}$ . From (26), the utility of the BS is maximized when  $\pi_n R_{s,n} = b_n P_{j_n}$ ; thus, the maximum contribution to the utility of the BS when Helper-Tx<sub>n</sub> is selected as a jammer and transmits at power  $P_{j_n}$  can be expressed as:

$$U_{B,n} = a R_{s,n} - b_n P_{j_n} - C_n (P_{j_n}). \quad (27)$$

In (34), the only variable is  $P_{j_n}$ ; thus, we aim to find the optimal transmit power to maximizes  $U_{B,n}$ . Specifically, we focus the secrecy rate maximization to obtain the optimal transmit power to approximately maximize the utility of the BS. To obtain the optimal secrecy rate, we formulate an

optimal beamforming design problem, which is divided into a two-part optimization problem. By solving this two-part optimization problem, we can obtain the optimal beamforming vectors of the BS and the jammer.

When a Helper-Tx (e.g., Helper-Tx<sub>n</sub>) is selected as a jammer, the achievable secrecy rate can be calculated as

$$R_{s,n} = [\log_2(1 + \gamma_{u,n}) - \log_2(1 + \gamma_{e,n})]^+. \quad (28)$$

where

$$\begin{aligned} \gamma_{u,n} &= \frac{\text{Tr}(\mathbf{W}_b \mathbf{H}_{b,u})}{\text{Tr}(\mathbf{W}_{j_n} \mathbf{H}_{j_n,u}) + \delta_u^2}, \\ \gamma_{e,n} &= \frac{\text{Tr}(\mathbf{W}_b \mathbf{H}_{b,e})}{\text{Tr}(\mathbf{W}_{j_n} \mathbf{H}_{j_n,e}) + \delta_e^2}, \end{aligned} \quad (29)$$

where  $\mathbf{H}_{j_n,u} = \mathbf{h}_{j_n,u} \mathbf{h}_{j_n,u}^H$  and  $\mathbf{H}_{j_n,e} = \mathbf{h}_{j_n,e} \mathbf{h}_{j_n,e}^H$ .

To obtain the optimal beamforming vectors of the BS and Helper-Tx<sub>n</sub>, the secrecy rate maximization problem is mathematically characterized as

$$2 \max_{\mathbf{W}_b, \mathbf{W}_{j_n}} R_{s,n}, \quad (30a)$$

$$\text{s.t. } \text{Tr}(\mathbf{W}_{j_n} \mathbf{H}_{j_n,u}) \leq \Gamma, \quad (30b)$$

$$\text{Tr}(\mathbf{W}_b) \leq P_b^m, \quad (30c)$$

$$\text{Tr}(\mathbf{W}_{j_n}) \leq P_j^m, \quad (30d)$$

$$\text{rank}(\mathbf{W}_b) = 1, \quad (30e)$$

$$\text{rank}(\mathbf{W}_{j_n}) = 1, \quad (30f)$$

where (30b) is the interference temperature limit ( $\Gamma$ ) imposed at user<sub>1</sub> from the jammer. (30c) and (30d) are the transmit power limits of the BS and Helper-Tx<sub>n</sub>, respectively. (30e) and (30f) are rank-one constraints of beamforming vectors  $\mathbf{W}_b$  and  $\mathbf{W}_{j_n}$ , respectively. Actually, the nulling beamformer designed at Helper-Txs is a suboptimal solution that cannot achieve the optimal secrecy performance, which has been demonstrated in the literature. Specifically, based on (30b), the optimal beamforming vector of artificial noise can guarantee that the resulting interference power at the legitimate user is kept below the interference temperature limit, which can achieve a similar effect to nulling beamformer.

In this subsection, we come up with a solution to the secrecy rate maximization problem. Due to fractional forms in the objective function, problem (30) is nonconvex and difficult to solve. First, we introduce a slack variable  $\tau = \gamma_{e,n}$ , and problem (30) can be equivalently transformed into

$$2 \max_{\mathbf{W}_b, \mathbf{W}_{j_n}, \tau} \frac{1 + \gamma_{u,n}}{1 + \tau}, \quad (31a)$$

$$\text{s.t. } \text{Tr}(\mathbf{W}_b \mathbf{H}_{b,e}) \leq \tau \left( \text{Tr}(\mathbf{W}_{j_n} \mathbf{H}_{j_n,e}) + \delta_e^2 \right), \quad (31b)$$

$$\text{Tr}(\mathbf{W}_{j_n} \mathbf{H}_{j_n,u}) \leq \Gamma, \quad (31c)$$

$$\text{Tr}(\mathbf{W}_b) \leq P_b^m, \quad (31d)$$

$$\text{Tr}(\mathbf{W}_{j_n}) \leq P_j^m, \quad (31e)$$

$$\text{rank}(\mathbf{W}_b) = 1, \quad (31f)$$

$$\text{rank}(\mathbf{W}_{j_n}) = 1. \quad (31g)$$

Based on [39], problem (31) can be solved optimally by reformulating it into a two-part optimization problem. The outer part is a one-dimensional line search problem with  $\tau$ , i.e.,

$$f(\tau) = \max_{\tau} \frac{1 + G(\tau)}{1 + \tau}, \quad (32a)$$

$$\text{s.t. } 0 \leq \tau \leq \text{Tr}(\mathbf{H}_{b,u}) P_b^m,$$

where  $G(\tau)$  is the objective function of the inner part optimization problem to be described below. The lower bound about  $\tau$  can be obtained directly from (31b), i.e.,  $0 \leq \text{Tr}(\mathbf{W}_b \mathbf{H}_{b,e}) / (\text{Tr}(\mathbf{W}_{j_n} \mathbf{H}_{j_n,e}) + \delta_e^2) \leq \tau$ . The upper bound is derived from the fact that the secrecy rate is greater than or equal to zero, i.e.,  $\tau \leq \text{Tr}(\mathbf{W}_b \mathbf{H}_{b,u}) / (\text{Tr}(\mathbf{W}_{j_n} \mathbf{H}_{j_n,u}) + \delta_u^2) \leq \text{Tr}(\mathbf{H}_{b,u}) P_b^m$ . For a fixed  $\tau$ , the inner part can be expressed as

$$G(\tau) \triangleq \max_{\mathbf{W}_b, \mathbf{W}_{j_n}} \frac{\text{Tr}(\mathbf{W}_b \mathbf{H}_{b,u})}{\text{Tr}(\mathbf{W}_{j_n} \mathbf{H}_{j_n,u}) + \delta_u^2}, \quad (33a)$$

$$\text{s.t. } (36b) - (36g).$$

Suppose that we can obtain  $G(\tau)$  by solving problem (33) for any fixed  $\tau$ . Then, we can solve problem (32) by applying the one-dimensional line search method, e.g., Golden Section Search to the interval  $[0, \text{Tr}(\mathbf{H}_{b,u}) P_b^m]$ . Therefore, the key step lies in computing  $G(\tau)$  for a fixed  $\tau$ , which requires solving the nonconvex problem (33). Applying the semidefinite relaxation (SDR) technique, problem (33) can be solved by dropping two rank-one constraints [43]. When the problem (33) is solved, we can obtain the optimal solution of problem (30), i.e.,  $(\mathbf{W}_b^*, \mathbf{W}_{j_n}^*)$ .

Therefore, the optimal transmit power of jammer is  $P_{j_n}^* = \text{Tr}(\mathbf{W}_{j_n}^*)$ . Then, the maximum contribution to the utility of the BS from the jammer is:

$$U_{B,n}^* = aR_{s,n}^* - b_n P_{j_n}^* - C_n \left( P_{j_n}^* \right). \quad (34)$$

In the reverse auction, each Helper-Tx<sub>n</sub> reports its valuation  $b_n$  to the BS. Then, we calculate the approximately maximized utility of the BS  $U_{B,n}^*$ . We denote that

$$w_{\max} = \arg \max_{n \in N} U_{B,n}^*. \quad (35)$$



In this case, we select Helper-Tx<sub>w<sub>max</sub></sub> as the auction winner. For Helper-Tx<sub>i</sub>, we assume that

$$w_{\max}^i = \arg \max_{n \in \mathcal{N}, n \neq i} U_{B,n}^* \quad (36)$$

When Helper-Tx<sub>i</sub> is the auction winner, the payment is given by:

$$p_i = U_{B,i}^* - U_{B,w_{\max}}^{i*} + b_i P_{j_i}^* \quad (37)$$

Then, the utility of Helper-Tx<sub>i</sub> can be calculated as:

$$U_{b_i,i} = U_{B,i}^* - U_{B,w_{\max}}^{i*} \quad (38)$$

In the UBM case, the reverse auction scheme also satisfies IR and IC. The proof is similar to Proposition 3, which is omitted here.

Similarly, in the UBM case, we can obtain the transmission time fraction of Helper-Tx<sub>i</sub> expressed as:

$$\beta_i = 1 - \frac{v \left( U_{B,i}^* - U_{B,w_{\max}}^{i*} \right)}{T} \quad (39)$$

To ensure that the selected Helper-Tx<sub>w</sub> (auction winner) is trustworthy as a jammer, we would evaluate the Helper-Tx's trustworthiness in the next section.

## 5. Trust Management and Jammer Selection

In this framework, we apply two trustworthiness metrics, i.e., the trust category and the trust degree to evaluate the trustworthiness of Helper-Tx<sub>w</sub>. Based on these two trustworthiness metrics, we can select a trustworthy Helper-Tx as a jammer.

**5.1. Trust Category.** Helper-Tx<sub>w</sub> is given an initial reputation  $r_0$ . In general, the value of  $r_0$  is half less than the maximum value of the reputation, i.e.,  $0 \leq r_0 \leq 0.5$ . The reason is that a high value may bring selfish behavior while a low value may be unfair to a newly joined Helper-Tx.

According to detection results, some policies can be adopted to encourage Helper-Tx<sub>w</sub> to cooperate. Specifically, the EC takes an additive increase/multiplicative decrease (AIMD) mechanism to update Helper-Tx<sub>w</sub>'s reputation based on the energy detection results [44]. The AIMD mechanism consists of reward and penalty; then, Helper-Tx<sub>w</sub>'s reputation can be updated as

$$\begin{aligned} r_{l,w} &= [\rho_1 r_{l-1,w} + \rho_2 (1 - e_{l,w}) - e_{l,w} (\rho_2 p r_{l-1,w})]^+, \\ &= [\rho_1 r_{l-1,w} + \rho_2 (1 - e_{l,w} - e_{l,w} p r_{l-1,w})]^+, \end{aligned} \quad (40)$$

where  $l = 1, 2, 3 \dots R$ ,  $\rho_1$  and  $\rho_2$  are weight factors that satisfy  $\rho_1 + \rho_2 = 1$ . They can be changed based on the requirement of the WCS. When the long term of the reputation plays a more important role, we increase  $\rho_1$ . On the contrary, when the demand for the sensitivity of reputation collection is higher, we increase  $\rho_2$ .  $R$  is the detection round during the

```

Input:  $r_0, R$ ;
Output:  $\alpha_w, C_w$ ;
1: Initialize  $p = 2, \rho_1 = 0.8, \rho_2 = 0.2$ ;
2: Set  $k = 0, l = 1$ ;
3: The reputation evidence of  $l$  round is  $e_{l,w}$ ;
4: repeat
5:    $r_l = [\rho_1 r_{l-1,w} + \rho_2 (1 - e_{l,w} - e_{l,w} p r_{l-1,w})]^+$ ;
6:    $\hat{e} = e_{l,w} \oplus e_{l+1}$ ;
7:   if  $\hat{e} = 1$  then
8:      $k = k + 1$ ;
9:   end if
10:  Set  $l = l + 1$ ;
11:  until  $l \geq R$ ;
12:  if  $(k = 0 \& e_{1,w} = 0)$  then
13:     $C_w = 1$ , A reputable user;
14:  else if  $(k = 1 \& e_{1,w} = 1) \mid (k = 2 \& e_{1,w} = 0)$  then
15:     $C_w = 2$ , an unstable user;
16:  else if  $(k > 2 \& e_{R,w} = 0)$  then
17:     $C_w = 3$ , A selfish user;
18:  else if  $(e_{R,w} = 1)$  then
19:     $C_w = 4$ , A greedy user;
20:  end if
21:  $\alpha_w = 1/R \sum_{l=1}^R r_{l,w}$ ;
22: Return  $\alpha_w, C_w$ .

```

ALGORITHM 1. Classification algorithm.

detection duration  $\tau$ .  $r_{l-1,w}$  is the historical reputation of Helper-Tx<sub>w</sub>, and  $r_{l,w}$  is the updated reputation of Helper-Tx<sub>w</sub>. As shown below,  $e_{l,w} \in \{0, 1\}$  is the reputation evidence of Helper-Tx<sub>w</sub>, which depends on the detection result at round  $l$ . This reputation evidence can determine whether the AIMD mechanism is reward or penalty. When the detection result shows that there is artificial noise ( $\mathcal{H}_1$ ):  $e_{l,w} = 0$ , then an additive increase ( $\rho_2 * 1$ ) for the value of the reputation is used. When the detection result shows there is no artificial noise ( $\mathcal{H}_0$ ):  $e_{l,w} = 1$ , then a multiplicative decrease ( $\rho_2 * p * r_{l,w}$ ) for the value of the reputation is used.

The value of  $p$  is the degree of penalty, which determines how severe is the penalty imposed on Helper-Tx<sub>w</sub>. The basic setting principle of the AIMD mechanism is to slow down the increasing rate and speed up the decreasing rate of the value of reputation.

Based on the number of inflection points of the reputation update curve and the initial reputation evidence, we propose a classification algorithm as shown in Algorithm 1. Then, Helper-Tx<sub>w</sub> can be classified into one of the following four trust categories.

- (i) *A Reputable User.* As shown in Figure 3, if the detection results show that Helper-Tx<sub>w</sub> continuously sends out the artificial noise, the value of its reputation increases gradually to 1. Then, Helper-Tx<sub>w</sub> is considered to be a reputable user.
- (ii) *A Selfish User.* As shown in Figure 4, Helper-Tx<sub>w</sub>'s reputation update curve is serrated, which means that Helper-Tx<sub>w</sub> intermittently sends out the

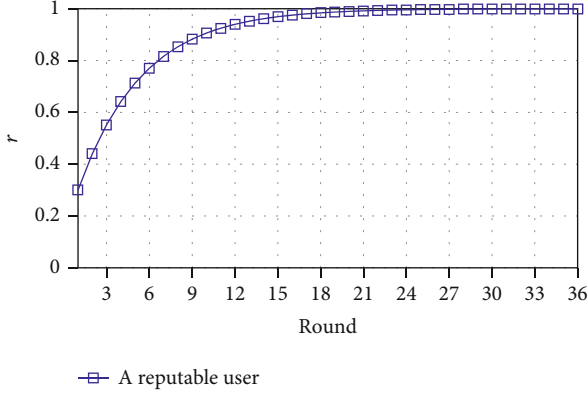


FIGURE 3: A reputable user.

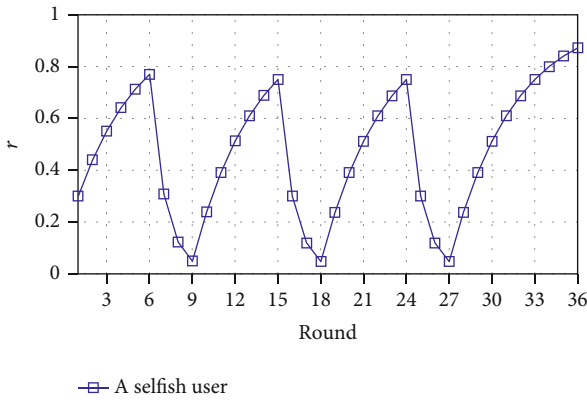


FIGURE 4: A selfish user.

artificial noise. Then, Helper-Tx<sub>w</sub> is considered to be a selfish user.

- (iii) *An Unstable User.* As shown in Figure 5, Helper-Tx<sub>w</sub> does not send the artificial noise for a while, but it recovers quickly and continues sending the artificial noise. It is assumed that the situation is caused by hardware damage or mobility, and Helper-Tx<sub>w</sub> is considered to be an unstable user.
- (iv) *A Greedy User.* As shown in Figure 6, we consider Helper-Tx<sub>w</sub> as a greedy user if it never sends the artificial noise, or it stops sending out the artificial noise in the middle time and never recovers.

**5.2. Trust Degree.** To evaluate the trustworthiness of Helper-Tx<sub>w</sub>, we adopt the concept of trust degree  $\alpha$ . The trust degree of Helper-Tx<sub>w</sub> is calculated by averaging the reputation, shown as

$$\alpha_w = \frac{1}{R} \sum_{l=1}^R r_{l,w}. \quad (41)$$

In the case with perfect CSI, we have to guarantee that Helper-Tx<sub>w</sub> is trustworthy enough to reach the target secrecy performance threshold  $R_s^{\text{th}}$ . In the case with statistical CSI, the target ETT performance threshold is defined as  $T^{\text{th}}$ . The calcu-

lation process of trust degree provides no different from the case with perfect CSI. It means that there is a target trust degree threshold  $\alpha^{\text{th}}$ . Next, we investigate how to calculate this threshold.

We adopt the concept of expected secrecy rate to evaluate the secrecy performance. When Helper-Tx<sub>w</sub> is trusted (the artificial noise is present), the secrecy rate can be expressed as

$$R_{s,w}^t = [\log_2(1 + \gamma_{u,w}^t) - \log_2(1 + \gamma_{e,w}^t)]^+, \quad (42)$$

where the SINRs are expressed as

$$\begin{aligned} \gamma_{u,w}^t &= \frac{\text{Tr}(\mathbf{W}_b^* \mathbf{H}_{b,u})}{\text{Tr}(\mathbf{W}_{j_w}^* \hat{\mathbf{H}}_{j_n,u}) + \delta_p^2}, \\ \gamma_{e,w}^t &= \frac{\text{Tr}(\mathbf{W}_b^* \mathbf{H}_{b,e})}{\text{Tr}(\mathbf{W}_{j_w}^* \hat{\mathbf{H}}_{j_n,e}) + \delta_e^2}. \end{aligned} \quad (43)$$

When Helper-Tx<sub>w</sub> is untrusted (artificial noise is absent), the secrecy rate can be expressed as

$$R_{s,w}^u = [\log_2(1 + \gamma_{u,w}^u) - \log_2(1 + \gamma_{e,w}^u)]^+, \quad (44)$$

where the SINRs are expressed as

$$\begin{aligned} \gamma_{u,w}^u &= \frac{\text{Tr}(\mathbf{W}_b^* \mathbf{H}_{b,u})}{\delta_p^2}, \\ \gamma_{e,w}^u &= \frac{\text{Tr}(\mathbf{W}_b^* \mathbf{H}_{b,e})}{\delta_e^2}. \end{aligned} \quad (45)$$

In this paper, it is assumed that the trust degree  $\alpha_w$  represents the probability that a Helper-Tx sends the artificial noise. Thus, we can obtain the expected secrecy rate as

$$\bar{R}_{s,w} = \alpha_w R_{s,w}^t + (1 - \alpha_w) R_{s,w}^u. \quad (46)$$

For the given target secrecy performance threshold  $R_s^{\text{th}}$ , the expected secrecy rate has to satisfy that

$$\beta_w \bar{R}_{s,w} \geq R_s^{\text{th}}, \quad (47)$$

then we can calculate the target trust degree threshold as

$$\alpha_w \geq \alpha^{\text{th}} = \frac{R_s^{\text{th}} - \beta_w R_s^u}{\beta_w R_s^t - \beta_w R_s^u}. \quad (48)$$

**5.3. Jammer Selection.** According to the classification algorithm, the trust degree of Helper-Tx<sub>w</sub> is updated, and Helper-Tx<sub>w</sub> is classified into one of four trust categories. As shown in Figure 2, Helper-Tx<sub>w</sub> would be selected as a cooperative friendly jammer if the following conditions are achieved at the same time:

- (i) Helper-Tx<sub>w</sub>'s trust degree satisfies that  $\alpha_w \geq \alpha^{\text{th}}$

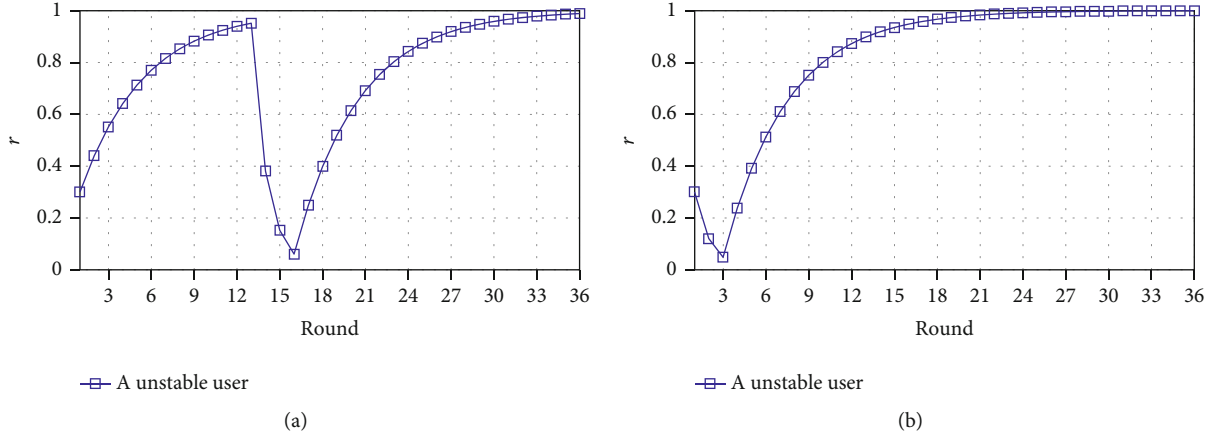


FIGURE 5: An unstable user.

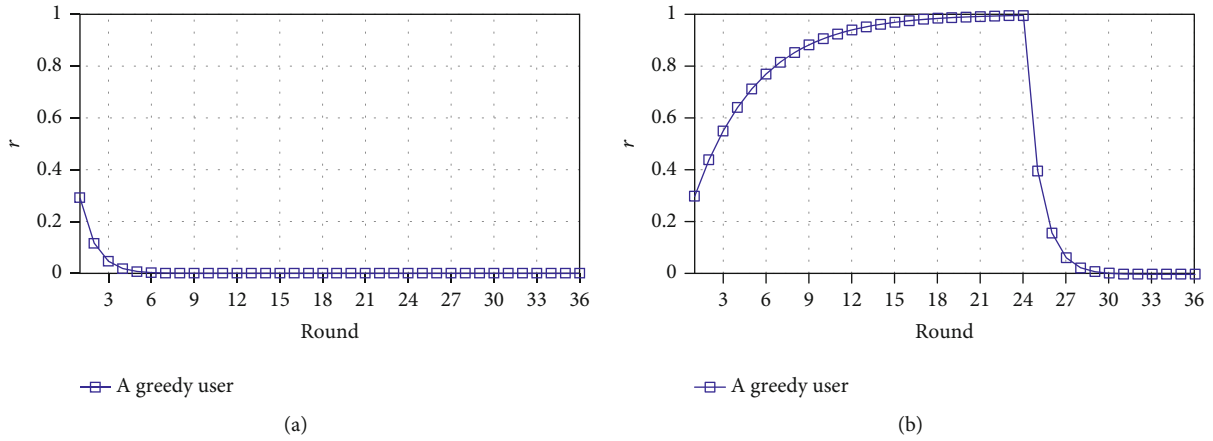


FIGURE 6: A greedy user.

TABLE 1: Simulation parameters.

Simulation parameter	Value
The maximum power of the BS $P_b^m$ (dBm)	30
The maximum power of Helper-Tx $_n$ $P_j^m$ (dBm)	30
The number of antennas of the BS	4
The number of antennas of Helper-Tx $_n$	4
The interference temperature limit imposed at user $_1$ $I$	0.1
The distances between the BS to user $_1$ and Eve $d_{b,u}$ ( $d_{b,e}$ ) (m)	120
The distance between Helper-Tx $_n$ and user $_1$ $d_{j_n,u}$ (m)	150
The distance between Helper-Tx $_n$ and Eve $d_{j_n,e}$ (m)	100
Noise power spectral density $N_{02}$ (dBm/Hz)	-127
Transmission bandwidth $B$ (MHz)	10

(ii) Helper-Tx $_w$  is classified as a reputable user or an unstable user

Otherwise, Helper-Tx $_w$  would be kicked out of the network, and we go back to the auction scheme to select another Helper-Tx.

## 6. Numerical Results

In this section, we present some numerical results of the reverse auction and the AIMD algorithm. In this paper, we consider that the WCS is static at a certain time duration. Therefore, it is assumed that the distances between users

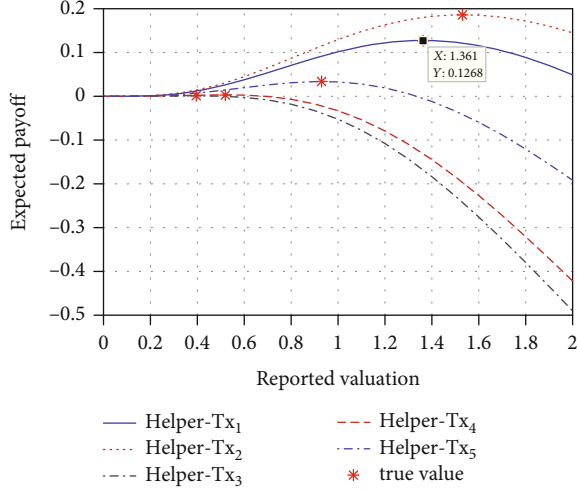
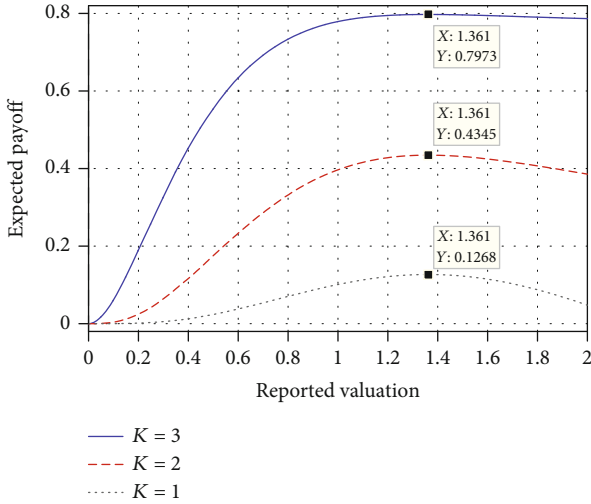


FIGURE 7: The expected payoff versus the reported valuation.

FIGURE 8: Expected payoff versus the reported valuation of Helper-Tx<sub>1</sub> with  $K = 1, 2, 3$ .

are fixed in this time duration, while the results of a static WCS can be well applied to a dynamic WCS. The simulation parameters are shown in Table 1. The values of these parameters are set according to the general guidelines in the existing literatures.

**6.1. Auction Scheme Evaluation.** In the WCS, each Helper-Tx reports its private information to the BS. It is assumed that each Helper-Tx does not know the reported valuation of other Helper-Txs. The reported valuation of each Helper-Tx obeys the probability density function:  $e^{-x_n}$ , where the random variable  $x_n \triangleq v_{-n}(g_{-n})$  ( $x_n \in [0, +\infty)$  and  $\int_0^{+\infty} e^{-x_n} dn = 1$ ). In the simulation, we adopt random variable  $x_k$  instead of calculating  $\pi_n R_{s,n}$  ( $n = 1, 2, \dots, N$ ). This randomly generated variable does not affect the outcome of the mechanism. For simplicity, we assume that the price paid per unit of secrecy rate is  $\pi_n = 1, \forall n$ .

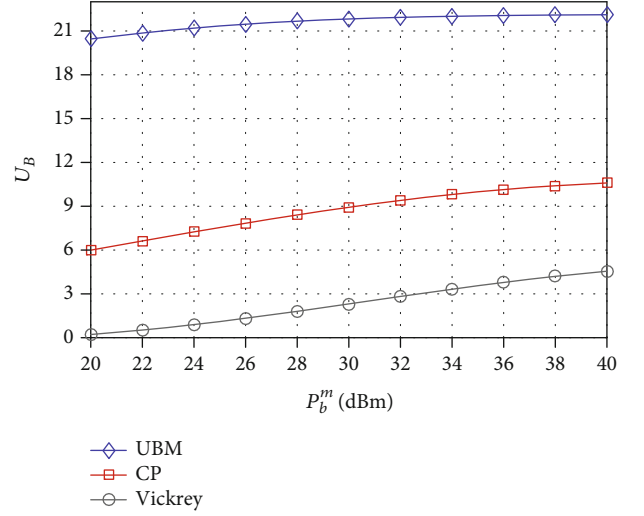


FIGURE 9: The BS utility under the reverse auction scheme and Vickrey auction.

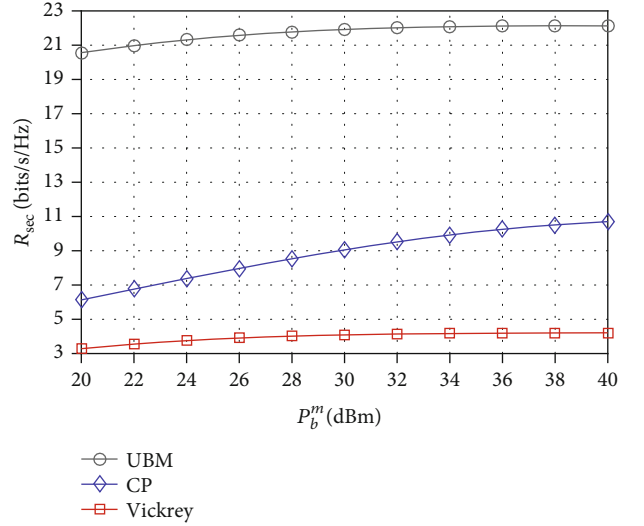


FIGURE 10: The secrecy performance under the reverse auction scheme for CP case and Vickrey auction.

Specifically, we consider a system with  $N = 5$  Helper-Txs, and the BS would select  $K = 1$  jammer. A random sample of these jammers' secrecy rates is obtained as  $[1.3610, 0.5184, 0.3954, 1.5313, 0.9302]$ . Figure 7 shows the expected payoff of each Helper-Tx versus the reported valuation. Specifically, the payoff of each Helper-Tx is the transmission time to access the data link. At each reported valuation, a large number ( $10^6$ ) of sample values is randomly generated to calculate the utility of each Helper-Tx. We can obtain that truth-telling is the dominant strategy in the reverse auction. Each Helper-Tx can expect its maximum payoff when reporting its valuation truthfully. For example, the true valuation of Helper-Tx<sub>2</sub> is 1.3610, and as we can see in Figure 7, Helper-Tx<sub>2</sub> gets the maximum utility 0.1268 when it reports its true valuation. Furthermore, a Helper-Tx with a larger valuation can gain a larger utility. As each selected Helper-Tx<sub>n</sub> has to pay a

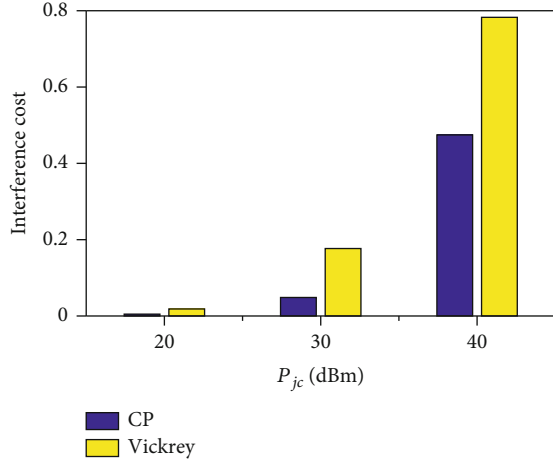


FIGURE 11: The interference cost under the reverse auction scheme for CP case and Vickrey auction.

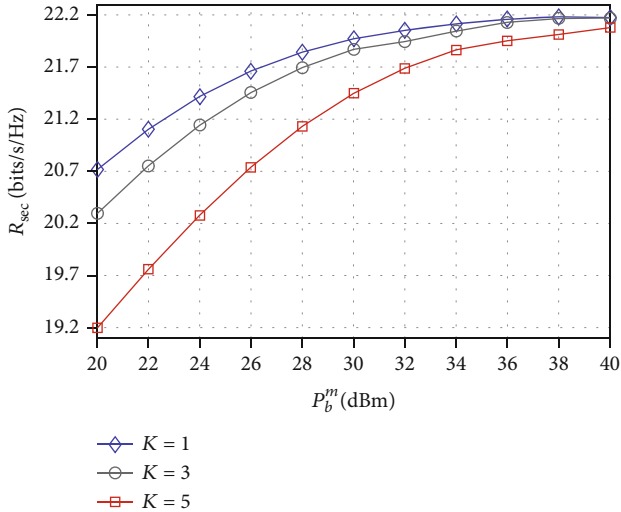


FIGURE 12: Secrecy performance with different number of jammers at the same location.

transfer payment, the maximum expected utility of the Helper-Tx is less than  $u_n(\hat{\mathcal{J}}_n)$ .

In Figure 8, we illustrate the expected utility versus the reported valuation of Helper-Tx<sub>1</sub> with different  $K$ . It is obtained that Helper-Tx<sub>1</sub> gains the maximum expected utility when it reports the true valuation (1.361) with different  $K$ . With  $K$  increases, Helper-Tx<sub>1</sub> gains a higher expected utility. It is because that as  $K$  increases, the probability that Helper-Tx<sub>1</sub> is being selected as a jammer becomes higher. Furthermore, it is observed that when  $K=3$ , the expected utility tends to be fixed as the reported valuation increases.

In Figure 9, we compare the BS's utility under the reverse auction scheme with two cases and the Vickrey auction. It shows that the UBM case outperforms the CP case in terms of the BS's utility. In addition, we can see that for the two cases, the reverse auction scheme outperforms the Vickrey auction scheme. These results show that the reverse auction

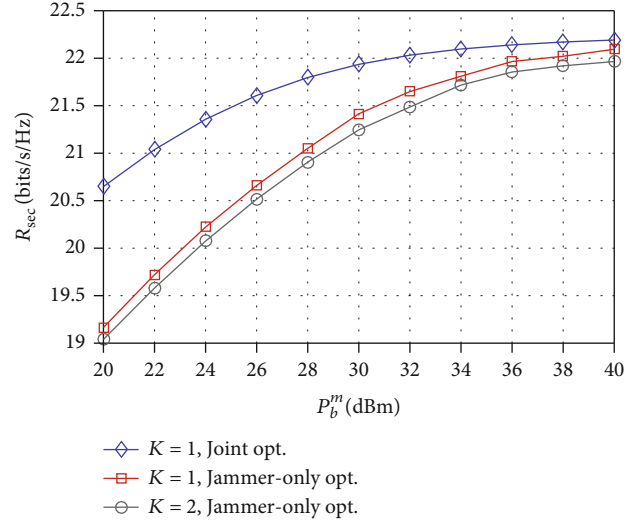


FIGURE 13: Joint beamforming design of the BS and jammers with  $K=1, 2$ .

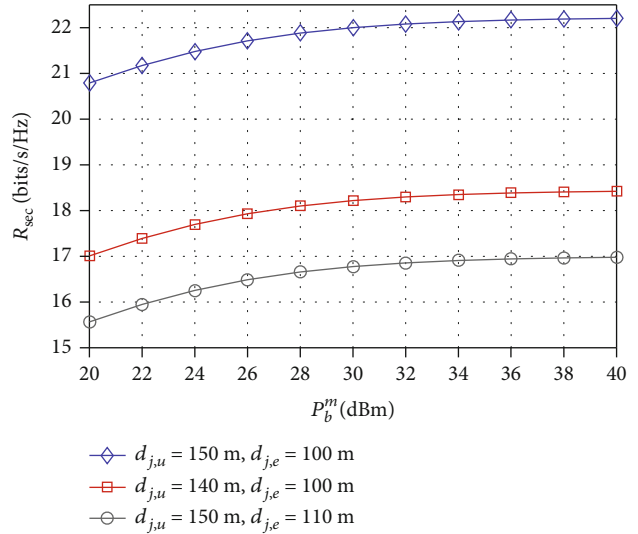


FIGURE 14: Secrecy performance with jammers at different locations.

scheme is valid and has a better performance than the Vickrey auction scheme.

Figure 10 compares the secrecy rate under the reverse auction scheme for UBM case, CP case, and the Vickrey auction scheme. We can see that the reverse auction scheme has a better secrecy performance than the Vickrey auction. It can be explained that our reverse auction takes the secrecy performance of each Helper-Tx into consideration, while the Vickrey auction only considers the price of each Helper-Tx.

In Figure 11, we illustrate the interference cost under CP case and the Vickrey auction scheme. In the UBM case, there is almost no interference cost and can be ignored. It shows that as the transmission power of jammer increases, a higher interference cost is incurred to the BS. In addition, the Vickrey auction scheme causes more interference cost to the BS than the reverse auction scheme. This result shows



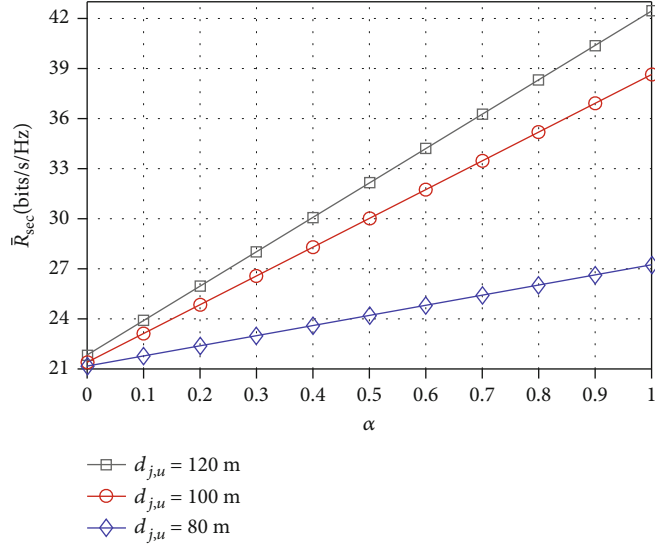


FIGURE 15: The expected secrecy rate versus the trust degree with different  $d_{j,u}$ .

that the reverse auction scheme has a better performance to degrade the interference to the BS.

**6.2. Optimal Beamforming Evaluation in the UBM Case.** In this subsection, we focus on the joint beamforming optimization of the BS and jammers. In Figure 12, we illustrate the total secrecy rate versus the transmitted power of the BS with  $K = 1, 3, 5$  jammers at the same location ( $d_{j,k,p} = 150$  m,  $d_{j,k,e} = 100$  m). It is observed that with the number of jammers increases, the secrecy rate decreases. It means that more jammers can not further improve the secrecy rate. This figure validates the Proposition 1, where the optimal secrecy rate can be achieved by selecting a one best Helper-Tx as jammer, i.e.,  $K = 1$ .

In Figure 13, we compare the secrecy performance of the proposed algorithm (“Joint opt.” in the figure) with the jammer-only optimization (“Jammer-only opt.”) algorithm. In the proposed algorithm, both the beamforming vector of the BS ( $\mathbf{w}_b$ ) and the beamforming vector of the jammer ( $\mathbf{w}_j$ ) are optimized. In the jammer-only optimization algorithm, the beamforming vector of the BS ( $\mathbf{w}_b$ ) is designed as homogeneous isotropic, and only the beamforming vector of the jammer  $\mathbf{w}_j$  is optimized. Figure 13 shows the performance improvement by the proposed joint optimization algorithm compared with the jammer-only optimization algorithm. In this figure, we select  $K = 1$  and  $K = 2$  jammers at the same location with the jammer-only optimization algorithm. We can obtain that in jammer-only optimization algorithm, more jammers cannot cause more interference to Eve.

In Figure 14, we illustrate the secrecy rate of Helper-Txs at different locations. The location of a Helper-Tx represents its private information (the CSI). It is obvious to see that the secrecy rate would be worse when  $d_{j,p}$  decreases or  $d_{j,e}$  increases. It can be explained that when  $d_{j,p}$  decreases or  $d_{j,e}$  increases, the jammer would cause more interference to the data link or less interference to the wiretap link, respec-

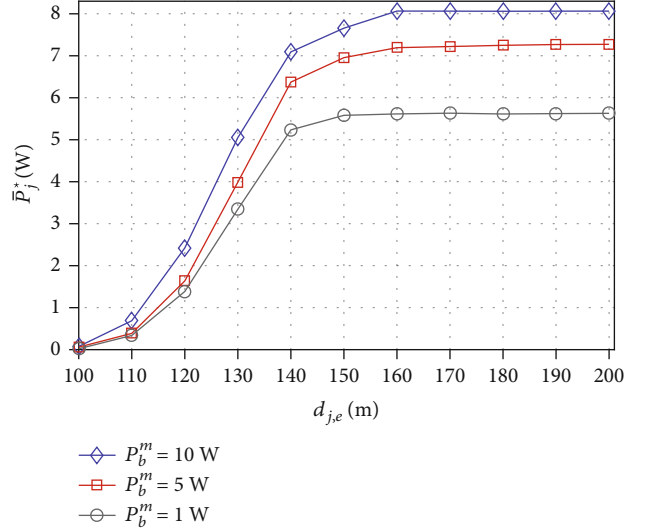


FIGURE 16: The optimal transmitted power of the jammer  $\bar{P}_j^*$  versus  $d_{j,e}$ .

tively. This result shows that the location of a Helper-Tx is critical to be selected as a jammer. Thus, a mechanism to make sure each Helper-Tx reports their CSI truthfully is the main task in a jammer selection scheme.

Figure 15 illustrates the performance comparison with regard to the trust degree for different distances between the jammer and user<sub>1</sub>. As we can see, the expected secrecy rate increases with a higher trust degree. Thus, we consider a Helper-Tx with a higher trust degree as a more trustworthy friendly jammer. Besides, Figure 15 also leads us to the conclusion that we can get a better expected secrecy rate when the jammer is farther to user<sub>1</sub>. The reason is that jammer would cause more interference when it is closer to user<sub>1</sub>, which means the distance is also an important design parameter in the jammer selection scheme.

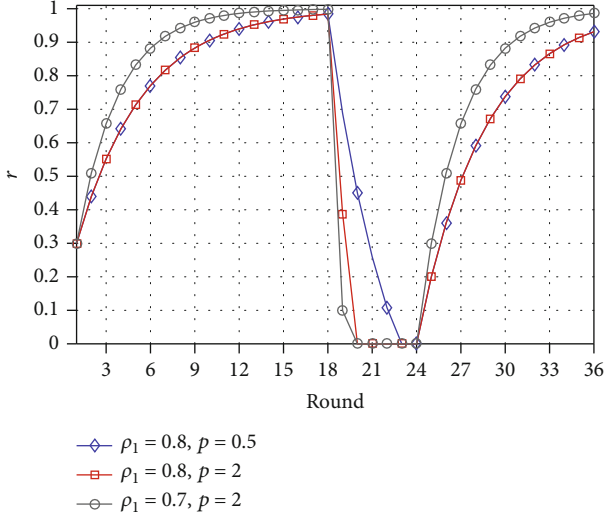


FIGURE 17: An unstable user: reputation update with different AIMD mechanisms.

In this paper, the jamming distance is defined as the distance between the friendly jammer and Eve, i.e.,  $d_{j,e}$ . It is assumed that Eve is one of legitimate users; thus, we can obtain the jamming distance. In Figure 16, we illustrate the optimal transmit power of the jammer over different maximum power of the BS ( $P_b^m$ ). Obviously, as  $P_b^m$  increases, the jammer should transmit the artificial noise with a higher power. The reason is that the transmitted message of a higher power needs more artificial noise to protect. Figure 16 also shows that with the jamming distance increases, a higher transmit power  $\bar{P}_j^*$  of the friendly jammer is required. Then, there is a higher upper bound of the jammer's residual energy. In other words, a jammer farther away from Eve should have more residual energy to guarantee the secrecy performance.

**6.3. AIMD Mechanism Evaluation.** In Figure 17, taking an unstable user as an example, we illustrate the reputation update process with different kinds of AIMD mechanisms. As we can see in Figure 17, when  $\rho_1$  goes up and  $\rho_2$  goes down, both the rates of increasing and decreasing slow down. In such a situation, the historical reputation plays a more important role while the AIMD mechanism is not sensitive to current reputation. Figure 17 also leads us to the conclusion that when  $p$  decreases, the rate of increasing stays the same while the rate of decreasing slows down. As the value of  $p$  is the degree of penalty, and it is related to the damage level caused by selfish behavior of a jammer. Thus, a lower value of  $p$  means a lower penalty while the reward stays the same.

## 7. Conclusion

This paper presents a trustworthy friendly jammer selection scheme with truth-telling for WCS. We develop a reverse auction scheme to enforce truth-telling as the dominant strategy for each Helper-Tx. We prove that the BS can achieve the highest secrecy rate by selecting a one best

Helper-Tx as the jammer. Furthermore, we introduce trust category and trust degree to evaluate the trustworthiness of each Helper-Tx. We then design a selection scheme based the trust category and trust degree for the EC to select a one best Helper-Tx. Lastly, we present numerical results to demonstrate the performance of our proposed jammer selection scheme. As a part of our future work, we plan to investigate the problem of joint relay and jammer selection in the WCS.

## Appendix

### Proof of Proposition 1

According to (3), the secrecy rate of the WCS when selecting  $n$  Helper-Txs can be expressed as  $R_s\{\mathcal{F}_n\} = \log_2(\Psi_n)$ . When  $n = K$ ,  $\Psi_K$  could be obtained, leading to the largest  $R_s\{\mathcal{F}_K\}$ . As a result, it is the optimal choice to select  $K$  Helper-Txs as jammers in the WCS.

It is assumed that  $\text{Tr}(\mathbf{W}_{j_n} \mathbf{H}_{j_n,u}) \gg \delta_u^2$  and  $\text{Tr}(\mathbf{W}_{j_n} \mathbf{H}_{j_n,e}) \gg \delta_e^2$ . Thus, we can omit  $\delta_u^2$  and  $\delta_e^2$  in the denominator of  $\gamma_{u,n}$  and  $\gamma_{e,n}$ , respectively. As  $q_1 \geq q_2 \cdots \geq q_N$ , we could obtain that

$$\begin{aligned} \frac{\gamma_{u,1}}{\gamma_{e,1}} > \frac{\gamma_{u,2}}{\gamma_{e,2}}, &\Rightarrow \frac{\text{Tr}(\mathbf{W}_{j_1} \mathbf{H}_{j_1,e})}{\text{Tr}(\mathbf{W}_{j_1} \mathbf{H}_{j_1,u})} > \frac{\text{Tr}(\mathbf{W}_{j_2} \mathbf{H}_{j_2,e})}{\text{Tr}(\mathbf{W}_{j_2} \mathbf{H}_{j_2,u})}, \\ &\Rightarrow \text{Tr}(\mathbf{W}_{j_1} \mathbf{H}_{j_1,e}) \text{Tr}(\mathbf{W}_{j_2} \mathbf{H}_{j_2,u}) \\ &\quad - \text{Tr}(\mathbf{W}_{j_1} \mathbf{H}_{j_1,u}) \text{Tr}(\mathbf{W}_{j_2} \mathbf{H}_{j_2,e}) > 0. \end{aligned} \quad (\text{A.1})$$

Then, we obtain the result expressed as

$$\begin{aligned} \frac{\gamma_{u,1}}{\gamma_{e,1}} - \frac{\gamma_{u,\{1,2\}}}{\gamma_{e,\{1,2\}}} &= \frac{\text{Tr}(\mathbf{W}_{j_1} \mathbf{H}_{j_1,e})}{\text{Tr}(\mathbf{W}_{j_1} \mathbf{H}_{j_1,u})} - \frac{\text{Tr}(\mathbf{W}_{j_1} \mathbf{H}_{j_1,e}) + \text{Tr}(\mathbf{W}_{j_2} \mathbf{H}_{j_2,e})}{\text{Tr}(\mathbf{W}_{j_1} \mathbf{H}_{j_1,u}) + \text{Tr}(\mathbf{W}_{j_2} \mathbf{H}_{j_2,u})} > 0, \\ &\Rightarrow \frac{\gamma_{u,1}}{\gamma_{e,1}} - \frac{\gamma_{u,\{1,2\}}}{\gamma_{e,\{1,2\}}} > 0, \Rightarrow \gamma_{u,1} \gamma_{e,\{1,2\}} > \gamma_{e,1} \gamma_{u,\{1,2\}}. \end{aligned} \quad (\text{A.2})$$

It is assumed that  $\gamma_{u,1} \gg 1$  and  $\gamma_{u,\{1,2\}} \gg 1$ . We can compare  $\Psi_1 = (1 + \gamma_{u,1}) / (1 + \gamma_{e,1})$  and  $\Psi_2 = (1 + \gamma_{u,\{1,2\}}) / (1 + \gamma_{e,\{1,2\}})$  as

$$\begin{aligned} \frac{\Psi_1}{\Psi_2} &= \frac{(1 + \gamma_{u,1})(1 + \gamma_{e,\{1,2\}})}{(1 + \gamma_{e,1})(1 + \gamma_{u,\{1,2\}})} \approx \frac{\gamma_{u,1}(1 + \gamma_{e,\{1,2\}})}{\gamma_{u,\{1,2\}}(1 + \gamma_{e,1})} \\ &= \frac{(1/\gamma_{u,\{1,2\}}) + (\gamma_{e,\{1,2\}}/\gamma_{u,\{1,2\}})}{(1/\gamma_{u,1}) + (\gamma_{e,1}/\gamma_{u,1})} \approx \frac{\gamma_{e,\{1,2\}}/\gamma_{u,\{1,2\}}}{\gamma_{e,1}/\gamma_{u,1}} \\ &= \frac{\gamma_{u,1} \gamma_{e,\{1,2\}}}{\gamma_{e,1} \gamma_{u,\{1,2\}}} > 1 \Rightarrow \Psi_1 > \Psi_2. \end{aligned} \quad (\text{A.3})$$

Thus,  $K = 1$  is the optimal choice in the jammer selection scheme, which completes the proof of Proposition 1.

### Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

### Conflicts of Interest

The authors declare that they have no conflicts of interest.

### Acknowledgments

This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant No. 2019JBZ001, in part by the National Natural Science Foundation of China under Grant No. 61871023 and Grant No. 61931001, and in part by Beijing Natural Science Foundation under Grant 4202054.

### References

- [1] F. Wang and X. Zhang, "Secure resource allocation for polarization-enabled green cooperative cognitive radio networks with untrusted secondary users," in *2017 51st Annual Conference on Information Sciences and Systems (CISS)*, pp. 1–6, Baltimore, MD, USA, 2017.
- [2] Y. Wen, T. Jing, Y. Huo, Z. Li, and Q. Gao, "Secrecy energy efficiency optimization for cooperative jamming in cognitive radio networks," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, pp. 795–799, Maui, HI, USA, March 2018.
- [3] H.-M. Wang, F. Liu, and M. Yang, "Joint cooperative beamforming, jamming, and power allocation to secure af relay systems," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 10, pp. 4893–4898, 2015.
- [4] S. Cheng, Z. Cai, J. Li, and H. Gao, "Extracting kernel dataset from big sensory data in wireless sensor networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 29, no. 4, pp. 813–827, 2016.
- [5] L. Wang and H. Wu, "Jamming partner selection for maximizing the worst D2D secrecy rate based on social trust," *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 2, p. e2992, 2017.
- [6] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6259–6274, 2016.
- [7] X. Zheng, Z. Cai, J. Li, and H. Gao, "A study on application-aware scheduling in wireless networks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 7, pp. 1787–1801, 2016.
- [8] Z. He, Z. Cai, S. Cheng, and X. Wang, "Approximate aggregation for tracking quantiles and range countings in wireless sensor networks," *Theoretical Computer Science*, vol. 607, pp. 381–390, 2015.
- [9] Z. Cai, X. Zheng, and J. Yu, "A differential-private framework for urban traffic flows estimation via taxi companies," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6492–6499, 2019.
- [10] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2016.
- [11] Z. Cai, R. Goebel, and G. Lin, "Size-constrained tree partitioning: approximating the multicast k-tree routing problem," *Theoretical Computer Science*, vol. 412, no. 3, pp. 240–245, 2011.
- [12] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1027–1053, 2017.
- [13] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: theories, technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2017.
- [14] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2018.
- [15] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2734–2771, 2018.
- [16] S. Sohaib and M. Uppal, "Full-duplex compress-and-forward relaying under residual self-interference," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 3, pp. 2776–2780, 2018.
- [17] Z. Chen, P. Fan, and D. O. Wu, "Joint power allocation and strategy selection for half-duplex relay system," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2144–2157, 2017.
- [18] X. Hu, P. Mu, B. Wang, and Z. Li, "On the secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4457–4462, 2017.
- [19] H. Lee, S. Eom, J. Park, and I. Lee, "UAV-aided secure communications with cooperative jamming," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 10, pp. 9385–9392, 2018.
- [20] Q. Wang, F. Zhou, R. Q. Hu, and Y. Qian, "Energy-efficient beamforming and cooperative jamming in IRS-assisted miso networks," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1–7, Dublin, Ireland, Ireland, June 2020.
- [21] Y. Su, X. Lu, Y. Zhao, L. Huang, and X. Du, "Cooperative communications with relay selection based on deep reinforcement learning in wireless sensor networks," *IEEE Sensors Journal*, vol. 19, no. 20, pp. 9561–9569, 2019.
- [22] J. Xing, T. Lv, and X. Zhang, "Cooperative relay based on machine learning for enhancing physical layer security," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1–6, Istanbul, Turkey, Turkey, September 2019.
- [23] N. Zhang, N. Cheng, N. Lu, X. Zhang, J. W. Mark, and X. S. Shen, "Partner selection and incentive mechanism for physical layer security," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4265–4276, 2015.
- [24] Z. He, Z. Cai, and J. Yu, "Latent-data privacy preserving with customized data utility for social network data," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 665–673, 2017.

- [25] M. Wen, K. Zhang, J. Lei, X. Liang, R. Deng, and X. Shen, "CIT: a credit-based incentive tariff scheme with fraud-traceability for smart grid," *Security and Communication Networks*, vol. 9, no. 9, pp. 823–832, 2016.
- [26] Z. He, Z. Cai, J. Yu, X. Wang, Y. Sun, and Y. Li, "Cost-efficient strategies for restraining rumor spreading in mobile social networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2789–2800, 2016.
- [27] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: interaction between source, eavesdropper, and friendly jammer," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, 2009.
- [28] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 310–320, 2012.
- [29] Rongqing Zhang, Lingyang Song, Zhu Han, and Bingli Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3693–3704, 2012.
- [30] Y. Wang, Z. Cai, G. Yin, Y. Gao, X. Tong, and G. Wu, "An incentive mechanism with privacy protection in mobile crowdsourcing systems," *Computer Networks*, vol. 102, pp. 157–171, 2016.
- [31] J. Deng, R. Zhang, L. Song, Z. Han, and B. Jiao, "Truthful mechanisms for secure communication in wireless cooperative system," *IEEE Transactions on Wireless Communications*, vol. 12, no. 9, pp. 4236–4245, 2013.
- [32] Z. Duan, W. Li, X. Zheng, and Z. Cai, "Mutual-preference driven truthful auction mechanism in mobile crowdsensing," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 1233–1242, Dallas, TX, USA, USA, July 2019.
- [33] M. R. Khandaker, K.-K. Wong, and G. Zheng, "Truth-telling mechanism for two-way relay selection for secrecy communications with energy-harvesting revenue," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3111–3123, 2017.
- [34] D. H. Ibrahim, E. S. Hassan, and S. A. El-Dolil, "Relay and jammer selection schemes for improving physical layer security in two-way cooperative networks," *computers & security*, vol. 50, pp. 47–59, 2015.
- [35] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, "Power-constrained secrecy rate maximization for joint relay and jammer selection assisted wireless networks," *IEEE Transactions on Communications*, vol. 65, no. 5, pp. 2180–2193, 2017.
- [36] L. Wang, H. Wu, and G. L. Stuber, "Cooperative jamming-aided secrecy enhancement in p2p communications with social interaction constraints," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1144–1158, 2017.
- [37] F. Gao, R. Zhang, Y.-C. Liang, and X. Wang, "Optimal design of learning based mimo cognitive radio systems," in *2009 IEEE International Symposium on Information Theory (ISIT)*, pp. 2537–2541, Seoul, South Korea, July 2009.
- [38] B. F. Lo, "A survey of common control channel design in cognitive radio networks," *Physical Communication*, vol. 4, no. 1, pp. 26–39, 2011.
- [39] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 35–38, 2013.
- [40] Y. Wen, Y. Huo, L. Ma, T. Jing, and Q. Gao, "A scheme for trustworthy friendly jammer selection in cooperative cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3500–3512, 2019.
- [41] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 28–33, 2013.
- [42] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [43] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 6, pp. 1154–1170, 2015.
- [44] M. Vojnovic, J. Y. Le Boudec, and C. Boutremans, "Global fairness of additive-increase and multiplicative-decrease with heterogeneous round-trip times," in *Proceedings IEEE INFOCOM 2000. Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No. 00CH37064)*, pp. 1303–1312, Tel Aviv, Israel, 2000.

## Research Article

# Histogram Publication over Numerical Values under Local Differential Privacy

Xu Zheng <sup>1,2</sup>, Ke Yan <sup>1,2</sup>, Jingyuan Duan,<sup>1</sup> Wenyi Tang,<sup>1</sup> and Ling Tian<sup>1,2</sup>

<sup>1</sup>School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

<sup>2</sup>Trusted Cloud Computing and Big Data Key Laboratory of Sichuan Province, Chengdu 610000, China

Correspondence should be addressed to Ke Yan; [kyan@uestc.edu.cn](mailto:kyan@uestc.edu.cn)

Received 17 September 2020; Revised 9 November 2020; Accepted 13 January 2021; Published 8 February 2021

Academic Editor: Yingjie Wang

Copyright © 2021 Xu Zheng et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Local differential privacy has been considered the standard measurement for privacy preservation in distributed data collection. Corresponding mechanisms have been designed for multiple types of tasks, like the frequency estimation for categorical values and the mean value estimation for numerical values. However, the histogram publication of numerical values, containing abundant and crucial clues for the whole dataset, has not been thoroughly considered under this measurement. To simply encode data into different intervals upon each query will soon exhaust the bandwidth and the privacy budgets, which is infeasible for real scenarios. Therefore, this paper proposes a highly efficient framework for differentially private histogram publication of numerical values in a distributed environment. The proposed algorithms can efficiently adopt the correlations among multiple queries and achieve an optimal resource consumption. We also conduct extensive experiments on real-world data traces, and the results validate the improvement of proposed algorithms.

## 1. Introduction

Integrating the IoT with strong intelligent capability has been one major trend of the IoT system design. However, one prominent prerequisite of AI-driven IoT is the ubiquitous support of sensing data [1]. Recently, the pervasive adoption of smart devices provides unprecedented opportunities for data collection, benefiting the development of AI-driven IoTs [2]. However, the severe concerns on privacy have thwarted the data sharing. Therefore, this paper introduces a novel framework for distributed data statistic collection in IoTs, especially the statistics over numerical data.

Within the privacy preserved data collection, local differential privacy [3] has dramatically extended the capability on the derivation of diverse statistic information in distributed manners [4, 5]. It jointly preserves the sensitive information for data contributors under strict privacy preservation, while allowing the absence of a trusted third party as the data coordinator. It is widely accepted that LDP will be the future design principle for distributed data query with strong privacy preservation. Corresponding techniques have already

been adopted by popular systems including Google Chrome [6], where contents are collected to evaluate the frequently visited websites. Currently, the studies are majorly and pervasively conducted on the frequency estimation of categorical data [7] and the mean value estimation for numerical data [8]. In this work, we consider another important topic, the histogram publication for numerical data under LDP, which is both critical and not well-handled.

The histogram provides some essential information for numerical values and can facilitate multiple services [9]. For example, understanding the distribution of health status among populations will be pivotal for policy making, which could be achieved by knowing the scales of exercises through the fitness data. The histograms can also work as a reference for numbers of values in concerned subranges, as they can be estimated via several consecutive bars in histograms. Actually, the histogram provides more abundant knowledge compared to the mean value and summation, especially for its capability on providing the contouring for data distribution. However, to mindlessly share the data for histogram publication will severely breach the privacy for contributors



[10], leading to numerous threats. For instance, the fitness data will reveal many details of a person, resulting in the pushing of spam advertisements and the raising on insurance fees. Fortunately, the local differential privacy provides potential opportunities for privacy-preserved histogram construction among multiple data contributors, even with a malicious data curator [11, 12]. Contributors can publish perturbed values to the data curator, which will aggregate the values and share it with data consumers without gaining significant knowledge on real values.

However, the implementation of the data collection must be carefully designed, as contributors are less willing to consume too much bandwidth and privacy budgets [13]. Firstly, contributors may have to spend their network resources to upload the numerical values to the data curators [14]. This is extremely unwillingness when many consumers request histograms with heterogeneous intervals. The heterogeneous histograms are common for consumers, as they usually hold different granularities of partition on the range. Some of them expect a moderate granularity on the whole range, while others may be interested in fine-grained histograms on some subintervals. Contributors will perturb the data values multiple times since the results are usually not reusable. The data value could fall in different intervals for different queries. Secondly, multiple data consumers may collude with each other and share their results. Then, the privacy of contributors will be pushed to an unexpected risk, due to the compositional property of local differential privacy.

Considering both challenges, current studies on LDP fails to provide rational solutions. Existing works can be categorized into two folds: LDP for categorical values and numerical values. The first fold mainly focuses on the frequency estimation, and they differ in how they achieve a balance between the variance and the bandwidth consumption. However, they are incapable for the histogram publication for numerical values, as there is no inherent category for a numerical value. An encoding result generated for one histogram could be totally inapplicable for another one. The second fold of studies is mainly designed for the mean value estimation over numerical data, where original data are usually perturbed into one of two fixed values [15] under LDP. The perturbed values are gathered by the data curator for estimation. However, there are few studies designed for the histogram publication under LDP.

To mitigate the gap, this paper for the first time thoroughly studies the problem of histogram publication over numerical values under LDP. In our framework, multiple data contributors each hold one numerical data. One semi-honest data collector acts as the data collector, and multiple data consumers post their queries with corresponding granularities on histograms. The data curator will distribute the queries to contributors, who will later upload their noisy contents to derive the requested histograms.

We first propose two algorithms design for single and multiple histogram publication. The algorithms apply the idea of random response and take advantage of the fact that intervals of different histograms can be overlapped. The proposed algorithms are proved to achieve the optimal bandwidth consumption and privacy preservation, thus improv-

ing the efficiency for histogram publication. This paper also theoretically analyzes the accuracy and variance for the derived histogram results, together with the satisfaction on local differential privacy. Finally, we evaluate the performance of all proposed algorithms on real-world datasets, and the results reveal both the high utility and improved efficiency for the published values. As far as we know, this is the first work focusing on the efficient histogram publication for numerical values under LDP. Our main contribution includes the following:

- (i) A novel framework for histogram publication over numerical data in distributed manners
- (ii) Two efficient algorithms for distributed histogram publication under LDP, where both the data curator and consumers are semihonest
- (iii) Theoretical analysis on the accuracy, the efficiency, and the privacy preservation
- (iv) Extensive experiments on real dataset to validate the performance of proposed algorithms

The rest of the paper is organized as follows. Section 2 reviews the literature works. Section 3 proposes the problem formulation and some preliminaries. Section 4 introduces two algorithms for histogram publication. The evaluation results are shown in Section 5. Section 6 concludes the paper.

## 2. Related Work

*2.1. Local Differential Privacy.* Local differential privacy [3] has been currently treated as the standard principle of privacy preservation for distributed data publication. Existing works can be organized into two major categories: the privacy preservation for categorical values and numerical values.

As for the categorical values, Google designs RAPPOR and Basic RAPPOR methods [6] to collect the web logs from users in a private manner. In these methods, the detailed web logs will not be disclosed, while the service provider can still extract reliable information like frequently visited websites. Following the solutions, subsequent studies are conducted both to extend the capability of data collection and to reduce the requested bandwidth. The covered topics include the histogram distribution [16], the general graph structures [17], the outliers [18], range counting [19], and the frequent items [7, 20]. There are also some works [15] trying to conclude current studies on LDP and providing guidelines for applications. The efficiency of these methods is analyzed and discussed. However, these works are majorly designed for categorical values [21], where each data item has an inherent category. As for the numerical values, the extension is nontrivial. Either multiple encoded vectors or extremely large bandwidth is required.

The publication of numerical values [22] has also been studied by several works [23, 24]. Current trends of studies mainly focus on the differentially private estimation of the mean value [8, 25, 26]. Duchi et al. initially propose a

mechanism [8] for numerical data collection under LDP. The mechanism encodes each datum into one of two fixed values, which are later decoded and aggregated for analysis. Some other studies argue that the perturbed values fall out the original ranges, and designs improved mechanisms for better utilities [24]. The publication of other types of data, like the key-value data, is also studied [27]. However, all such methods are majorly designed for mean value estimation and incapable for the histogram publication.

**2.2. Differential Privacy.** The histogram publication is also a typical task for data publication under typical differential privacy [9, 28–31]. These works handle the differentially private releasing of histograms on different types of data structure, including the numerical values, hierarchical structures, general graphs, or other sophisticated schemas [32]. Corresponding mechanisms are proposed to reduce the scale of injected noise. All such methods request the existence of a trusted third party and ignore the bandwidth consumption during data collection.

**2.3. Distributed Privacy-Preserved Data Publication.** The distributed publication of private IoT data [33] has long been considered a primary task and focus. Typical techniques like  $K$ -anonymity are applied where the content held by each participant is at least indistinguishable among other  $K - 1$  participants. These works mainly achieve this by mixing the contents among a group of related participants [34–36]. For example, Palanisamy and Liu [37] propose a method for sensitive location concealing, by exchanging information with users in the same region. However, these studies mainly focus on the location data, which is just one domain of IoT data, the guarantees on privacy are also divergent from the differential privacy.

### 3. Problem Formulation

This section first provides the corresponding settings for the privacy-preserved histogram publication and then introduces some preliminaries on local differential privacy.

**3.1. Problem Formulation.**  $N$  data contributors are involved in the system, denoted as  $\{u_1, u_2, \dots, u_N\}$ . Each contributor  $u_i$  holds one content  $d_i$  to be published. As our framework considers the publication of numerical values, each content  $d_i$  is assumed to fall in the range of  $[D_L, D_U]$ , where  $D_L$  and  $D_U$  stand for the minimum and maximum values.

One *data curator* collects the contents from contributors and publishes them to *data consumers*. Specifically, each data consumer provides  $l_j$  as the length of intervals in histogram queries, constituting the query set  $l_1, l_2, \dots, l_M$ . The data curator first publishes the request to contributors. Upon receiving feedbacks, the data curator aggregates and derives the results for different queries. It allocates each received content  $d_i$  into the  $k$ th interval  $C_{jk}$  for  $j$ th query, where  $D_L + (C_{jk} - 1)l_j \leq d_i \leq D_L + C_{jk}l_j$ . The aggregated counting  $R_{jk}$ s are returned to different data consumers as the final outputs. As for each data contributor, the total bandwidth spent on the uploading of  $d_i$  is denoted as  $B_i$ .

**3.1.1. Adversarial Model.** In our framework, the data curator and the consumers are both malicious. They are honest-but-curious, which means they will infer the true values upon receiving the results. In this work, we adopt the local differential privacy as the measurement for privacy preservation. LDP allows the arbitrary background knowledge of adversaries while preserving the private contents for data owners. With LDP, a data contributor  $u_i$  will publish a noisy version of the content  $d_i$  to the data curator, which could be either a value or some relative data structure. The formal definition of local differential privacy is shown in Definition 1.

**Definition 1** (local differential privacy). An algorithm  $Q(\cdot)$  satisfies  $\epsilon$ -local differential privacy ( $\epsilon$ -LDP) where  $\epsilon \geq 0$ , if and only if for two arbitrary contents  $T_i$  and  $T_j$ ,

$$\forall y \in \text{Range}(Q): \Pr [Q(T_i) = y] \leq e^\epsilon \Pr [Q(T_j) = y], \quad (1)$$

where  $\text{Range}(Q)$  denotes the set of all possible outputs of  $Q(\cdot)$ .

Intuitively, the local differential privacy ensures no significant information will be disclosed to the data receivers with arbitrary background knowledge. The parameter indicates the degree of privacy, where a larger means data contributors are less sensitive and will produce more accurate results.

**3.1.2. Design Object.** In our framework, the data contributors try to minimize their bandwidth consumption during the data uploading, while their privacy preservation is guaranteed. The data curator and consumers try to maintain the high utility for the derived histograms. Corresponding results should be both accurate and stable. Generally, the optimization goal is formulated as follows:

$$\begin{aligned} \min \quad & \sum_{i=1}^N B_i \\ \text{s.t.} \quad & E(R'_{jk}) = R_{jk}, \quad \forall l_1, l_2, \dots, l_M \end{aligned} \quad (2)$$

$d_i$  is preserved under LDP,  $\forall i \in \{1, 2, \dots, N\}$ .

**3.2. Preliminaries.** Local differential privacy has been applied as the fundamental method for distributed content collection with strong privacy preservation. The random response method provides some basic idea for the implementation of this property. We take the Basic RAPPOR as an example, which is designed for the publication of categorical data.

In Basic RAPPOR, assume there is a  $L$ -bits vector with binary entry, denoted as  $V = (v_1, v_2, \dots, v_L)$ .  $v_i = 1$  indicates the data item  $d$  belongs to the  $i$ th category; otherwise,  $v_i = 0$ .

Then,  $V^0$  can be generated by randomized response:

$$\Pr [V'[i] = 1] = \begin{cases} 1 - \frac{1}{2}f, & \text{if } V[i] = 1, \\ \frac{1}{2}f, & \text{if } V[i] = 0. \end{cases} \quad (3)$$

Finally,  $V'$ 's will be sent to the data curator for subsequent analysis. Actually, this mechanism of perturbation achieves LDP property for vector  $V$ , which is proved by a previous work [15]:

**Theorem 2.** *For an arbitrary vector  $V = (v_1, v_2, \dots, v_L)$ , the Basic RAPPOR achieves  $\epsilon$ -LDP for  $\epsilon = \ln(((1 - (1/2)f)/(1/2))^2)$ .*

The data sampling, where contributors only partially upload their contents, is also a major strategy for resource saving in distributed data collection. It is believed that this can further reduce the disclosure of information. There are also some works arguing the amplification of the privacy preservation over data sampling. Li et al. have theoretically proved the effect [38], as is given in Theorem 3.

**Theorem 3.** *Assume  $F(\cdot)$  to be an  $\epsilon$ -differentially private algorithm and  $S(\cdot)$  to be a sampling method algorithm. Then if  $S(\cdot)$  is first applied to a dataset, which is later perturbed by  $F(\cdot)$ , the derived result satisfies  $\ln(1 + P_0(e^\epsilon - 1))$ -differential privacy, where  $P_0$  is the sampling probability.*

Finally, the compositional property of differential privacy can also be merged with the LDP.

**Theorem 4** (sequential composition [39]). *Let  $\{F_1(\cdot), F_2(\cdot), \dots, F_k(\cdot)\}$  be a set of functions satisfying differential privacy and the privacy budgets to be  $\epsilon_1, \epsilon_2, \dots, \epsilon_k$ , respectively. Then applying all  $F_i(\cdot)$ 's to one data item  $d_0$  will provide a  $\sum_{i=1}^k \epsilon_i$ -differential privacy.*

## 4. Distributed Histogram Publication under Local Differential Privacy

This section provides the algorithms for histogram publication. It first introduces the algorithm designed for single query; then an efficient algorithm designed for multiple queries is proposed.

**4.1. Baseline Algorithm for Single Query.** The first algorithm helps the data curator collect data from contributors for one single query. The main idea of this algorithm is to first convert the numerical value into categorical version and then applies typical mechanisms like the Basic RAPPOR. This conversion is feasible as a single query will provide a fixed partition on the whole range. We name the algorithm as *Single Histogram Publication* to distinguish it with subsequent methods, SHP for short.

In SHP, the data curator initially receives the query from data consumers, i.e., the width  $l_0$  for each interval in histogram and the privacy budget  $\epsilon_0$ . The data curator pushes the parameters to all data contributors, together with the range  $[D_L, D_U]$ .

**4.1.1. Local Encoding.** Upon receiving the message, each contributor  $u_i$  first encodes her value  $d_i$  into vector

$$D_i = (0, \dots, 0, 1, 0, \dots, 0), \quad (4)$$

where the  $j$ th entry equals 1 when

$$D_L + (j - 1)l_0 \leq d_i \leq D_L + j \cdot l_0. \quad (5)$$

With the vector  $D_i$ , SHP applies the typical perturbation mechanisms like Basic RAPPOR, where

$$f = \frac{2}{e^{\epsilon/2} + 1}. \quad (6)$$

Assume the perturbed vector to be  $D'_i$  and contributor  $u_i$  uploads this vector to the data curator.

**4.1.2. Decoding and Publishing.** The data curator will first collect the vectors from all contributors. Then, it decodes and aggregates the vectors to derive the estimated counting for values in each interval. For each interval  $C_k$ , the number of contents that fall in this slot is calculated as

$$R_k = \frac{\left\| \left\{ D'_i \mid D'_{ik} = 1 \right\} \right\| - 1/2 \cdot f \cdot N}{1 - f}, \quad (7)$$

where  $\|\cdot\|$  indicates the number of elements in the set.

Finally, the data curator publishes the estimated results  $(R_1, R_2, \dots)$  to the data consumer.

**4.1.3. Analysis.** Several properties should be analyzed for the proposed algorithm, including the accuracy for the derived results, the guarantee on privacy preservation, and the efficiency.

Firstly, SHP provides an unbiased estimation for the histogram when applying Basic RAPPOR as the perturbation mechanism. The analysis is as follows: according to the property of the perturbation mechanism, the data curator can aggregate the vectors and derive an unbiased estimation on the histogram, as

$$E(R_k) = R_k^0, \quad (8)$$

where  $R_k^0$  is the original result derived from all vectors  $\{D_1, D_2, \dots, D_N\}$ . Meanwhile, SHP generates each vector  $D_i$  by projecting  $d_i$  into a corresponding interval. Then, the only 1 in  $D_i$  exactly refers to the index of interval  $d_i$  belonging to. Therefore, SHP can provide an unbiased estimation in each interval.

**Theorem 5** (unbiased estimation). *The published result of SHP is an unbiased estimation for the real histogram, i.e.,  $E(R_k) = \|\{d_i \mid D_L + (k - 1)l_0 \leq d_i \leq D_L + k \cdot l_0, \forall_i \leq N\}\|$ .*

Furthermore, the variance of SHP is determined by the applied perturbation mechanism, as generating  $D_i$  will introduce no extra randomness.

Now, we discuss the capability of privacy preservation of SHP. The analysis is also straightforward. The information in  $D_i$  is preserved with local differential privacy, where the privacy budget is  $\epsilon_0$ . Furthermore,  $D_i$  provides identical information with  $d_i$  in the histogram publication, according to the encoding phase. Therefore, SHP can preserve the private content for each contributor with expected differential privacy.

**Theorem 6** (local differential privacy). *SHP can preserve the numerical content of each contributor with  $\epsilon_0$  local differential privacy.*

Finally, we briefly discuss the efficiency of SHP. The bandwidth spent on content uploading is  $O((D_U - D_L)/l_0)$ .

The time complexity for each contributor is also  $O((D_U - D_L)/l_0)$  during the encoding phase and  $O(N \cdot ((D_U - D_L)/l_0))$  for the data curator during the decoding phase.

**4.2. An Efficient Algorithm for Multiple Queries.** This part gives the algorithm for histogram publication towards multiple queries. These queries could be heterogeneous on their widths of intervals, making the data publication nontrivial. To simply apply SHP for each query separately will consume huge bandwidths and privacy budgets. Therefore, the main idea of the proposed algorithm is to implement a single-time publication meeting all queries, to improve the efficiency for contributors. The algorithm is named as *Composited Histogram Publication*, CHP for short.

Initially, the data curator receives the queries from multiple data consumers, each with a set of parameters  $(l_i, \epsilon_i)$ . CHP extracts the minimum privacy budgets  $\epsilon_0 = \min_i \epsilon_i$ , which will provide a most rigorous privacy preservation for contributors. Then, CHP adopts all  $l_i$ s. It first derives intervals for all queries and records the boundaries for these intervals as

$$\{\{W11, W12, \dots, W1K1\}, \{W21, W22, \dots, W1K2\}, \dots, \{WM1, WM2, \dots, WMKM\}\}. \quad (9)$$

Then, CHP arranges all boundaries on one single line in an ascending order. The start point of the line is  $D_L$ , and the end point of the line is  $D_U$ . CHP merges multiple boundaries when they refer to the same value. After the arrangement, CHP derives an integrated partition on  $[D_L, D_U]$ , denoted as

$$\{W_1, W_2, \dots, W_{K_0}\}, \quad (10)$$

where  $W_1 = D_L$  and  $W_{K_0} = D_U$ . At the end of this phase, CHP distributes the partition together with the privacy budget  $\epsilon_0$  to all contributors.

**4.2.1. Local Encoding.** Upon receiving the partition on whole range, each contributor  $u_i$  first encodes her value  $d_i$  into the vector similar with SHP:

$$D_i = (D_{i1}, \dots, D_{iK_0-1}), \quad (11)$$

where the  $D_{ij} = 1$  when

$$W_j \leq d_i \leq W_{j+1} \quad (12)$$

and  $D_{ij} = 0$  otherwise.

With the vector  $D_i$ , CHP also applies the typical perturbation mechanisms, for example, Basic RAPPOR, with the following perturbation probability:

$$f = \frac{2}{e^{\epsilon_0/2} + 1}. \quad (13)$$

Finally, the perturbed vector  $D'_i$  will be sent to the data curator.

**4.2.2. Decoding and Publishing.** In this phase, the data curator will fuse the vectors collected from contributors and estimate the accumulated contents within each interval. Then, the data curator generates and publishes results for consumers, respectively.

In the first step, CHP estimates the counting  $R_k$  for each interval  $[W_k, W_{k+1}]$  in the integrated partition as

$$R_k = \frac{\left\| \left\{ D'_i | D'_{ik} = 1 \right\} \right\| - 1/2 \cdot f \cdot N}{1 - f}, \quad \forall k \leq K_0. \quad (14)$$

In the second step, for each consumer, CHP estimates the counting in each interval by accumulating the corresponding intervals in the integrated partition.

$$R_{ij} = \sum_{h=p}^q R_h, \quad (15)$$

where  $R_{ij}$  indicates the number of numerical values falling in range  $[W_{ij}, W_{ij+1}]$  and  $W_p = W_{ij}$ ,  $W_q = W_{ij+1}$ .

Finally, the data curator distributes the corresponding result set  $R_i$  to each consumer.

**4.2.3. Analysis.** Now, we analyze the performance for CHP. This part first proves that CHP can derive unbiased estimation of histograms for all data consumers. Then, the guarantee on differential privacy is given. Finally, this part shows the efficiency of CHP on bandwidth consumption.

The estimation in CHP includes three major steps: the generation of the integrated partition, the vector encoding and decoding, and the counting of outputs for each consumer. In the first step, CHP guarantees that there will be exactly a continuous set of intervals  $W_i, W_{i+1}, \dots, W_{i+p}$  covering the same range for every  $[W_{jk}, W_{jk+1}]$ . As for each of the interval in the set, the encoding and decoding in CHP will provide an unbiased estimation for the counting of numerical values inside. Finally, CHP estimates the result for  $[W_{jk}, W_{jk+1}]$  by adding up the results for intervals in  $W_i, W_{i+1}, \dots, W_{i+p}$ . This accumulation is a combination of unbiased estimation covering the same range, and thus, the final output is unbiased. The following theorem gives the corresponding conclusion.



**Theorem 7** (unbiased estimation). *In CHP, the data curator provides unbiased histograms for all data consumers.*

Similar with SHP, the variance of the estimated result for CHP is also determined by the adopted perturbation mechanism. The major difference is the composition of multiple intervals during the final step, which will not change the scale of the variance.

Now, we discuss the property of differential privacy for CHP. It is obviously that CHP can provide  $\epsilon_0$ -local differential privacy for each contributor. The analysis is the same with SHP as CHP applies the similar idea for data encoding and perturbation.

Furthermore, CHP allows each contributor to publish only once to respond for all queries. This is different from the baseline solution where SHP has to be applied  $M$  times, due to the heterogeneous partitions on the range. In the later case, it should be noticed that multiple data consumers could be malicious, and they will collude by sharing their results. Then, the actual privacy budget could be larger than  $M \cdot \epsilon_0$ , which is much worse and usually unacceptable for data contributors. Theorem 8 states this property.

**Theorem 8** (local differential privacy). *CHP preserves the numerical content of each contributor with  $\epsilon_0$ -local differential privacy, even if the data consumers are malicious and comprehensively share their results.*

Finally, we discuss the efficiency of CHP. The bandwidth consumption for each contributor is no more than  $O(\sum_{i=1}^M (D_U - D_L)/l_i)$ . Accordingly, the time complexity for each contributor is also  $O(\sum_{i=1}^M (D_U - D_L)/l_i)$ , while the time complexity for the data curator in deriving the results is  $O((\sum_{i=1}^M (D_U - D_L)/l_i)^2)$ .

Actually, CHP also guarantees the minimum number of bits in providing unbiased estimation for all queries. This property indicates CHP achieves optimal efficiency on bandwidth consumption. Theorem 9 shows the property and analysis.

**Theorem 9** (efficiency). *With the unbiased perturbation mechanism, CHP achieves the unbiased estimation for all histograms with minimum number of encoding bits.*

*Proof 1.* We prove the theorem by contradiction. To derive an unbiased estimation for all queries, the boundaries in each of them must also appear in the integrated partition. This is exactly the same with the construction of the integrated partition.

Now, assume that some consecutive intervals can be merged to reduce the total bits, i.e.,  $R_i$  and  $R_j$ , while the unbiased estimation is kept. Then, some boundaries in the integrated partition will be eliminated, i.e., the boundary between  $R_i$  and  $R_j$ . This is contradicted with the requirement where the boundaries for all queries should be retained for

TABLE 1: Statistics for datasets.

	Total contributors	Max salary	Min salary
Baltimore	13,683	250,000	1,800
New York	138,715	297,625	1
San Francisco	291,825	515,102	0

unbiased estimation, as the boundary between  $R_i$  and  $R_j$  is generated according to some queries.

Therefore, no intervals in CHP could be merged, and the minimum number of encoding bits is achieved.

**4.3. Discussion.** Our framework assumes that each participant holds exactly one content. However, it can also fit participants with multicontents. The extension could be achieved by two strategies. In the first category, a participant can encode each of her content into one independent bit vector, and then uploads these vectors to the service provider. In this case, the total bandwidth of uploading is determined by the scales of contents and the bits for encoding. In the second category, a participant can first encode each of her content according to the first strategy. Then, these bit vectors will be accumulated, and each entry of the aggregated vector will record the total number of vector with “1” for the same entry in the vector. In this later case, the total number of bandwidth will be determined by the bits within one vector, which is significantly reduced when compared with the first strategy. We can also prove the results are still unbiased, which can be extended from Theorems 5 and 7.

## 5. Evaluation

This section evaluates the performance of the proposed algorithms. We adopt the salary data collected for normal citizens in the United States [40]. Specifically, we extract the information in New York city, San Francisco, and Baltimore, respectively. The statistics of the three cities are shown in Table 1. In our evaluation, multiple data consumers expect to derive the distribution of incoming levels in different granularities. Therefore, they will post their requests on histogram publication. The data contributors will publish their data to the consumers, and the privacy concerns and the bandwidth consumption should be treated. The data curator acts as the coordinator among the two sides.

As the extension of current studies on numerical values is nontrivial, we compare their performance with one baseline algorithm. In this algorithm, the data contributors respond to each consumer separately. To thwart the collusion among consumers, the baseline algorithm requests the consumers to share the privacy budgets among multiple responses, e.g., assume the total privacy budgets to be  $\epsilon_0$ , then a contributor will apply  $\epsilon_0/K$  budget to each of  $K$  queries. We also compare the performance with the sampling algorithm.

The metric applied for the evaluation is the mean square errors (MSE for short). Furthermore, we run each test group 20 times to alleviate the influence of randomness.



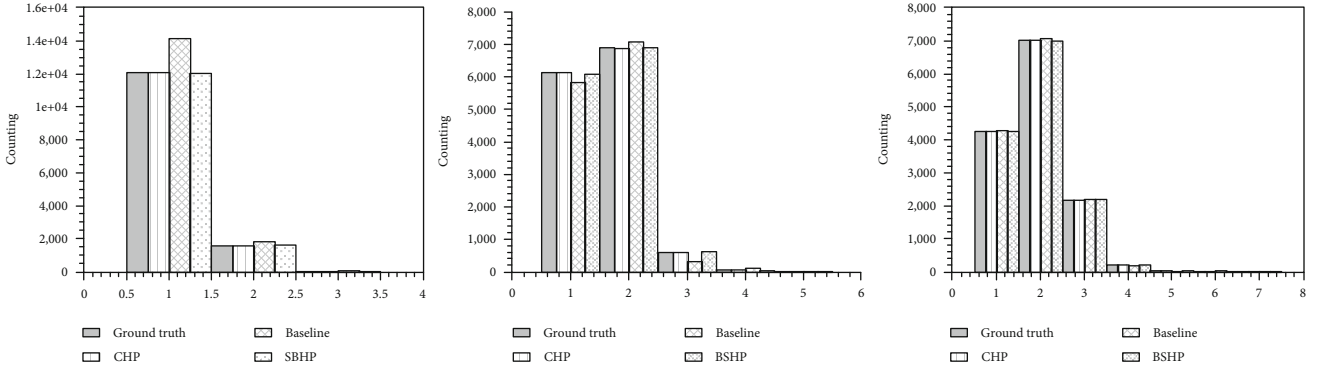


FIGURE 1: Multigranularity histograms for Baltimore.

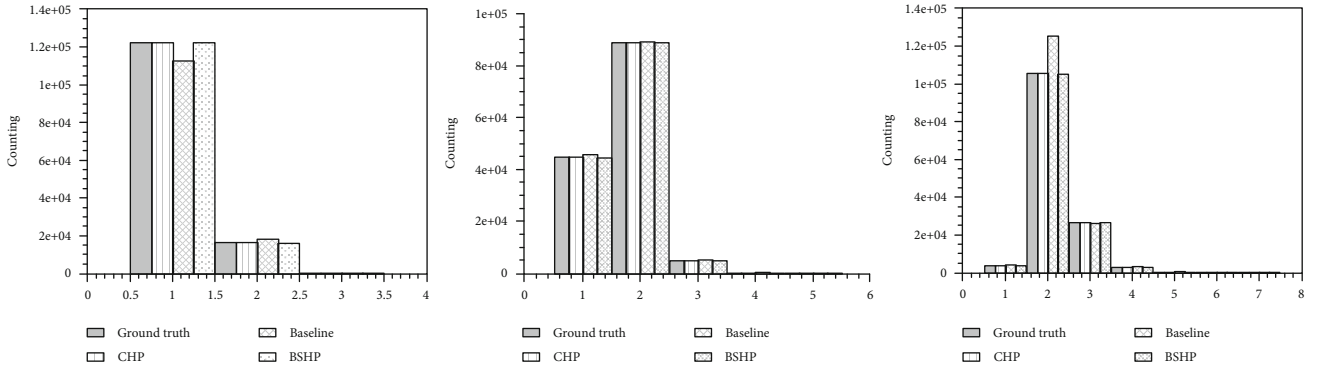


FIGURE 2: Multigranularity histograms for New York city.

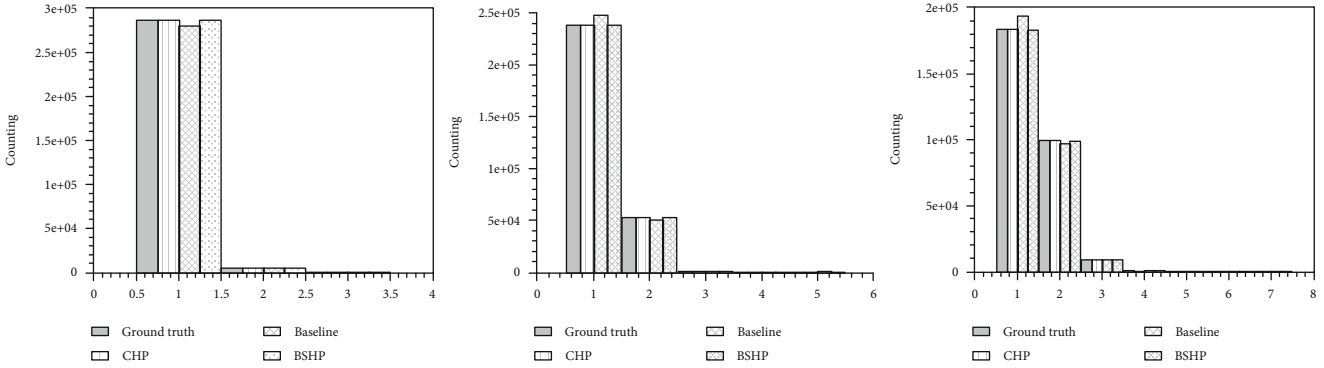


FIGURE 3: Multigranularity histograms for San Francisco.

5.1. *Basic Performance.* This part studies the basic performance for all proposed methods. We are interested in both the derived results and the overall effectiveness of the methods. The parameter settings are as follows: there are three consumers in the system, requesting 3-fold, 5-fold, and 7-fold histograms, respectively. They share the total budgets with  $\epsilon = 15$ , where the baseline algorithm partitions the budgets among all three consumers. Our proposed algorithms, on the other hand, can allocate all budgets in one output.

The results are shown in Figures 1–3. As we see, the proposed algorithms provide better utilities. They outperform the baseline algorithms in all groups and achieve more accurate shapes for histograms. The difference is actually very significant, when considering there are many data values

belonging to some intervals to reduce the influence of randomness.

We also compare the MSE performance of all algorithms with various privacy budgets. In this group, the privacy budgets vary from 3 to 18. According to the results in Figure 4, the proposed algorithms can reduce the MSE for histograms. The improvement is more significant when the privacy budgets is relatively large. We can see that CHP will introduce few errors when  $\epsilon = 18$ , indicating the achievement of high accuracy. The reason is that these algorithms bypass the partition of budgets towards multiple queries, thus reducing the noise in published data.

Finally, the performance for San Francisco is worse than those for NYC and Baltimore. One potential reason is that

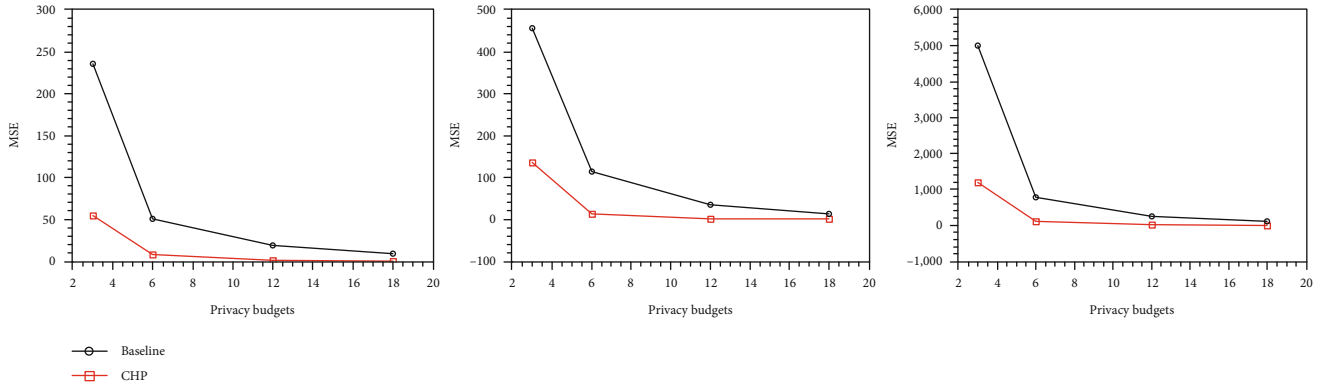


FIGURE 4: Mean square errors for histogram with various privacy budgets.

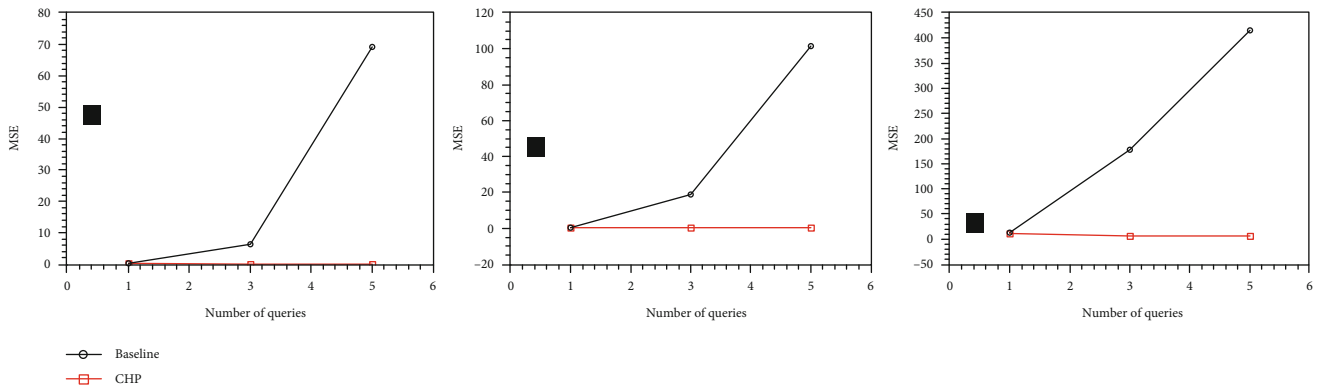


FIGURE 5: Mean square errors with different numbers of queries.

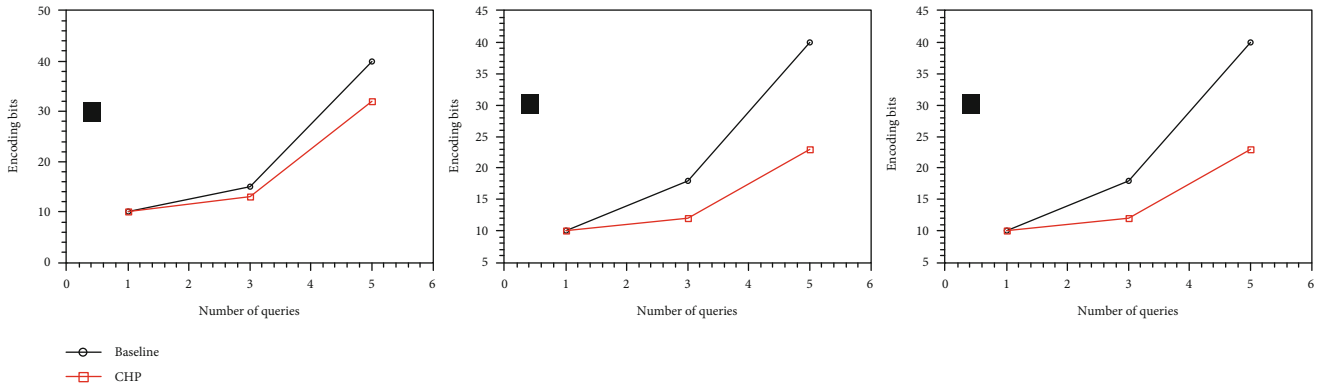


FIGURE 6: Encoding bits with different methods.

some intervals of histograms for San Francisco include few data values. However, the noise in the outputs still exists, which will be aggravated and lead to severe increase on MSE.

**5.2. Heterogeneous Data Consumers.** Within the real histogram publication, data consumers could be diverse on their behaviors. Therefore, the performance should be validated under different circumstances. In this part, three groups of data consumers are considered. The first group includes one single consumer, requesting a 10-fold histogram. The second group includes three data consumers requesting 3-

fold, 5-fold, and 7-fold histograms. The third one has 5 consumers inside, whose requests are 3 folds, 5 folds, 7 folds, 10 folds, and 15 folds. The privacy budget is 15, and the sampling ratio is 0.8. The results are shown in Figure 5.

We observe that CHP and the sampling-based algorithm can maintain a similar performance among different groups, besides their low MSE. This is due to the fact that both algorithms request the data publication to be executed only once for multiple queries. Nevertheless, the baseline algorithm will execute the publication once for each queries. Then, the performance will suffer dramatic falling when the number of

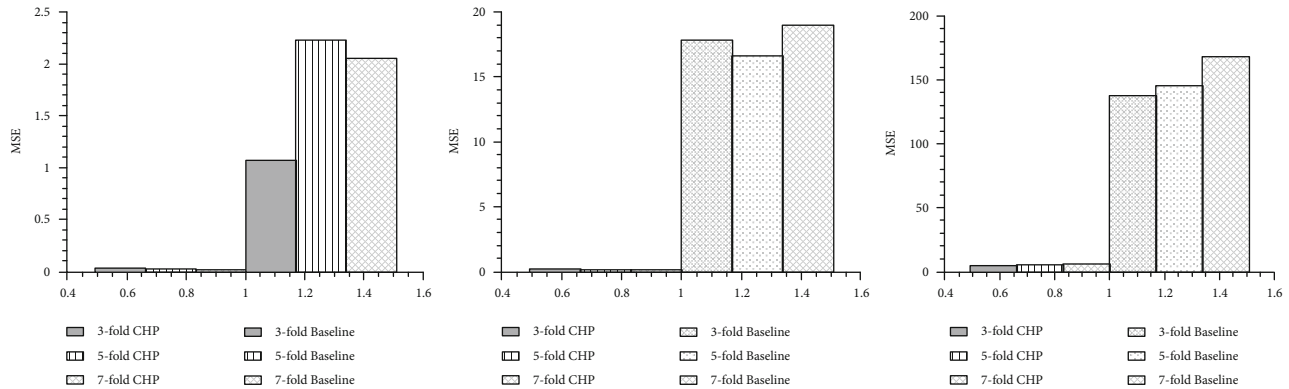


FIGURE 7: Comparison of MSE among different queries.

queries rises. We also observe that CHP reduces the number of total bits for encoding in Figure 6, which is already noticeable with very few queries.

We also compare the performance among different queries. Figure 7 shows the MSEs for 3-fold, 5-fold, and 7-fold histograms. According to the results, both CHP and the baseline algorithm can guarantee relatively similar performance on all queries. This again validates our analysis that the variance is determined by the privacy budgets, which are identical for different queries and their folds.

## 6. Conclusion

Local differential privacy provides novel paradigms for distributed and safety data queries. Various techniques have been designed towards heterogeneous categories of queries. However, the histogram, providing some essential information for the numerical data, has not been thoroughly considered. Existing methods are either incapable or lead to unwillingness resource consumption. As a result, this paper proposes a novel framework towards the differentially private publication of histogram over numerical values. A novel encoding mechanism is designed where the numerical data could be encoded once for multiple queries. It achieves highly efficient bandwidth consumption and can reduce the unnecessary waste on privacy budgets. The accuracy of derived results, the optimization on bandwidth consumption, and the strict privacy preservation are analyzed for all algorithms, and we also discuss the extension for online queries.

## Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This work was supported by the National Key R&D Program of China (No. 2018YFC0807500), by the National Natural Science Foundation of China (Nos. U19A2059 and 61802050), and by the Ministry of Science and Technology of Sichuan Province Program (Nos. 2018GZDZX0048 and 20ZDYF0343).

## References

- [1] X. Wang, L. T. Yang, L. Song, H. Wang, L. Ren, and J. Deen, "A tensor-based multi-attributes visual feature recognition method for industrial intelligence," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 2231–2241, 2020.
- [2] L. Ren, Z. Meng, X. Wang, L. Zhang, and L. T. Yang, "A data-driven approach of product quality prediction for complex production systems," *IEEE Transactions on Industrial Informatics*, no. 99, p. 1, 2020.
- [3] R. Bassily and A. Smith, "Local, private, efficient protocols for succinct histograms," in *Proceedings of the forty-seventh annual ACM symposium on Theory of Computing*, pp. 127–135, New York, NY, USA, June 2015.
- [4] W. Zhu, P. Kairouz, H. Sun, B. McMahan, and W. Li, "Federated heavy hitters discovery with differential privacy," 2019, <http://arxiv.org/abs/1902.08534>.
- [5] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.
- [6] Ú. Erlingsson, V. Pihur, and A. Korolova, "Rappor: randomized aggregatable privacy-preserving ordinal response," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1054–1067, Scottsdale, Arizona, USA, November 2014.
- [7] M. Bun, J. Nelson, and U. Stemmer, "Heavy hitters and the structure of local privacy," in *Proceedings of the 37th ACM SIGMOD-SIGACT-SIGAI Symposium on Principles of Database Systems*, pp. 435–447, Houston, TX, USA, May 2018.
- [8] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Minimax optimal procedures for locally private estimation," *Journal of the American Statistical Association*, vol. 113, no. 521, pp. 182–201, 2018.

- [9] J. Xu, Z. Zhang, X. Xiao, Y. Yang, G. Yu, and M. Winslett, "Differentially private histogram publication," *The VLDB Journal*, vol. 22, no. 6, pp. 797–822, 2013.
- [10] J. Wang, Z. Cai, and J. Yu, "Achieving personalized k-anonymity-based content privacy for autonomous vehicles in cps," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4242–4251, 2020.
- [11] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial iots," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.
- [12] X. Zheng, G. Luo, and Z. Cai, "A fair mechanism for private data publication in online social networks," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 880–891, 2020.
- [13] X. Zheng, Z. Cai, J. Li, and H. Gao, "Locationprivacy-aware review publication mechanism for local business service systems," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, pp. 1–9, Atlanta, GA, USA, 2017.
- [14] Z. Cai, X. Zheng, and J. Yu, "A differential-private framework for urban traffic flows estimation via taxi companies," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6492–6499, 2019.
- [15] T. Wang, J. Blocki, N. Li, and S. Jha, "Locally differentially private protocols for frequency estimation," in *Proc. of the 26th USENIX Security Symposium*, pp. 729–745, Vancouver, BC, Canada, 2017.
- [16] S. Wang, L. Huang, P. Wang, H. Deng, H. Xu, and W. Yang, "Private weighted histogram aggregation in crowdsourcing," in *International Conference on Wireless Algorithms, Systems, and Applications*, pp. 250–261, Springer, 2016.
- [17] Z. Qin, T. Yu, Y. Yang, I. Khalil, X. Xiao, and K. Ren, "Generating synthetic decentralized social graphs with local differential privacy," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 425–438, Dallas, TX, USA, 2017.
- [18] X. Zheng, A. Chen, G. Luo, L. Tian, and Z. Cai, "Privacy-preserved distinct content collection in human-assisted ubiquitous computing systems," *Information Sciences*, vol. 493, pp. 91–104, 2019.
- [19] Z. Cai and Z. He, "Trading private range counting over big iot data," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 144–153, Dallas, TX, USA, 2019.
- [20] Z. Qin, Y. Yang, T. Yu, I. Khalil, X. Xiao, and K. Ren, "Heavy hitter estimation over set-valued data with local differential privacy," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 192–203, Vienna, Austria, 2016.
- [21] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2018.
- [22] L. Ren, Z. Meng, X. Wang, R. Lu, and L. T. Yang, "A wide-deep-sequence model-based quality prediction method in industrial process analysis," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 9, pp. 3721–3731, 2020.
- [23] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Local privacy and statistical minimax rates," in *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, pp. 429–438, NW Washington, DC, USA, 2013.
- [24] N. Wang, X. Xiao, Y. Yang et al., "Collecting and analyzing multidimensional data with local differential privacy," in *2019 IEEE 35th International Conference on Data Engineering (ICDE)*, pp. 638–649, Macao, China, 2019.
- [25] J. Soria-Comas and J. Domingo-Ferrer, "Optimal data-independent noise for differential privacy," *Information Sciences*, vol. 250, pp. 200–214, 2013.
- [26] Q. Geng, P. Kairouz, S. Oh, and P. Viswanath, "The staircase mechanism in differential privacy," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 7, pp. 1176–1184, 2015.
- [27] Q. Ye, H. Hu, X. Meng, and H. Zheng, "Privkv: key-value data collection with local differential privacy," in *PrivKV: Key-Value Data Collection with Local Differential Privacy*, San Francisco, CA, USA, 2019.
- [28] X. Zhang, R. Chen, J. Xu, X. Meng, and Y. Xie, "Towards accurate histogram publication under differential privacy," in *Proceedings of the 2014 SIAM international conference on data mining*, pp. 587–595, Philadelphia, Pennsylvania, USA, 2014.
- [29] M. Hay, V. Rastogi, G. Miklau, and D. Suciu, "Boosting the accuracy of differentially private histograms through consistency," *Proceedings of the VLDB Endowment*, vol. 3, no. 1-2, pp. 1021–1032, 2010.
- [30] G. Acs, C. Castelluccia, and R. Chen, "Differentially private histogram publishing through lossy compression," in *2012 IEEE 12th International Conference on Data Mining*, pp. 1–10, Brussels, Belgium, 2012.
- [31] Y.-H. Kuo, C.-C. Chiu, D. Kifer, M. Hay, and A. Machanavajjhala, "Differentially private hierarchical count-of-counts histograms," *Proceedings of the VLDB Endowment*, vol. 11, no. 11, pp. 1509–1521, 2018.
- [32] Z. He, Z. Cai, and J. Yu, "Latent-data privacy preserving with customized data utility for social network data," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 665–673, 2018.
- [33] X. Wang, L. T. Yang, Y. Wang, L. Ren, and M. J. Deen, "Adtt: a highly-efficient distributed tensor-train decomposition method for iiot big data," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1573–1582, 2020.
- [34] S. Amini, J. Lindqvist, J. Hong, J. Lin, E. Toch, and N. Sadeh, "Caché: caching location-enhanced content to improve user privacy," in *Proceedings of the 9th international conference on Mobile systems, applications, and services - MobiSys '11*, pp. 197–210, Washington, DC, USA, 2011.
- [35] R. Lu, X. Lin, Z. Shi, and J. Shao, "Plam: a privacy-preserving framework for local-area mobile social networks," in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, pp. 763–771, Toronto, ON, Canada, April 2014.
- [36] N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Optimal geo-indistinguishable mechanisms for location privacy," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 251–262, Scottsdale, Arizona, USA, November 2014.
- [37] B. Palanisamy and L. Liu, "Mobimix: protecting location privacy with mix-zones over road networks," in *2011 IEEE 27th International Conference on Data Engineering*, pp. 494–505, Hannover, Germany, April 2011.
- [38] N. Li, W. Qardaji, and D. Su, "On sampling, anonymization, and differential privacy or, kanonymization meets differential

privacy,” in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security - ASIACCS '12*, pp. 32-33, Seoul, Korea, 2012.

- [39] F. McSherry and I. Mironov, “Differentially private recommender systems: building privacy into the net,” in *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining - KDD '09*, pp. 627–636, New York, NY, USA, 2009.
- [40] “Data.world,” <https://data.world/datasets/salary>.



## Research Article

# A Transaction Trade-Off Utility Function Approach for Predicting the End-Price of Online Auctions in IoT

Xiaohui Li <sup>1,2</sup> and Hongbin Dong <sup>1</sup>

<sup>1</sup>College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China

<sup>2</sup>Harbin Vocational & Technical College, Harbin 150081, China

Correspondence should be addressed to Hongbin Dong; [donghongbin@hrbeu.edu.cn](mailto:donghongbin@hrbeu.edu.cn)

Received 9 November 2020; Revised 11 December 2020; Accepted 23 January 2021; Published 3 February 2021

Academic Editor: Yaguang Lin

Copyright © 2021 Xiaohui Li and Hongbin Dong. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

To stimulate large-scale users to participate in the big data construction of IoT (internet of things), auction mechanisms based on game theory are used to select participants and calculate the corresponding reward in the process of crowdsensing data collection from IoT. In online auctions, bidders bid many times and increase their bid price. All the bidders want to maximize their utility in auctions. An effective incentive mechanism can maximize social welfare in online auctions. It is complicated for auction platforms to calculate social welfare and the utility of each bidder's bidding items in online auctions. In this paper, a transaction trade-off utility incentive mechanism is introduced. Based on the transaction trade-off utility incentive mechanism, it can make the forecasting process consistent with bidding behaviors. Furthermore, an end-price dynamic forecasting agent is proposed for predicting end prices of online auctions. The agent develops a novel trade-off methodology for classifying online auctions by using the transaction trade-off utility function to measure the distance of auction items in KNN. Then, it predicts the end prices of online auctions by regression. The experimental results demonstrate that an online auction process considering the transaction utility is more consistent with the behaviors of bidders, and the proposed prediction algorithm can obtain higher prediction accuracy.

## 1. Introduction

With the rapid development of IoT and e-commerce, the traditional model of commodity trading and resource allocation has changed. Online market platforms like eBay, Yahoo, and Amazon have attracted more and more trading users. eBay is the leading auction market platform, and it adopts the English auction format. There are more than 100 million members and 20 million items for sale at any given time. Auction is an important mechanism of economic exchange [1]. Online auction is an online marketing model on the internet, which has turned out to be an effective way to allocate goods and resources [2–4]. It has become an important form of e-commerce. Online auctions have attracted more and more scholars' attention and research. Online auctions will produce a large amount of electronic transaction data in a transaction process, which contains enough economic

behavior information and product information. A lot of researchers studied the distributed data collection and privacy problems [5–7]. It is beneficial for all buyers, sellers, and marketplace managers to make full use of these transaction data for predicting the end prices of online auctions using machine learning algorithms, data mining technology, and time series analysis [8–10].

Many firms can be offered a great benefit by efficient strategies in social networks [11]. An auction problem can be regarded as a resource allocation problem [12–14]. To allocate resources reasonably, the utility should be considered. Considering transaction utility is more suitable for bidding behaviors in auctions. As the utility of items is different for everyone in online auctions, not all items can be sold at a uniform price. We restrict items to bidders with very simple utility functions which we call “transaction trade-off utility function” in this paper.

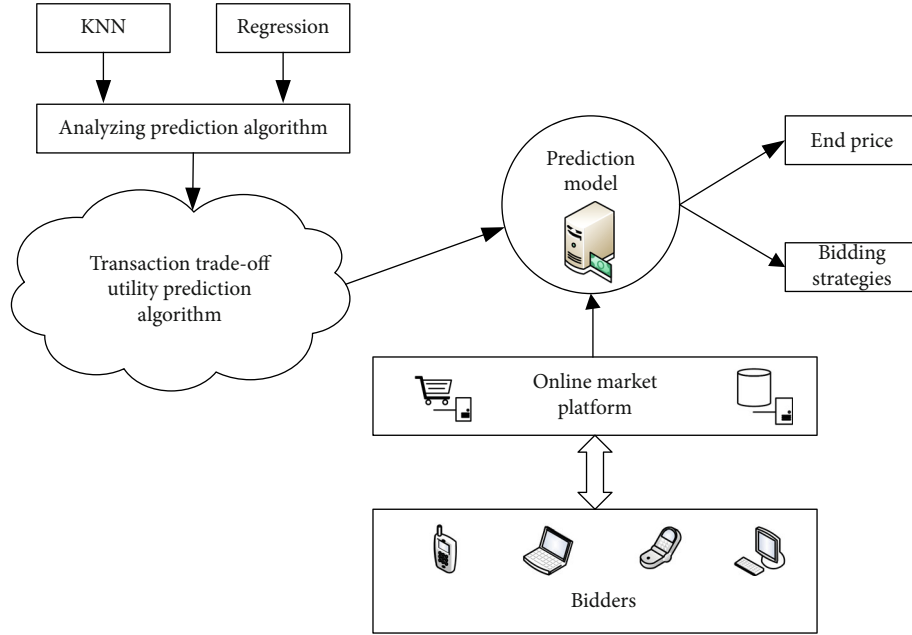


FIGURE 1: The architecture of an online auction system.

Transaction utility is considered as possibly the determinant that affects bidding behaviors [15]. In systems, the social welfare should be maximized through the design of incentive mechanism [16]. But many online auction formats including English auction, Dutch auction, first-price sealed-bid, and second-price sealed-bid do not consider and calculate bidders' utility. Without considering bidders' utility and bidding motivation, the prediction algorithm with a good effect on a homogeneous dataset may not work well on heterogeneous datasets.

According to the above discussions, we research a transaction trade-off utility incentive mechanism and give the lemmas and proofs about item allocation problems in online auctions. In our model, the online auction framework of considering transaction utility is shown in Figure 1.

Agent technology is playing an increasingly important role in online auction platforms. An end-price dynamic forecasting agent (EDFA) is proposed, which can use the transaction trade-off utility incentive mechanism to predict whether an auction will be successful and how much end prices are in online auctions. Machine learning algorithms, which combine transaction trade-off utility, are used to predict final auction prices. EDFA predicts the end prices of online auctions in two phases: phase 1 for classifying online auctions by using the transaction trade-off utility function in KNN and phase 2 for predicting end prices of online auctions by regression. The results illustrate that the proposed algorithm considering utility not only improves the accuracy of a homogeneous dataset but also improves the accuracy of a heterogeneous dataset. As predicting whether an auction item will be sold, the proposed algorithm gave about 98% accuracy.

According to the bidding behaviors and price prediction problems in online auctions, the specific contributions of this work are shown as follows.

- (1) To better understand the allocation process of auction items and transaction utility, we present a transaction trade-off utility incentive mechanism and the related lemmas and proofs. The proposed transaction trade-off utility incentive mechanism can maximize the utility of auction platforms and bidders
- (2) Considering the transaction utility and bidding motivation, a transaction trade-off utility incentive mechanism is proposed. To improve the accuracy of classification and prediction, the transaction trade-off utility function is proposed by combining KNN and regression named as the transaction trade-off utility prediction (TTUP) algorithm. The transaction trade-off utility function includes three aspects of GSP auctions, which are a reserve price, a click-through rate, and the number of item impressions. The function is used to classify in KNN, and end prices of online auctions are predicted by regression
- (3) We conduct comparison experiments on homogeneous and heterogeneous auction dataset to verify the effectiveness and accuracy based on the proposed transaction trade-off utility incentive mechanism and the TTUP algorithm. All results show that the proposed mechanism and algorithm are significantly better than other system algorithms both in terms of bidding behaviors and prediction accuracy

The rest of the paper is organized as follows. The related works are introduced in Section 2. In Section 3, we present the transaction trade-off utility incentive mechanism, including the proposed end-price dynamic forecasting agent, the system model, and the proposed algorithm TTUP. Experiments and results are explained in Section 4. We conclude the paper and provide our further research in Section 5.

TABLE 1: The descriptions for notations in our incentive mechanism and algorithm.

Notation	Description
$p$	The reservation price of an online auction
$n$	The impressions of auction items
$c$	The click-through rate of auction items
$U$	The bidder transaction trade-off utility as a function of relevant variables

## 2. Related Works

Bidders in online auctions face difficulties when looking for the best bidding strategies to win their interesting items. Many kinds of research focus on the design of bidding strategies. Kaur et al. [17] proposed a comprehensive methodology and designed bidding strategies with regression analysis and negotiation decision functions. Carbonneau and Vahidov [18] proposed an approach to facilitate multiattribute bidding in single-attribute auctions. Sayman and Akcay [19] indicated transaction utility can explain some bidding patterns on eBay. They showed that both underbidding and multiple bidding behaviors can be consistent with utility maximization if the buyer's utility incorporates a transaction utility component. Wang et al. [20–22] proposed a truthful incentive mechanism and improved the two-stage auction algorithm in mobile crowdsourcing. Efficient incentive mechanisms and auction algorithms can improve the efficiency and utility of the systems.

In the data mining and machine learning field, there are a lot of researches on predicting price. Many researchers used data mining techniques to predict price. The history auction data can be exploited for predicting the end-price of an auction by using support vector machines,  $k$ -nearest neighbor, clustering, regression, and multiple binary classifications [23–27]. Many different approaches have been proposed for predicting the end price of online auctions. Li et al. [28] used machine learning algorithms and traditional statistical methods to forecast the final prices of auction items. Ghani [29] predicted the end prices of online auctions using classification and regression trees, multiclass classification, and multiple binary classification methods. Heijst et al. [8] created a support system for predicting end prices on eBay using the CART regression tree. Khadge and Kulkarni [30] proposed a system using Naïve Bayes for classification and kernel mapping SVM for predicting whether an item maximizes profit or not. Moreover, if the model predicts the price of Nike shoes, a regression-type model will put equal weight on the shoe dataset, which may be inappropriate if the goal is to predict an auction price for a Sony laptop. While some of the brands and product differences can be controlled using appropriate predictor variables, there might still be intrinsic differences that are hard to measure. But we can measure the utility in different item transactions. As for the researches on using machine learning techniques and utility theory to predict the end price of the online auctions, fewer can be found.

The utility function is researched and adopted in some studies. Using utility function, which measures social welfare or satisfaction of a consumer as a function of consumption, can model different consumption behaviors [15]. In [31], the impact of time-based demand response programs on calculating incentive payments had been investigated considering the customer's utility function. In [32], the utility function was used to identify different customers' behavior and determine appropriate incentive payments to convince different customers to participate in the demand response program.

Logistic regression, Bayesian linear regression, decision trees, and deep recurrent neural network can be regarded as parametric models. Optimal parameters are usually different in different datasets, so the same group of parameters does not apply to predicting different item end-price of online auctions. The KNN method is a nonparametric model without strict assumption. However, there are many restrictions in the parametric models. To overcome these limitations of some parametric models, the proposed TTUP approach has better adaptability and robustness.

In generalized second-price (GSP) auctions, a reserve price is an important factor for a pricing model. The impact of a reserve price on GSP auctions was studied by Edelman and Schwarz [33]. In [33], the relationship between reserve prices and revenues was shown. Sellers want to have a relatively higher click-through rate (CTR) and a large number of impressions [34], which can increase their revenues. Thus, a reserve price, CTR, and the number of impressions were added to the proposed transaction trade-off utility function, and the function also follows this relationship in [33, 34].

Each bidder behaves independently based on his preferences. Few studies consider transaction utility in price forecasting. In this paper, we focus on identifying the bidding behavior of different bidders and predicting end prices considering the transaction trade-off utility function. We propose a novel trade-off utility approach for predicting online auction end prices based on the transaction trade-off utility incentive mechanism.

## 3. The Proposed Transaction Trade-Off Utility Incentive Mechanism

In this section, we mainly research the proposed transaction trade-off utility incentive mechanism, which includes the EDFA and the TTUP algorithm. We describe some attributes from the vast feature space of online auctions in Table 1.

*3.1. The Proposed End-Price Dynamic Forecasting Agent.* The EDFA is shown in Figure 2. The agent can use auction information to rank bidders and predict end prices of online auctions. Formally, our novel trade-off utility approach consists of four steps. Firstly, the bid server extracts auction history data and input it. Secondly, the utility-estimator and KNN-estimator agent determines the best number  $k$  of partitions for input data and then clusters the utility similar auctions together in  $k$  groups. Thirdly, price-predictor forecasts end prices and designs bidding strategies by regression. Finally, the model is evaluated and deployed. Then, the optimized end prices and bidding strategies are output to the bid server.

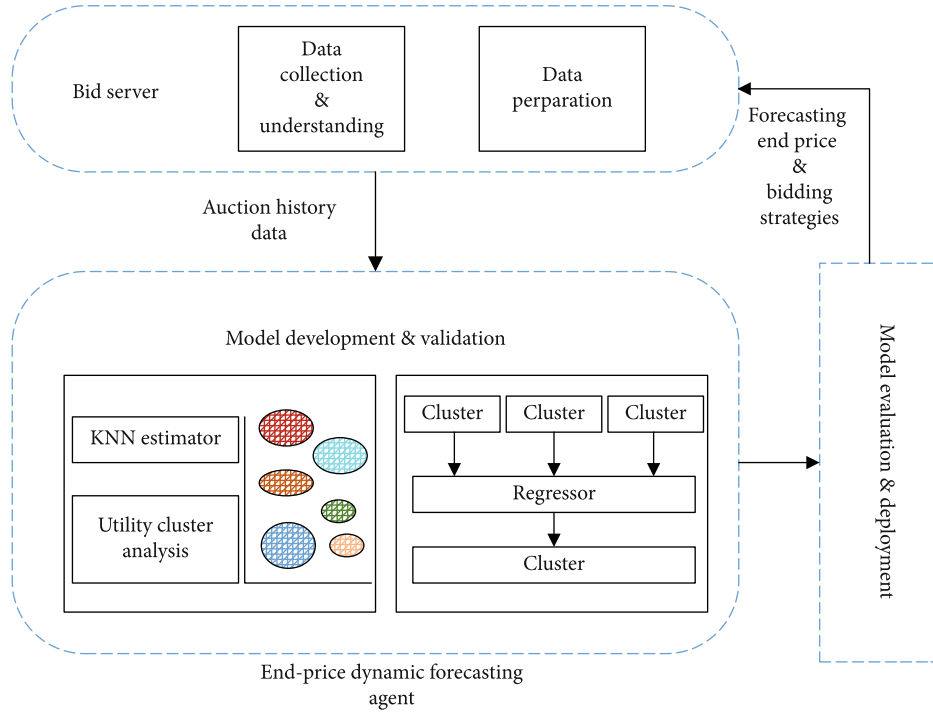


FIGURE 2: End-price dynamic forecasting agent.

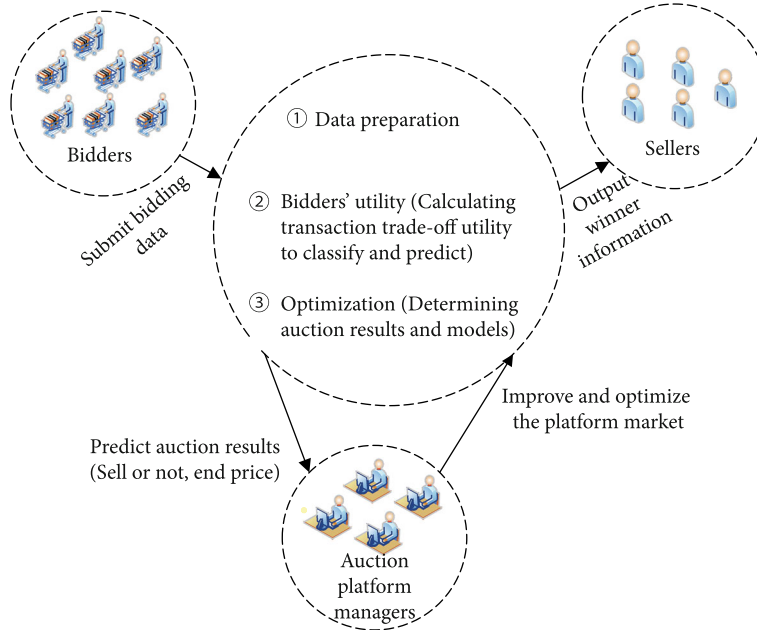


FIGURE 3: The process of the proposed incentive mechanism.

3.2. *System Model.* The utility is a form of measuring consumer satisfaction from commodity consumption and service. The utility function could accurately measure a consumer’s preferences. As part of the process, factors such as customer satisfaction, total bid counts, and the rate of consumption by customers are considered key to accurately assessing the utility of the product. Unlike other forms of measuring the success of a given product, the utility function does not

concern itself with the amount of return generated for the entity that manufactures and sells the product.

The transaction trade-off utility function is derived from a novel LP-based approach. It can be written as

$$\psi(x) = 1 - \exp(x - 1). \tag{1}$$

<p><b>Inputs:</b> auction training dataset <math>X</math>, testing dataset <math>Y</math>, the total number of clusters <math>K</math></p> <p><b>Outputs:</b> classifying accuracy, KNeighborsRegressor model</p> <p><b>Training Stage:</b></p> <ol style="list-style-type: none"> <li>(1) For <math>i = 1; i++; i &lt; = n</math></li> <li>(2) {</li> <li>(3) transaction trade-off utility distance between any two auction items can be calculated by Equation (3)</li> <li>(4) classifying the training dataset into <math>K</math> clusters</li> <li>(5) For <math>k = 1; k++; k &lt; = K</math></li> <li>(6) {</li> <li>(7) get transaction trade-off utility of each cluster</li> <li>(8) get regression prediction price model for each cluster</li> <li>(9) }</li> <li>(10) }</li> </ol> <p><b>Test Stage:</b></p> <ol style="list-style-type: none"> <li>(11) For <math>k = 1; k++; k &lt; = K</math></li> <li>(12) {</li> <li>(13) If (the transaction trade-off utility distance between test data <math>i</math> and cluster <math>k</math>)</li> <li>(14) test data <math>i</math> belongs to cluster <math>k</math></li> <li>(15) Apply KNeighborsRegressor() to classify and forecast</li> <li>(16) Obtain the classification accuracy</li> <li>(17) Obtain RMSE</li> <li>(18) }</li> </ol>
---

ALGORITHM 1: The proposed TTUP algorithm

Next, the  $U$  value of each auction item will be calculated by Equation (2). We call  $U$  as auction transaction trade-off utility. Let  $U$  be the following function:

$$U_i = c(i) \times \psi(f(i)), \quad (2)$$

where  $c(i)$  is the CTR of auction item  $i$ ;  $f(i)$  is the fraction of a reserve price and auction item  $i$ 's impression number, that is,  $f(i) = p(i)/n(i)$ , where  $p(i)$  is a reserve price of an online auction for item  $i$  and  $n(i)$  is the number of auction item  $i$ 's impressions.

Transaction trade-off utility distance is proposed to metric auction items. Suppose that auction item  $i$  has  $n$  feature variables  $(x_1, x_2, \dots, x_n)$ , and the transaction trade-off utility of auction item  $i$  is  $U_i$  calculated by Equation (2). Similarly, auction item  $j$  also has  $n$  feature variables  $(y_1, y_2, \dots, y_n)$ , and the transaction trade-off utility of auction item  $j$  is  $U_j$  calculated by Equation (2). The transaction trade-off utility distance of item  $i$  and item  $j$  can be calculated as

$$D_{ij} = \sqrt{(U_i - U_j)^2 \sum_{i=1}^n (x_i - y_i)^2}. \quad (3)$$

The process of the proposed incentive mechanism is shown in Figure 3. The core parts of the mechanism include data preparation, calculating transaction trade-off utility to classifying and predicting, and optimization.

**3.3. The Proposed Transaction Trade-Off Utility Prediction Algorithm.** In this section, we use the transaction trade-off utility distance metric to find  $k$ -nearest neighbors from auction items. An algorithm based on KNN can achieve a high

TABLE 2: Data file description.

Data file name	File description	Data rows
TraingSet	All auctions in April 2013	258588
TestSet	All auctions in the first week of May 2013	37460
TrainingSubset	All auctions successfully traded in April 2013	79732
TestSubset	All auctions successfully traded in the first week of May 2013	9392

level of accuracy in time series [35]. In [36], the utility had been modelled to determine the price.

Firstly, the transaction trade-off utility distance of the feature variables between the auction item  $i$  and another auction item  $j$  in the training dataset is calculated by Equation (3).

Secondly, all the auction items in the training set are sorted in ascending order according to the distance from item  $j$ .

Thirdly,  $K$  data points with the smallest distance from item  $i$  are select.

Finally,  $K$  data points will be considered as the category of item  $i$ .

The proposed TTUP algorithm is described in Algorithm 1.

**3.4. Properties of Proposed Transaction Trade-Off Utility Incentive Mechanism.** With the emergence of new market and resource allocation models on the internet, there is a need for a new artificial intelligence algorithmic theory of combining utility theory and machine learning algorithms. We call bidders with very simple utility functions "single-



mindful bidders” [37]. The proposed algorithm can help understand online auction repercussions to bid price, auction strategies, bidding behaviors, and social welfare caused by auction mechanisms or transaction utility.

Considering that an online auction website is composed of a set  $N = \{1, 2, \dots, n\}$  of items and a set  $M = \{1, 2, \dots, m\}$  of bidders. For each bidder  $i$ , if he bids for item  $j$ , he will get the utility  $U_{ij}$  and pay  $P_{ij}$  for bidding item  $j$ . In the online auction platform, the objective function of each bidder is shown as follows:

$$\begin{aligned} \max \quad & \sum_{i=1}^m \sum_{j \in N} U_{ij}, \\ \text{s.t.} \quad & \sum_{j \in N} P_{ij} \leq B_i \cdot \forall i \in M, \end{aligned} \quad (4)$$

where  $B_i$  is the possessed budget by bidder  $i$ .

We assume that the customers, who bid for the same quantity of items, have the same utility and the same bidding price. In online auctions, there are different reserved prices, different bidding strategies, and different budgets. A uniform price on all items is not feasible, so each bidder will not necessarily get items that she is interested in. We will find that not all items can be sold at a uniform bidding price.

In the book of algorithmic game theory [37], the combinatorial auction problem statement is introduced by *Blumrosen and Nisan*. As they introduced the transaction utility, we have the following definitions by the proposed transaction utility.

*Definition 1.* A utility  $u$  is a real-utility function that for each subset  $S$  of items,  $u(S)$  is the total utility that bidder  $i$  obtains if he receives this bundle of bidding items.

*Definition 2.* An allocation of the bidding items among the bidders is  $S_1, \dots, S_n$ , where  $S_i \cap S_j = \emptyset$  for every  $i \neq j$ . The total utility obtained by an allocation is  $\sum_i u_i(S_i)$ . A socially efficient allocation (among bidders with utility valuations  $u_1, \dots, u_n$ ) is an allocation with maximum social welfare and utility among all allocations.

*Definition 3.* The allocation problem among single-minded bidders is the following:

Input:  $(S_i^*, u_i^*)$  for each bidder  $i = 1, \dots, n$ , where  $S_i^*$  is a bundle of bidding items and  $u_i^*$  is a utility valuation.

Output: a subset of winning bids  $W \subseteq \{1, \dots, n\}$  such that for every  $i \neq j \in W$ ,  $S_i^* \cap S_j^* = \emptyset$  with maximum social welfare  $\sum_{i \in W} u_i^*$ .

**Lemma 4.** *The proposed transaction trade-off utility incentive mechanism is computationally efficient.*

*Proof.* In the proposed transaction trade-off utility incentive mechanism, KNN and regression algorithms are applied to bidder grouping and price forecasting. When the number of samples is  $n$ , the time complexity is  $O(n)$  in the KNN algorithm. Besides, when samples are divided into  $k$  clusters,

TABLE 3: The main features and descriptions of dataset 1.

Feature name	Feature description
Price	End prices of auctions
StartingBid	Minimum transaction price of an auction
BidCount	Number of bids won in an auction
Title	Transaction title
QuantitySold	Successful sale number (0 or 1)
SellerRating	Seller’s rating on eBay
StartDate	Auction start date
EndDate	Auction end date
PositiveFeedbackPercent	Percentage of positive feedback received by seller (for all feedback)
BuyitNowPrice	Price for immediate purchase
HighBidderFeedbackRating	eBay rating of the highest-price bidder
IsHOF	The seller is or not a hall of fame player (0 or 1)
AvgPrice	Average price of a good in inventory
MedianPrice	Median price of a good in inventory
AuctionCount	Total number of auctions in inventory
SellerSaleToAveragePriceRatio	Proportion of auction goods price to average price
StartDayOfWeek	The beginning day of the auction in a week
EndDayOfWeek	The end day of the auction in a week
AuctionDuration	Auction duration days
StartingBidPercent	The ratio of the starting bidding price to the average transaction price
SellerClosePercent	The proportion of a seller’s successful auctions to all online auctions
ItemAuctionSellPercent	Percentage of successful auctions in all online auctions

the prediction price time complexity is  $O(n * k)$  in the TTUP algorithm. The proposed transaction trade-off utility incentive mechanism is computationally efficient because the bidding items and bidders can be selected in polynomial time.

**Lemma 5.** *The proposed transaction trade-off utility incentive mechanism is truthful.*

*Proof.* When classifying the bidders into  $K$  clusters by transaction trade-off utility distance, the TTUP algorithm considers reservation price, the total bid counts of an auction item, and the creditability of a bidder. In online auctions, each bidder wants to maximize total utility, which indicates that bidders should tell their truthfulness. Therefore, the

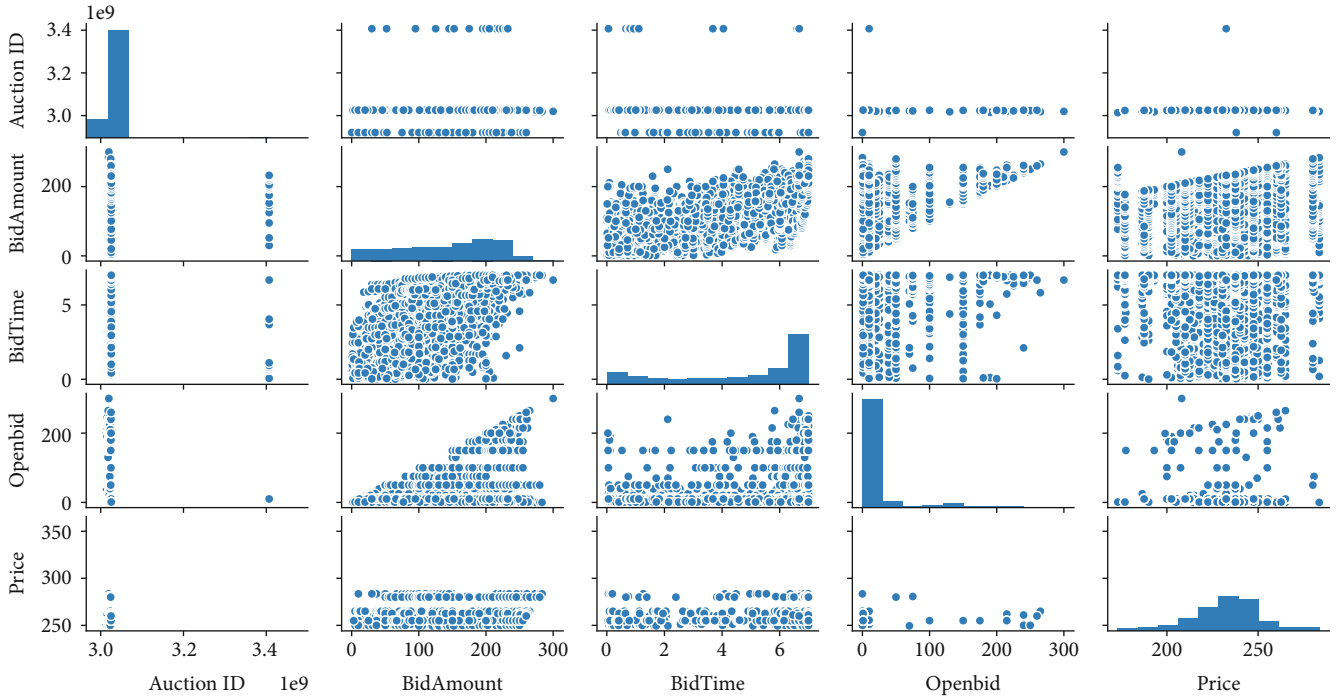


FIGURE 4: The illustration of impact from bid characteristics.

proposed transaction trade-off utility incentive mechanism is truthful.

**Lemma 6.** *The proposed transaction trade-off utility incentive mechanism can maximize social welfare.*

*Proof.* In the proposed transaction trade-off utility incentive mechanism, social welfare can be shown by  $\sum_{i \in W} u_i^*$ , where  $W \subseteq \{1, \dots, n\}$  is a subset of winning bids. Therefore, social welfare can be maximized based on the utility of bidders. It indicates that the proposed transaction trade-off utility incentive mechanism can maximize the social welfare of online auction platforms.

## 4. Experiment and Result Analysis

### 4.1. Evaluation Metrics

**4.1.1. Discrete Prediction.** When we predict an auction item will sell or not, it is a classification problem. We can use an accuracy metric to judge the performance of our algorithm. Accuracy metric is defined as follows:

$$\text{accuracy} = \frac{\text{TC}}{\text{TN}} \times 100\%, \quad (5)$$

where TC is the number of correct prediction samples and TN is the total number of prediction samples.

**4.1.2. Continuous Prediction.** When we predict the end prices of online auctions, it is a continuous problem. We can use the root mean square error (RMSE) to evaluate the prediction performance. RMSE is a widely used numerical prediction evaluation index. It measures the average deviation degree

TABLE 4: Trade-off utility values with different parameters.

Item	$c(i)$	$p(i)$	$n(i)$	$\frac{U_i = c(i) \times \psi(f(i))}{f(i) = p(i)/n(i)}$
A	0.1	0.1	100	0.06318
B	0.1	0.3	100	0.06310
C	0.1	0.5	100	0.06303
D	0.1	0.8	100	0.06292
E	0.1	1	100	0.06284
F	0.3	0.1	100	0.18953
G	0.3	0.3	100	0.18930
H	0.5	0.1	500	0.31602
I	1	0.1	500	0.63205

between the predicted values and the actual values. The smaller the value of RMSE is, the better it is. RMSE is defined as follows:

$$\text{RMSE} = \sqrt{\text{MSE}} = \sqrt{\frac{1}{n} \sum_{i=1}^n E_i^2} = \sqrt{\frac{1}{n} \sum_{i=1}^n (y_i - \hat{y}_i)^2}, \quad (6)$$

where  $y_i$  is the actual value of sample  $i$ ,  $\hat{y}_i$  is the estimate of sample  $i$ , and  $n$  is the total number of samples.

**4.2. Data.** In this section, we use two datasets with eBay auctions. Dataset 1 is downloaded from <https://cims.nyu.edu/~munoz/data/>. The dataset contains four data files that are described in Table 2. Dataset 2 is a real-world dataset on Canon that we used a special collection program to collect from eBay. The dataset contains 4889 auction data rows.

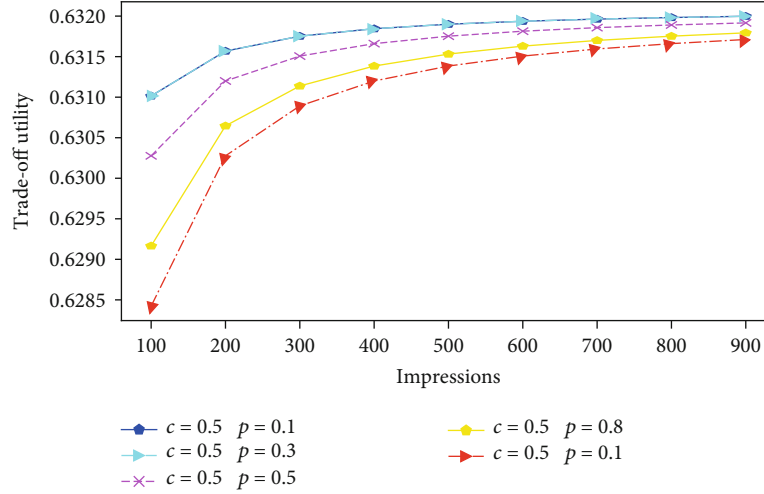


FIGURE 5: The trade-off utility as a function of impressions.

TABLE 5: Model performance.

	Dataset 1		Dataset 2	
	Accuracy	RMSE	Accuracy	RMSE
TTUP	98.45%	4.56	97.52%	5.21
KNN	86.53%	5.11	88.56%	7.96
Linear regression	82.67%	5.56	87.67%	8.79
CART (regression tree)	94.72%	4.88	95.33%	6.16
SVM	95.74%	4.97	94.28%	6.20

We use 70% of the dataset as the training data and 30% of the dataset as the test set.

The main feature names and descriptions of dataset 1 are shown in Table 3. Independent variable analysis is the main diagnostic process used to obtain reliable prediction results. Because there are many bid characteristics of online auction data, it is essential to analyze the relationship and distribution of the independent variables before modelling. Some main characteristics, which are related to auction price, could be found by bid characteristic analysis. Figure 4 is a scatter matrix of auction characteristics in dataset 2, which illustrates the impact of bid characteristics. The diagonal is the histogram of characteristic variables. Through the histogram, we can see that the price histogram illustrates that price obeys normal distribution.

**4.3. Numerical Simulation and Analysis.** Table 4 shows the calculated trade-off utility values with different online auction parameters. This has a bigger trade-off utility value in the relatively higher range of CTR.

Figure 5 represents the trade-off utilities as a function of impressions. With these online auction parameters, the lower the reserve prices are, the more the trade-off utilities are at the same CTR, and the number of impressions. As the reserve prices increase, the trade-off utilities fall. However, if the number of impressions exceeds certain values, the reduction will be less sharp. When the number of impressions reaches a certain number, the utilities tend to converge.

Table 5 shows accuracy and RMSE in the existing system and proposed system. The results demonstrate that the end-price dynamic forecasting agent who adopts the transaction trade-off utility approach outperforms agents following other methodologies. The proposed system using the TTUP algorithm gives 98.45% and 97.52% accuracy. The proposed system performs best compared with other algorithms. It also can be found that transaction trade-off utility is a potential driver of bidders' behaviors in bidding. Transaction trade-off utility is also an important factor for predicting end prices in online auctions.

## 5. Conclusions

In this paper, we present a transaction trade-off utility incentive mechanism and the related lemmas and proofs. The proposed EDFA is based on the incentive mechanism and system model. The contribution of this study is twofold: it is the first study that proposes the transaction trade-off utility incentive mechanism and transaction trade-off utility function, and it is the first study that uses transaction utility in the prediction of online auction end prices. Considering the transaction utility, our system is good for bidders, sellers, and the platform markets. Furthermore, social welfare is also maximized. We tested our price prediction model in a series of experiments. For both homogeneous and heterogeneous datasets, our model gives better accuracy. This proposed transaction trade-off utility incentive mechanism can be used in other auction prediction systems. Building the EDFA is then started automatically.

In further work, we plan to use our transaction utility incentive mechanism in reinforcement learning and transfer learning. Besides, we will combine offline with online data to predict the end prices of online auctions.

## Data Availability

Dataset 1 in this study can be downloaded from <https://cims.nyu.edu/~munoz/data/>. Dataset 2 is available upon request from the first author.

## Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

## Acknowledgments

We acknowledge the support from the National Science Foundation of China (No. 61472095). This work is partially supported by the Natural Science Foundation of Heilongjiang Province under Grant No. LH2020F023, and by the Educational Science Planning of Heilongjiang Province under Grant No. ZJB1421113 and No. GJB1421252.

## References

- [1] K. Hasker and R. Sickles, "eBay in the economic literature: analysis of an auction marketplace," *Review of Industrial Organization*, vol. 37, no. 1, pp. 3–42, 2010.
- [2] Y. Wang, Y. Gao, Y. Li, and X. Tong, "A worker-selection incentive mechanism for optimizing platform-centric mobile crowdsourcing systems," *Computer Networks*, vol. 171, article 107144, 2020.
- [3] E. Haruvy and P. T. L. P. Leszczyc, "Internet auctions," *Foundations and Trends(R) in Marketing*, vol. 4, no. 4, pp. 1–75, 2010.
- [4] Z. Cai, S. Ji, J. He, L. Wei, and A. G. Bourgeois, "Distributed and asynchronous data collection in cognitive radio networks with fairness consideration," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 8, pp. 2020–2029, 2014.
- [5] V. Nikolaidou and P. A. Mitkas, "A sequence mining method to predict the bidding strategy of trading agents," in *Agents and Data Mining Interaction. ADMI 2009. Lecture Notes in Computer Science*, vol. 5680, pp. 139–151, Springer, Berlin, Heidelberg, 2009.
- [6] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.
- [7] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2018.
- [8] D. V. Heijst, R. Potharst, and M. V. Wezel, "A support system for predicting eBay end prices," *Decision Support System*, vol. 44, pp. 970–982, 2008.
- [9] M. Bin and M. Kamel, "Intelligent system for price premium prediction in online auctions," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 3, pp. 329–334, 2020.
- [10] S. Zhang, W. Jank, and G. Shmueli, "Real-time forecasting of online auctions via functional K-nearest neighbors," *SSRN Electronic Journal*, vol. 26, pp. 666–683, 2010.
- [11] Z. He, Z. Cai, J. Yu, X. Wang, Y. Sun, and Y. Li, "Cost-efficient strategies for restraining rumor spreading in mobile social networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2789–2800, 2017.
- [12] A. L. Jin, W. Song, and W. Zhuang, "Auction-based resource allocation for sharing cloudlets in mobile cloud computing," *IEEE Transactions on Emerging Topics in Computing*, vol. 6, no. 1, pp. 45–57, 2018.
- [13] W. Shi, L. Zhang, C. Wu, Z. Li, and F. C. M. Lau, "An online auction framework for dynamic resource provisioning in cloud computing," *IEEE/ACM Transactions on Networking*, vol. 24, no. 4, pp. 2060–2073, 2016.
- [14] Y. Wang, Z. Cai, Z.-H. Zhan, B. Zhao, X. Tong, and L. Qi, "Walrasian equilibrium-based multiobjective optimization for task allocation in mobile crowdsourcing," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 4, pp. 1033–1046, 2020.
- [15] C. Millan, "Theory of utility and consumer behaviour: a comprehensive review of concepts, properties and the most significant theorems," in *Utility and Production. Contributions to Economics*, Physica, Heidelberg, 1999.
- [16] Y. Wang, Z. Cai, Z.-H. Zhan, B. Zhao, X. Tong, and L. Qi, "An optimization and auction-based incentive mechanism to maximize social welfare for mobile crowdsourcing," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 3, pp. 414–429, 2019.
- [17] P. Kaur, M. Goyal, and J. Lu, "A comparison of bidding strategies for online auctions using fuzzy reasoning and negotiation decision functions," *IEEE Transactions on Fuzzy Systems*, vol. 25, no. 2, pp. 425–438, 2017.
- [18] R. Carbonneau and R. Vahidov, "A multi-attribute bidding strategy for a single-attribute auction marketplace," *Expert Systems with Applications*, vol. 43, no. 1, pp. 42–50, 2016.
- [19] S. Sayman and Y. Akcay, "A transaction utility approach for bidding in second-price auctions," *Journal of Interactive Marketing*, vol. 49, no. 2, pp. 86–93, 2020.
- [20] Y. Wang, Z. Cai, X. Tong, Y. Gao, and G. Yin, "Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems," *Computer Networks*, vol. 135, pp. 32–43, 2018.
- [21] Y. Wang, Z. Cai, G. Yin, Y. Gao, X. Tong, and G. Wu, "An incentive mechanism with privacy protection in mobile crowdsourcing systems," *Computer Networks*, vol. 102, pp. 157–171, 2016.
- [22] Y. Wang, G. Yin, Z. Cai, Y. Dong, and H. Dong, "A trust-based probabilistic recommendation model for social networks," *Journal of Network and Computer Applications*, vol. 55, pp. 59–67, 2015.
- [23] I. Raykhel and D. Ventura, "Real-time automatic price prediction for eBay online trading," in *Proceedings of the Twenty-First Conference on Innovative Applications of Artificial Intelligence*, Pasadena, CA, USA, July 2009.
- [24] S. Khwaja, M. Naeem, A. Anpalagan, A. Venetsanopoulos, and B. Venkatesh, "Improved short-term load forecasting using bagged neural networks," *Electric Power Systems Research*, vol. 125, pp. 109–115, 2015.
- [25] L. Yu, Z. Wang, and L. Tang, "A decomposition-ensemble model with data-characteristic-driven reconstruction for crude oil price forecasting," *Applied Energy*, vol. 156, pp. 251–267, 2015.
- [26] J. Mendes-Moreira, C. Soares, A. M. Jorge, and J. F. D. Sousa, "Ensemble approaches for regression," *ACM Computing Surveys*, vol. 45, no. 1, pp. 1–40, 2012.
- [27] M. Oliveira and L. Torgo, "Ensembles for time series forecasting," *Proceedings of Asian Conference on Machine Learning*, vol. 39, pp. 360–370, 2014.
- [28] X. Li, L. Liu, L. Wu, and Z. Zhang, "Predicting the final price of online auction items," *Expert Systems with Application*, vol. 31, no. 3, pp. 542–550, 2006.

- [29] R. Ghani, "Price prediction and insurance for online auctions," *KDD '05: Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining*, 2005, pp. 411–418, New York, NY, USA, August 2005.
- [30] M. R. Khadge and M. V. Kulkarni, "Machine learning approach for predicting end price of online auction," in *2016 International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, India, August 2017.
- [31] J. Wang and B. Ravindran, "Time-utility function-driven switched Ethernet: packet scheduling algorithm, implementation, and feasibility analysis," *IEEE Transactions on Parallel and Distributed Systems*, vol. 15, no. 2, pp. 119–133, 2004.
- [32] A. Niromandfam, A. S. Yazdankhah, and R. Kazemzadeh, "Modeling demand response based on utility function considering wind profit maximization in the day-ahead market," *Journal of Cleaner Production*, vol. 251, article 119317, 2019.
- [33] B. Edelman and M. Schwarz, *Optimal auction design in a multi-unit environment: the case of sponsored search auctions, working paper*, Harvard University, 2006.
- [34] K. Ren, W. Zhang, K. Chang, Y. Rong, Y. Yu, and J. Wang, "Bidding machine: learning to bid for directly optimizing profits in display advertising," *IEEE Transactions on Knowledge & Data Engineering*, vol. 30, no. 4, pp. 645–659, 2018.
- [35] D. Xu, Y. Wang, P. Peng, S. Beilun, Z. Deng, and H. Guo, "Real-time road traffic state prediction based on kernel-KNN," *Transportmetrica A: Transport Science*, vol. 16, no. 1, pp. 104–118, 2020.
- [36] N. Cicek and H. Delic, "Demand response management for smart grids with wind power," *IEEE Transactions on Sustainable Energy*, vol. 6, no. 2, pp. 625–634, 2015.
- [37] N. Nisan, T. Roughgarden, E. Tardos, and V. Vazirani, *Algorithmic Game Theory*, Cambridge University Press, Cambridge, 2020.



## Research Article

# On Constructing $t$ -Spanner in IoT under SINR

Xiujuan Zhang <sup>1,2</sup>, Yongcai Wang <sup>1</sup>, Wenping Chen,<sup>1</sup> Yuqing Zhu,<sup>3</sup> Deying Li <sup>1</sup>,  
and Guangshun Li <sup>2</sup>

<sup>1</sup>School of Information, Renmin University of China, Beijing 100872, China

<sup>2</sup>School of Computer Science, Qufu Normal University, Rizhao 276826, China

<sup>3</sup>Department of Computer Science, California State University, Los Angeles, CA 90032, USA

Correspondence should be addressed to Deying Li; [deyingli@ruc.edu.cn](mailto:deyingli@ruc.edu.cn)

Received 25 October 2020; Revised 28 December 2020; Accepted 15 January 2021; Published 2 February 2021

Academic Editor: Zhuojun Duan

Copyright © 2021 Xiujuan Zhang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Following the recent advances in the Internet of Things (IoT), it is drawing lots of attention to design distributed algorithms for various network optimization problems under the SINR (Signal-to-Interference-and-Noise-Ratio) interference model, such as spanner construction. Since a spanner can maintain a linear number of links while still preserving efficient routes for any pair of nodes in wireless networks, it is important to design distributed algorithms for spanners. Given a constant  $t > 1$  as the required stretch factor, the problem of our concern is to design an efficient distributed algorithm to construct a  $t$ -spanner of the communication graph under SINR such that the delay for the task completion is minimized, where the delay is the time interval between the time slot that the first node commences its operation to the time slot that all the nodes finish their task of constructing the  $t$ -spanner. Our main contributions include four aspects. First, we propose a proximity range and proximity independent set (PISet) to increase the number of nodes transmitting successfully at the same time in order to reduce the delay. Second, we develop a distributed randomized algorithm SINR-Spanner to construct a required  $t$ -spanner with high probability. Third, the approximation ratio of SINR-Spanner is proven to be a constant. Finally, extensive simulations are carried out to verify the effectiveness and efficiency of our proposed algorithm.

## 1. Introduction

The Internet of Things (IoT) has attracted great attention in recent years, owing to its potential military and civilian applications [1, 2]. Such a network generally consists of a large number of autonomous network nodes, in which algorithms are usually distributed since these algorithms have to work without global information and coordinated central control. Hence, there is an imperative need to design efficient distributed algorithms for various network optimization problems in the IoT.

Constructing a  $t$ -spanner with a minimum number of edges is one of the fundamental network optimization problems since the spanner property is a critical requirement of topology control in the IoT [3]. The IoT is commonly modeled as a graph  $G(V, E)$ , in which  $V$  is the set of wireless nodes and  $E$  represents the set of communication links

(edges) connecting the nodes in  $V$ . A spanning subgraph  $H$  of  $G$  is called a  $t$ -spanner, for  $t \geq 1$  if for all pairs of nodes  $u, v \in V$ , the length of the shortest path from  $u$  to  $v$  in  $H$  is at most  $t$  times of that in  $G$ . Here,  $t$  is called the *stretch factor*. A spanner can not only decrease the number of links and maintain connectivity but also ensure that the length of a path between any pair of communication nodes is within some constant factor from the shortest possible one. Therefore, constructing a spanner of the communication graph is enormously helpful for topology control, geographic routing, and compact routing in the IoT [3].

Spanners have been extensively studied in computational geometry [4], in which  $G(V, E)$  is generally the complete Euclidean graph of the node set  $V$  in the Euclidean plane. However, even in the field of computational geometry, computing a minimum stretch factor spanner using not more than a given number of edges is NP-hard [5]. In the IoT,

current spanner construction algorithms either do not consider interference, such as [6], or only handle it under the protocol interference model [7].

However, when multiple nodes send messages at the same time, a node may be unable to receive the message from its given sender owing to the interference caused by simultaneous transmissions. The *protocol interference model* and the *SINR (Signal-to-Interference-and-Noise-Ratio) interference model* are the commonly used interference models. SINR can take into account cumulative interference of wireless communications and is more realistic [8], thus has been widely adopted now. However, designing and analyzing algorithms are challenging under the SINR model since each given receiver should compute accumulated interference generated by all other senders at the same time.

*1.1. Outline of the Problem.* In this paper, we consider a general case of constructing a  $t$ -spanner under SINR, namely  $t$ -spanner-SINR. That is, given a constant  $t$  as the required stretch factor, our objective is to design an efficient distributed algorithm for constructing a  $t$ -spanner of the communication graph to minimize the delay of constructing the  $t$ -spanner. The delay of constructing a  $t$ -spanner is defined as the time interval from the start time-slot that nodes start to work to the last time-slot that all the nodes finish their task of constructing the  $t$ -spanner.

A large scale IoT discussed in this work consists of  $n$  sensor nodes, with uniform transmission powers, deployed randomly and uniformly in the two-dimensional Euclidean space. Nodes act in synchronous rounds; in every communication round, a node can transmit a message and attempt to receive a message. Each node initially knows only its own unique ID and its own coordinates. Since we adopt the SINR interference model when nodes communicate, the pre-designed receivers can successfully decode the messages if and only if SINR constraints are satisfied. Owing to the accumulation and uncertainty of the SINR model, it is challenging to design a  $t$ -spanner distributed algorithm based on SINR in wireless networks. How to make more nodes transmit simultaneously and meanwhile make their given neighbor nodes successfully decode the messages is crucial to the performance of the algorithm under SINR.

The authors in [9] proposed a distributed algorithm SINR-Undirected-YG under SINR and proved that the resultant graph is a  $t$ -spanner. Zhang et al. [9] claim to be able to construct a spanner at  $O(\log n)$  time-slots, but the running time of its algorithm is very large during the simulation. In this paper, we study a general case of constructing a  $t$ -spanner under SINR and try to reduce the delay.

*1.2. Summary of Contributions.* The summary of contributions of this paper is as follows:

- (1) We identify the general case of constructing a  $t$ -spanner under SINR ( $t$ -spanner-SINR problem), and we design an efficient distributed algorithm SINR-Spanner to construct a required  $t$ -spanner under SINR with high probability, i.e., with a probability of at least  $1 - e^{-(n/4)}$ , where  $n$  is the total number

of nodes in the network. Moreover, the resultant  $t$ -spanner has  $O(n)$  edges

- (2) Our distributed algorithm SINR-Spanner is also a local algorithm, in which the topology can be locally and self-adaptively maintained based on the information from the neighbor nodes without affecting the whole network. We reasonably utilize one kind of proximity graph—Yao graph (YG)—to construct spanner under SINR. YGs divide the surrounding area of each node into  $k$  sectors of equal angles and add edges only to the nearest neighbor within each sector [10]. If there are two or more nearest neighbors in a sector, one can choose the first neighbor receiving the message. In our design, each node is capable of independently performing successful local broadcasts to collect its neighborhood information within a certain range, such that it can get the nearest neighbor in each sector and the resultant  $t$ -spanner is a special YG
- (3) We introduce the definition of proximity range and proximity-independent set (PISet) to increase the number of nodes transmitting successfully at the same time and to reduce the delay in the SINR-Spanner algorithm. The approximation ratio of SINR-Spanner is proven to be a constant
- (4) Extensive simulations are carried out to verify the effectiveness and efficiency of our proposed distributed and randomized algorithm

The rest of this paper is organized as follows. Section 2 reports the most related work. Section 3 precisely defines the formulation of the problem and introduces relevant models and notations. The spanner construction algorithm SINR-Spanner is presented in Section 4. Section 5 gives a theoretical analysis of the algorithm. In Section 6, we evaluate the performance of the algorithm via simulation. Section 7 concludes the paper with suggestions for future work.

## 2. Related Work

In this section, we first investigate the spanner algorithms in computational geometry and in the IoT, then discuss the method of applying randomized and distributed solutions under SINR.

*2.1.  $t$ -Spanner.* The book [4] by Narasimhan and Smid is a comprehensive overview of geometric spanners. For geometric spanners, several structures and methods have been proposed, such as the Greedy method [11], Well-Separated Pair Decomposition method, Delaunay triangulation,  $\theta$ -graphs, and YGs. Constructing YGs is one of the simplest ways of constructing  $t$ -spanners. Yao [10] used YGs to simplify the computation of the Euclidean minimum spanning tree. Althöfer et al. [11] firstly proved that YGs are the  $t$ -spanners for the corresponding complete graph. For the corresponding complete graph, YGs are  $1/(1 - 2 \sin(\pi/k))$ -spanners with  $k > 6$  [12].

In wireless networks, the spanner property was first discussed by Li et al. in [6]. They modeled the network as a unit disk graph (UDG) and analyzed the energy stretch factor of several common subgraphs of a UDG:  $n - 1$  for the relative neighborhood graph (RNG), 1 for the Gabriel graph (GG), and  $O(1)$  for YG. And these proximity graphs have been widely used in spanner construction as subgraphs of a UDG. There also exist spanner construction mechanisms for quasi-unit disk graphs, disk graphs, and unit ball graphs [13]. In [14], Kothapalli et al. proposed a local-control protocol for establishing a constant density spanner among a set of mobile stations. The LISE (low interference spanner establisher) algorithm was presented to establish a spanner in [7], where the interference definition is based on how many nodes are affected by the communication over a certain link. However, since the above spanner algorithms for wireless networks are all studied without considering interference or handling interference under the protocol interference model, they cannot deal with interference effectively under the SINR interference model. Zhang et al. [9] first consider spanner construction under SINR, and this work improves it.

Constructing spanners under a computational geometry field greatly promotes the study under the wireless network setting. Meanwhile, wireless network requirements, which generally need to efficiently satisfy various topological characteristics, encourage the development of geometric spanner construction. Recent results on sparse geometric spanners focused on satisfying one or multiple topological characteristics such as lightness, small degree [15], fault tolerance, no central agent [16], and multiple characteristics [17].

**2.2. SINR Model.** In wireless networks, the SINR model received increasing attention [8]. Despite the vast amount of researches in the design and analysis of centralized algorithms under SINR [18], few results are known about distributed solutions in this model, especially for global communication tasks, owing to the accumulation and uncertainty of interference.

There is a growing interest in developing randomized distributed solutions to local broadcast [19], which is defined as successfully transmitting a message to all neighbors in the corresponding reachable proximity of a node. Randomized distributed solutions to local broadcast are often used as a building block for global communication tasks, such as multiple-message broadcast [20], synchronization [21], and multiple channels broadcast [22]. In [20], selected leader nodes adopt local broadcast to collect the messages that arrive at their dominated nonleader nodes and then disseminate the received messages to the whole network. The algorithm in [21] starts from very low probabilities and increases them gradually until nodes can hear a reasonable number of messages and implement all nodes' clock synchronization. In [22], the selected leader in different channel collects locally the messages of its dominated nonleader nodes in the same channel to speedup multiple channel broadcast. Note that most of the existing distributed and randomized works under SINR are still in the theoretical stage except [19] and Fuchs's coloring study, such as [23]. Using local broadcasting as a basic unit, we propose an algorithm of

spanner construction in this paper and perform simulations to verify the performance of the algorithm.

### 3. Model and Problem Formulations

Assume that a set  $V$  of  $n$  wireless network nodes, modeled as a graph  $G$ , is deployed randomly and uniformly in a 2-dimensional geographic plane. Nodes act in synchronous rounds. Each node is conscious of its ID and coordinates and has the same transmission power  $P$  ( $P > 0$ ). Let the Euclidean distance for the two endpoints  $u$  and  $v$ , denoted by  $d_{uv}$ , be the length of an edge in  $G$ . And let  $d_{uv}(G)$  be the length of the shortest path between  $u$  and  $v$  in  $G$  which is defined as the sum of the lengths of its edges.

A commonly assumed model for the propagation effect of wireless nodes is deterministic path loss, i.e.,  $P_r = P/d_{uv}^\alpha$ , where  $u$  transmits a message to  $v$ ,  $P_r$  is the received power at a receiver  $v$ , and  $\alpha$  is the path loss exponent (typically,  $2 < \alpha \leq 6$ ). A deterministic path loss model is applied to the following interference model.

**3.1. SINR (Signal-to-Interference-and-Noise-Ratio) Interference Model.** In the SINR model, a transmission from node  $u$  to node  $v$  is successful iff the SINR condition holds:

$$\frac{P/d_{uv}^\alpha}{N + \sum_{w \in T \setminus \{u\}} (P/d_{wv}^\alpha)} \geq \beta, \quad (1)$$

where  $T \subseteq V$  is the set of transmitting nodes,  $\alpha \in (2, 6]$  is the path loss exponent depending on the network environment,  $\beta > 1$  is a hardware-defined threshold, and  $N$  is the environmental noise.

The transmission range  $R_{\max}$  of a node  $u$  is the maximum distance at which a node  $v$  can receive a clear transmission from  $u$  while no other node is transmitting at the same time, i.e.,  $\sum_{w \in T \setminus \{u\}} (P/d_{wv}^\alpha) = 0$ . The SINR condition (1) tells us that

$$R_{\max} = (P/N\beta)^{1/\alpha}, \quad (2)$$

for the given power level  $P$ . Note that  $R_{\max}$  is for only one node  $u$  transmitting in the whole network at the time slot.

**3.2. Local Broadcasting Range ( $R_b$ ).** We set the local broadcasting range

$$R_b = (1 - \varepsilon)R_{\max}, \quad (3)$$

where  $0 \leq \varepsilon < 1$  is a fixed model parameter.

We say a node transmits  $R_b$  successfully in a time slot if it transmits a message, and this message is received by all its neighbors in a distance smaller or equal to  $R_b$  in the time slot. In Section 4, we define the proximity range  $R_p$  such that the nodes which are in a distance greater or equal to  $R_p$  can transmit  $R_b$  successfully at the same time slot.

We denote the region within  $R_b$  of node  $u$  as a local broadcasting region  $B_u$  and the number of nodes in it as  $\Delta_u^b$ . Furthermore, let  $\Delta^b = \max_{u \in V} \{\Delta_u^b\}$ .

**3.3. Communication Graph.** The communication graph  $G^{R_b}(V, E^{R_b})$  of a given network consists of all network nodes and edges  $(u, v)$  such that  $d_{uv} \leq R_b$ . Since  $R_{\max}$  is for only one transmission in the whole network at the same time, we adopt a slightly smaller range  $R_b$  as [22] which suffice for practical communication. In the communication graph  $G^{R_b}(V, E^{R_b})$ , which is simply denoted by  $G^{R_b}(V)$ , a node  $v$  is a neighbor of node  $u$  if  $d_{uv} \leq R_b$ .

**3.4. Yao Graph (YG).** The directed Yao graph  $\overrightarrow{YG}_k(V)$  with a fixed integer parameter  $k > 0$  is defined as follows. Any  $k$  equally separated rays starting at the origin node define  $k$  sectors. The orientation of the cut is identical for all nodes. Translate the sectors to each node  $u \in V$ . In each sector with a node  $u$ , pick the shortest directed edge  $\langle u, v \rangle$ , if there is one, to  $\overrightarrow{YG}_k(V)$ . Ties are broken arbitrarily.

This implies that  $\overrightarrow{YG}_k(V)$  preserves the shortest outgoing edge in each sector. Accordingly,  $\overleftarrow{YG}_k(V)$  preserves the shortest incoming edge in each sector.

An undirected Yao graph, in which the edge directions are ignored, is denoted by  $YG_k(V)$ .  $YG_k^{R_b}(V)$  is the Yao graph in which only the edges whose lengths are no more than  $R_b$  are preserved from  $YG_k(V)$ . In other words,  $YG_k(V)$  is the spanning subgraph of a complete Euclidean graph  $K_n(V)$  on node set  $V$  and  $YG_k^{R_b}(V)$  is the spanning subgraph of  $G^{R_b}(V)$ .

**3.5.  $t$ -Spanner.** Let  $t > 1$  be a real number. A spanning subgraph  $H(V, E_H)$  of  $G(V, E)$  is said to be a  $t$ -spanner of  $G$ , if for any two nodes  $u$  and  $v$  in  $V$ , the shortest path between  $u$  and  $v$  in  $H$ , whose length is at most  $t$  times that of the shortest path in  $G$ , i.e.,

$$d_{uv}(H) \leq t \cdot d_{uv}(G). \quad (4)$$

The constant  $t$  is called the *stretch factor* of  $H$  (w.r.t.  $G$ ). Note that  $G$  can be  $K_n(V)$  or a communication graph that is a spanning subgraph of  $K_n(V)$ .

**3.6. Delay of Constructing a  $t$ -Spanner.** The delay of constructing a  $t$ -spanner is defined as the time interval from the start time slot that the first node starts to work to the last time slot that all the nodes finish their task of constructing the  $t$ -spanner.

Next, we present the definition of the problem, the  $t$ -spanner under the SINR problem, which is our focus in this paper.

**3.7.  $t$ -Spanner under the SINR Problem ( $t$ -Spanner-SINR).** Assume that a set  $V$  of  $n$  wireless network nodes deployed randomly and uniformly in a 2-dimensional geographic plane, in which each node is aware of its ID and coordinates, has the same transmission power  $P$  ( $P > 0$ ) and a local broadcasting range  $R_b$ ; given a constant  $t > 1$ , the goal is to design a distributed algorithm to find a  $t$ -spanner of the corresponding communication graph  $G^{R_b}(V, E^{R_b})$  under SINR, such that the delay of constructing a  $t$ -spanner is minimized.

## 4. Algorithm

**4.1. Algorithm Outline.** The main idea of our algorithm is to construct  $YG_k(V)$  for the  $t$ -spanner-SINR problem. The reason is that the  $YG_k(V)$  graph is a  $t = 1/(1 - 2 \sin(\pi/k))$ -spanner [9]. Consequently, given a constant  $t > 1$ , we compute a  $k$  and construct  $YG_k(V)$  under SINR in our distributed algorithm to get the required  $t$ -spanner.

To construct  $YG_k(V)$ , each node  $u$  needs the node  $v$ 's information which is the closest to  $u$  in the sector  $v$  belongs. Accordingly, each node should locally broadcast its ID and coordinates to its neighbors. However, if all the nodes transmit together under SINR, no node will receive any message owing to the interference. To avoid collision, each node could locally broadcast one by one. However, in a distributed algorithm, there is not a centralized coordination for arranging nodes to transmit in sequence. Accordingly, each node can only transmit with the probability  $1/n$ . Furthermore, in order to reduce the delay, it has an obligation to have as many nodes as possible to transmit simultaneously. Therefore, each node will make a range as the radius of its neighborhood circle region and next take the inverse of the number of nodes in its neighborhood circle region as the sending probability.

First, we will compute the range and give the node set in which all nodes can transmit simultaneously.

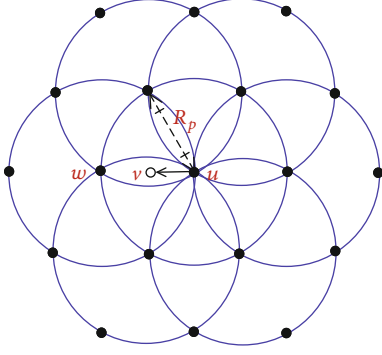
**4.2. Proximity Range and Proximity Independent Set (PISet).** How to make more nodes transmit simultaneously and meanwhile make their neighbor nodes successfully decode the messages is crucial for the performance of the algorithms under SINR. Thus, we define the proximity range  $R_p$  such that any nodes  $u$  and  $v$  can transmit simultaneously if  $d_{uv} \geq R_p$ . Intuitively, a tiny  $R_p$  implies a high degree of channel utilization. We examine how to set a proper  $R_p$  to guarantee SINR threshold and meanwhile the highest channel utilization degree. For clarity, we define the proximity range and proximity independent set as follows.

**4.2.1. Proximity Range  $R_p$  and the Corresponding Proximity Independent Set  $PISet_p$ .** Proximity range  $R_p$  is a length, and a  $PISet_p$  is a subset of  $V$  that satisfies  $d_{uv} \geq R_p$  for  $\forall u, v \in PISet_p$  ( $u \neq v$ ). A  $PISet_p$  is maximal if and only if  $d_{uw} < R_p$  for  $\forall u \in PISet_p$  and  $\forall w \notin PISet_p$ . How to design  $R_p$ ? The basic idea underlying the design is to ensure the nodes in the same  $PISet_p$  transmit simultaneously and all their neighbors receive the message successfully.

We refer to the region within  $R_p$  of node  $u$  as proximity region  $X_u$  and the number of nodes in it as  $\Delta_u^p$ . Besides, let  $\Delta^p = \max_{u \in V} \{\Delta_u^p\}$ .

Before designing  $R_p$ , we first give an example for  $R_p$  and  $PISet_p$ .  $R_p$  and  $PISet_p$  are illustrated in Figure 1 where 19 nodes represented by solid circles are in the same  $PISet_p$ . Note that this  $PISet_p$  is maximal. The distance between the given receiver  $v$  with the sender  $u$  and the nearest of other senders, which is  $w$  in Figure 1, is at least  $(R_p - R_b)$ . In other words,  $d_{uv} \geq (R_p - R_b)$  in Figure 1.



FIGURE 1: Proximity range  $R_p$  and a corresponding  $\text{PISet}_p$ .

By observing the above example, we give the specific relationship between  $R_p$  and  $R_b$  in the following theorem.

**Theorem 1.** Suppose that  $R_p = (c_2 \cdot \beta \cdot (c_1/(c_1 - 1)))^{1/\alpha} \cdot R_b + R_b$  where  $c_1 = (1/(1 - \varepsilon)^\alpha) > 1$  and  $c_2 = 6 + (\pi^2 - 6)(\sqrt{3}/2)^{-\alpha}$ , the nodes in the same  $\text{PISet}_p$  can transmit  $R_b$  successfully at the same time slot.

*Proof.* Let  $I = R_p - R_b$ . We begin by estimating the smallest value of  $I$  when  $u$  transmits to  $v$  successfully and  $u$  transmits simultaneously with other nodes in the same  $\text{PISet}_p$ . Further, we prove that the nodes in the same  $\text{PISet}_p$  can transmit  $R_b$  successfully at the same time slot with the above  $I$ . We say a node transmits  $R_b$  successfully in a time slot if it transmits a message and this message is received by all its neighbors in a distance smaller or equal to  $R_b$  in the time slot.

In order for  $v$  to be able to receive the message from  $u$ , we require  $\text{SINR}_{uv} \geq \beta$ .

Thus,

$$\frac{P/d_{uv}^\alpha}{N + \sum_{w \in \text{PISet}_p \setminus \{u\}} (P/d_{wv}^\alpha)} \geq \beta. \quad (5)$$

Since the equations (2) and (3),  $N = P/c_1 \beta R_b^\alpha$  where  $c_1 = 1/(1 - \varepsilon)^\alpha$  is a fixed parameter.

Now

$$\begin{aligned} \frac{P/d_{uv}^\alpha}{N + \sum_{w \in \text{PISet}_p \setminus \{u\}} (P/d_{wv}^\alpha)} &= \frac{P/d_{uv}^\alpha}{(P/c_1 \beta R_b^\alpha) + \sum_{w \in \text{PISet}_p \setminus \{u\}} (P/d_{wv}^\alpha)} \\ &= \frac{d_{uv}^{-\alpha}}{(R_b^{-\alpha}/c_1 \beta) + \sum_{w \in \text{PISet}_p \setminus \{u\}} d_{wv}^{-\alpha}}. \end{aligned} \quad (6)$$

We derive the lower bound of the above formula. First,  $d_{uv}^{-\alpha} \geq R_b^{-\alpha}$  since  $R_b$  is the maximum local broadcasting range of a node. Furthermore, if a node  $w$  transmit together with  $u$  as shown in Figure 1,  $w$  produces the largest interference when  $w$  and the given receiver  $v$  have the closest distance  $I$ . If we represent a link as a node as shown in Figure 2(a), for the nodes in the  $\text{PISet}_p$ , the densest packing of interfering links is the hexagon packing [24] with edge length  $I$  as shown

in Figure 2(b). There are at most six nodes in the first layer, and the distance is  $I$  with respect to the abstracting node  $uv$ . Furthermore, the distance between  $uv$  and any node in the  $l$ th ( $l \geq 2$ ) layer is no less than  $(\sqrt{3}/2)lI$  with the  $l$ th layer having at most  $6l$  nodes.

$$\begin{aligned} \sum_{w \in \text{PISet}_p \setminus \{u\}} d_{wv}^{-\alpha} &\leq 6 \cdot I^{-\alpha} + \sum_{l \geq 2} 6l \cdot \left(\frac{\sqrt{3}}{2}lI\right)^{-\alpha} \\ &= 6 \cdot I^{-\alpha} + 6 \cdot \left(\frac{\sqrt{3}}{2}I\right)^{-\alpha} \cdot \sum_{l \geq 2} l^{-\alpha+1}. \end{aligned} \quad (7)$$

Since  $\sum_{l \geq 2} l^{-\alpha+1} = \zeta(\alpha - 1) - 1$ , where  $\zeta(\cdot)$  is the Riemann zeta function, considering that  $\alpha \geq 3$ , then  $\zeta(\alpha - 1) \leq \zeta(2) = \pi^2/6$ . Thus, we have

$$\begin{aligned} \sum_{w \in \text{PISet}_p \setminus \{u\}} d_{wv}^{-\alpha} &\leq 6 \cdot I^{-\alpha} + 6 \cdot \left(\frac{\sqrt{3}}{2}I\right)^{-\alpha} \cdot \left(\frac{\pi^2}{6} - 1\right) \\ &= \left(6 + (\pi^2 - 6) \left(\frac{\sqrt{3}}{2}\right)^{-\alpha}\right) \cdot I^{-\alpha} = c_2 \cdot I^{-\alpha}, \end{aligned} \quad (8)$$

where  $c_2 = 6 + (\pi^2 - 6)(\sqrt{3}/2)^{-\alpha}$ .

Therefore, to make  $(d_{uv}^{-\alpha}/((R_b^{-\alpha}/c_1 \beta) + \sum_{w \in \text{PISet}_p \setminus \{u\}} d_{wv}^{-\alpha})) \geq \beta$  valid, it is sufficient to have

$$\frac{R_b^{-\alpha}}{(R_b^{-\alpha}/c_1 \beta) + c_2 I^{-\alpha}} \geq \beta. \quad (9)$$

Therefore,  $I \geq (c_2 \cdot \beta \cdot (c_1/(c_1 - 1)))^{1/\alpha} \cdot R_b$ .

Hence,  $R_p = (c_2 \cdot \beta \cdot (c_1/(c_1 - 1)))^{1/\alpha} \cdot R_b + R_b$ , where  $c_1 = 1/(1 - \varepsilon)^\alpha > 1$  and  $c_2 = 6 + (\pi^2 - 6)(\sqrt{3}/2)^{-\alpha}$ .

Conversely, if  $R_p$  have the value as shown in the above, the nodes in the same  $\text{PISet}_p$ , which is maximal as shown in Figure 1 or not maximal, can transmit  $R_b$  successfully at the same time slot since the receiver power is no less than  $(P \cdot) R_b^{-\alpha}$  in (9) and the cumulative interference is less than  $(P \cdot) c_2 I^{-\alpha}$ .

Figure 3 depicts visually the relation between proximity range  $R_p$  and local broadcasting range  $R_b$  with different  $\alpha$ ,  $\beta$ , and  $\varepsilon$ , which is helpful to pick these values during subsequent algorithm simulation. These parameters are reasonably set as follows: the path loss exponent  $\alpha \in \{3, 4, 5, 6\}$ , the threshold  $\beta \in [1, 10]$ , and  $\varepsilon \in [0.4, 0.95]$ . From Figure 3, one can see that  $R_p$  increases when  $\alpha$  decreases,  $\beta$  increases, and  $\varepsilon$  decreases. So we can get that  $R_p$  is as about 2.57 times at a minimum as  $R_b$  when  $\alpha = 6$ ,  $\beta = 1$ , and  $\varepsilon = 0.95$ , while  $R_p$  is as about 6.34 times at a maximum as  $R_b$  when  $\alpha = 3$ ,  $\beta = 10$ , and  $\varepsilon = 0.4$ .

**4.3. Algorithm.** From the above Theorem 1, the nodes in the same  $\text{PISet}_p$  can transmit  $R_b$  successfully at the same time slot while each node takes the value of  $R_p$  as Theorem 1, so the sending probability for each node  $u$  is set to the inverse of the number of nodes in its proximity region  $\Delta_u^p$ . Thus, we



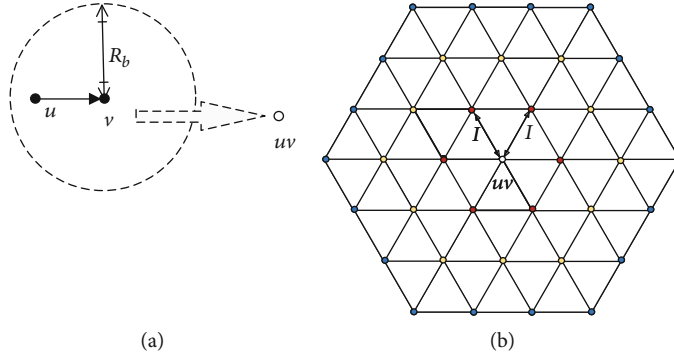


FIGURE 2: Link abstraction and the densest packing of interfering links.

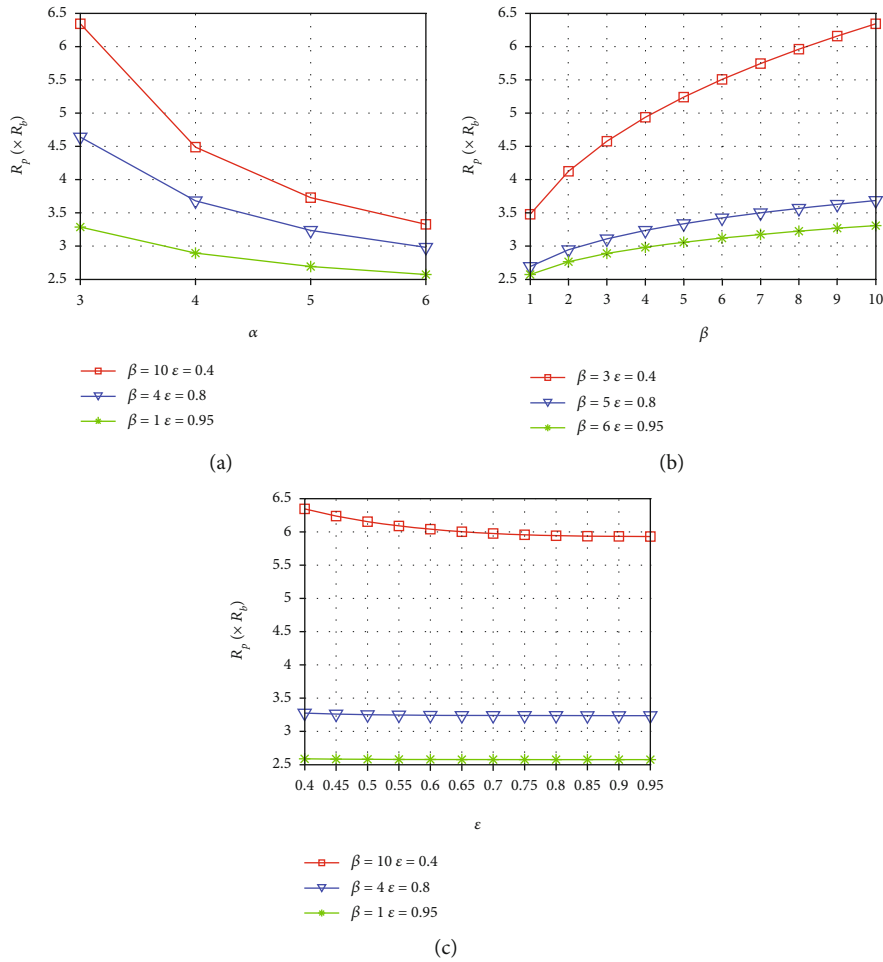


FIGURE 3:  $R_p$  vs.  $\alpha$ ,  $\beta$ , and  $\epsilon$ .

guess all its neighbors can receive the message successfully with high probability, and we will give the proof in the next section. The pseudo-code for node  $u$  is given in Algorithm 1, which implies that each node runs it independently.

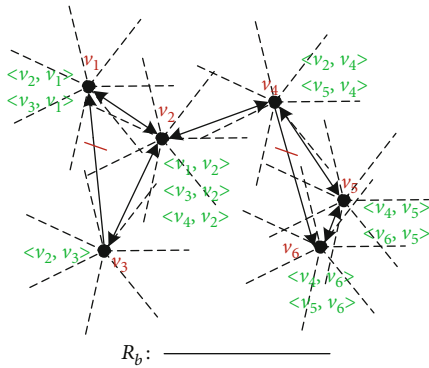
Now, we describe the full operation of our distributed algorithm SINR-Spanner. Each node  $u$  carries out the same operations and has its local memory. The algorithm consists of three parts. In part 1 (line 1-line 5), each node performs initialization work. Each node  $u$  first computes the required

number of sectors depending on the given stretch factor  $t$ . Then, each node  $u$  takes the inverse of  $\Delta_u^p$  as the sending probability. Thus how to obtain  $\Delta_u^p$  a priori is critical to our algorithm design. Some existing works, such as [19, 23], assume the availability of  $\Delta_u^p$  to facilitate the algorithm design and analysis. Such requirements are common under SINR in order to enable initial communication. Therefore, in our algorithm, we also assume that  $\Delta_u^p$  is available to simplify the presentation. In part 2 (line 6-line 20), each node obtains

```

1: Initialize the stretch factor  $t$ ;
2: Initialize  $k = \lceil \pi / \arcsin((t-1)/(2t)) \rceil$ ;
3: Compute the number of nodes in its proximity region, i.e.,  $\Delta_u^p$ ;
4: Initialize  $p_u = 1/\Delta_u^p$ ;
5: Initialize  $I_u[i] = -1$  for  $i = 1, 2, \dots, k$ ;
6: for  $j = 1$  to  $\Delta^p$  time-slots do
7:   Send a message containing its ID  $u$  and coordinates with probability  $p_u$ , and remains listening with probability  $1 - p_u$ ;
8:   while receiving a message from some node  $v$  do
9:      $i =$  the index of the sector to which  $v$  belongs;
10:    if  $I_u[i] == -1$  or the distance  $d_{I_u[i]u} > d_{vu}$  then
11:       $I_u[i] = v$ 
12:    end if
13:  end while
14: end for
15:  $\overleftarrow{E}_u = \emptyset$ ;
16: for  $i = 1$  to  $k$  do
17:   if  $I_u[i] \neq -1$  then
18:      $\overleftarrow{E}_u = \overleftarrow{E}_u \cup \langle I_u[i], u \rangle$ ;
19:   end if
20: end for
21:  $E_u = \{(u, v) \mid \langle v, u \rangle \in \overleftarrow{E}_u\}$ ;
22: for  $i = 1$  to  $\Delta^p$  time-slots do
23:   Broadcast the incoming neighbor set with probability  $p_u$ ;
24:   while receiving a message from some node  $v$  do
25:     if  $u$  is the incoming neighbor of  $v$  and  $(u, v) \notin E_u$  then
26:        $E_u = E_u \cup (u, v)$ ;
27:     end if
28:   end while
29: end for

```

ALGORITHM 1: SINR-Spanner( $u$ ).FIGURE 4:  $\overleftarrow{YG}_k^{R_b}(V)$  after part 2, where  $k = 7$ .

the incoming neighbor in each sector by receiving the neighbors' messages, and thus, a directed Yao graph forms. Figure 4 shows an intermediate result after part 2 in which there are 6 nodes; the edge length is at most  $R_b$  and  $k = 7$ . Here,  $\overrightarrow{E}_{v_1} = \{\langle v_3, v_1 \rangle, \langle v_2, v_1 \rangle\}$ ,  $\overrightarrow{E}_{v_2} = \{\langle v_1, v_2 \rangle, \langle v_3, v_2 \rangle, \langle v_4, v_2 \rangle\}$ ,  $\overrightarrow{E}_{v_3} = \{\langle v_2, v_3 \rangle\}$ , and so on. In part 3 (line 21-line 29), each node sends an acknowledgement message back to its incoming neighbor, and thus, an undirected Yao graph is constructed which is a  $t$ -spanner we require. An example of  $\overleftarrow{YG}_k^{R_b}(V)$  is

presented in Figure 5, in which edge directions are ignored from the graph shown in Figure 4. Here,  $E_{v_1} = \{(v_1, v_2), (v_1, v_3)\}$ ,  $E_{v_2} = \{(v_2, v_1), (v_2, v_3), (v_2, v_4)\}$ ,  $E_{v_3} = \{(v_3, v_1), (v_3, v_2)\}$ , and so on.  $E_{v_1}$  has local data  $(v_1, v_3)$ , and  $E_{v_3}$  has local data  $(v_3, v_1)$ ; thus, the undirected edge  $(v_1, v_3)$  is known by two endpoints.

Our distributed and randomized algorithm SINR-Spanner, which is different from the algorithms in [9], can solve the  $t$ -spanner-SINR problem. In part 1, the algorithm first initializes the stretch factor  $t$  to attain a  $t$ -spanner. The sending probability for each node  $u$  is set to the inverse of  $\Delta_u^p$  to reduce the delay; then,  $u$  repeats randomized transmission for  $8\Delta^p$  time slots, respectively, in part 2 and part 3.

## 5. Performance Analysis of Algorithm SINR-Spanner

**5.1. The Delay of SINR-Spanner.** In order to obtain the main result of this section in Theorem 8, we first prove that a graph  $\overleftarrow{YG}_k^{R_b}(V)$  is constructed with high probability after the algorithm SINR-Spanner terminates in  $16\Delta^p + c$  time slots in Theorem 3; next, analyze why the resultant  $\overleftarrow{YG}_k^{R_b}(V)$  is the required  $t$ -spanner of the communication graph  $G^{R_b}(V)$  in Theorem 3.

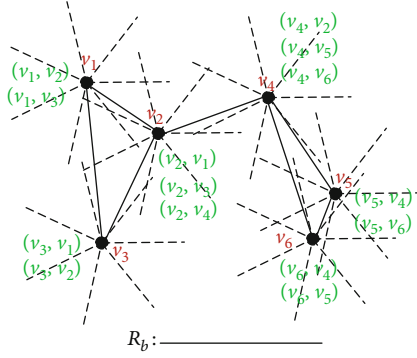


FIGURE 5:  $YG_k^{R_b}(V)$  after part 3, where  $k = 7$ .

Now, we give a form of Chernoff bounds which can be found in [22] and some advanced textbooks, such as [25], for the proof of Theorem 3.

**Lemma 2** [22, 25] (Chernoff bounds). *Let  $0 < \delta \leq 1$  and  $X_1, X_2, \dots, X_n$  be independent Bernoulli random variables, and let  $X := \sum_{i=1}^n X_i$  and  $\mu = E[X]$ . Then, for any  $\delta > 0$ , it holds that*

$$\text{Prob}(X < (1 - \delta)\mu) < \left( \frac{e^{-\delta}}{(1 + \delta)^{(1 + \delta)}} \right)^\mu < e^{-\delta^2 \mu / 2}. \quad (10)$$

And for  $\delta = 1/2$ ,

$$\text{Prob}\left(X < \frac{1}{2}\mu\right) < e^{-\mu/8}. \quad (11)$$

**Theorem 3.** *A graph  $YG_k^{R_b}(V)$  is constructed with high probability after the algorithm SINR-Spanner terminates in  $16\Delta^p + c$  time-slots, where  $\Delta^p$  is the maximum of the node number in one proximity region and  $c$  is a constant for the number of time slots for the initialization work.*

*Proof.* Since  $R_p$  is as about 2.57 times to 6.34 times as  $R_b$  from Theorem 1 and the resultant graph is connected,  $\Delta_u^p > 2$  for any node  $u$ . The probability that  $u$  transmits as the only transmitting node in its proximity region is

$$C_{\Delta_u^p}^1 \cdot \frac{1}{\Delta_u^p} \cdot \left(1 - \frac{1}{\Delta_u^p}\right)^{\Delta_u^p - 1} = \left(1 - \frac{1}{\Delta_u^p}\right)^{\Delta_u^p - 1} > \left(1 - \frac{1}{\Delta_u^p}\right)^{\Delta_u^p} > \frac{1}{4}. \quad (12)$$

The last inequality holds, since  $(1 - (1/\Delta_u^p))^{\Delta_u^p}$  increases when  $\Delta_u^p$  increases, and it obtains the minimum value  $1/4$  when  $\Delta_u^p$  is 2.

Since the nodes can transmit  $R_b$  successfully if they belong to the same PISet $_p$  owing to Theorem 1, there are at least  $n/\Delta^p$  nodes transmitting together in one time slot. Consequently, there are at least  $(n/\Delta^p) \cdot (1/4)$  nodes transmitting  $R_b$  successfully together in one time slot.

Therefore, after  $8\Delta^p$  time slots, there are at least  $2n$  nodes transmitting  $R_b$  successfully in expectation. By Chernoff bound (Lemma 2), after  $8\Delta^p$  time slots, the probability

$$\text{Prob}(X < n) = \text{Prob}\left(X < \left(1 - \frac{1}{2}\right) \cdot 2n\right) < e^{-n/4}. \quad (13)$$

Therefore, the probability for all  $n$  nodes transmitting  $R_b$  successfully is

$$\text{Prob}(X = n) = 1 - \text{Prob}(X < n) \geq 1 - e^{-n/4}. \quad (14)$$

Thus, after  $8\Delta^p$  time slots in part 2 of the algorithm SINR-Spanner, all the node transmit its ID and coordinates  $R_b$  successfully with high probability, i.e., each node obtains the “nearest” incoming neighbor in its proper sectors. Then, after a further  $8\Delta^p$  time slots in part 3, all the node transmit acknowledgement messages  $R_b$  successfully with high probability. As a result, a graph  $YG_k^{R_b}(V)$  is constructed with high probability.

In addition, the number of time slots for the initialization work in part 1 is a constant, which is denoted by  $c$ . So the algorithm SINR-Spanner terminates in  $16\Delta^p + c$  time slots.

Obviously, the number of nodes in the proximity region is upper bound by  $n$ . If  $\Delta^p = n$ , a graph  $YG_k^{R_b}(V)$  is constructed with high probability in  $16n + c$  time slots.

Next, in order to prove that the resultant  $YG_k^{R_b}(V)$  of the algorithm is a  $t$ -spanner of the communication graph  $G^{R_b}(V)$ , we apply some conclusions about  $YG_k(V)$  where  $YG_k(V)$  is constructed from  $K_n(V)$ .

**Lemma 4** ([11]). *If  $V$  is a set of  $n$  points in the plane, and the integer  $k \geq 2$ , then the graph  $YG_k(V)$  contains at most  $kn = O(n)$  edges.*

**Lemma 5** ([12]). *Let  $t = 1/(1 - 2 \sin(\pi/k))$  for the integer  $k > 6$ ,  $YG_k(V)$  is a  $t$ -spanner of  $K_n(V)$ , where  $n$  is the number of nodes in  $V$ .*

In the next, we show that  $YG_k^{R_b}(V)$  is the required  $t$ -spanner of the communication graph  $G^{R_b}(V)$  if  $G^{R_b}(V)$  is connected in the following lemma of our previous work [9]. Zhang et al. [9] first give the condition that  $G^{R_b}(V)$  is connected if and only if the longest edge in Euclidean minimum spanning tree of the node set  $V$  is at most  $R_b$ . Note that if the nearest neighbor of each node in every sector is within the local broadcast region, the graph  $YG_k^{R_b}(V)$  is a  $YG_k(V)$  and it is also a  $1/(1 - 2 \sin(\pi/k))$ -spanner of  $K_n(V)$ .

**Lemma 6** ([9]). *Let  $t = 1/(1 - 2 \sin(\pi/k))$ . If  $G^{R_b}(V)$  is connected and the integer  $k > 6$ ,  $YG_k^{R_b}(V)$  is a  $t$ -spanner of  $G^{R_b}(V)$ .*

Now, we show that the resultant  $YG_k^{R_b}(V)$  of the algorithm is a  $t$ -spanner of the communication graph  $G^{R_b}(V)$ .

**Theorem 7.** *Given a constant  $t > 1$ , setting  $k = \lceil \pi / (\arcsin((t-1)/(2t))) \rceil$ , the resultant graph  $YG_k^{R_b}(V)$  is the required*

*t*-spanner with at most  $kn$  edges after the algorithm SINR-Spanner terminates.

*Proof.* As  $k > 6$ , the sector angle is not larger than  $\pi/6$ . Hence,  $\sin(\pi/k)$  is a monotone decreasing function of  $k$ , and its value is less than  $1/2$ . As a result,  $t(=1/(1-2\sin(\pi/k)))$  increases as  $k$  increases when  $k > 6$  and approaches 1 as  $k \rightarrow \infty$ , i.e.,  $t$  is an injective and increasing function of  $k$ . Hence, its inverse function  $k = \pi/(\arcsin((t-1)/(2t)))$  is a decreasing function of  $t$ . Therefore, given a constant  $t > 1$ , we will find a  $k$  such that the Yao graph with the number of sectors of no less than  $k$  is the required  $t$ -spanner.

Since the number of sectors is an integer, and the number of edges becomes larger as the number of sectors increases from Lemma 4,  $k$  is assigned to  $\lceil \pi/\arcsin((t-1)/(2t)) \rceil$ . Therefore, the resultant graph  $YG_k^{R_b}(V)$  is the required  $t$ -spanner. Furthermore,  $YG_k^{R_b}(V)$  have  $kn$  edges by Lemma 4.

Based on Theorems 3 and 7, we can state the main conclusion of this section in Theorem 8.

**Theorem 8.** *The distributed algorithm SINR-Spanner constructs the required  $t$ -spanner with high probability, and the delay is  $16\Delta^p + c$  time slots, where  $\Delta^p$  is the maximum of the node number in one proximity region and  $c$  is a constant for the number of time slots for the initialization work.*

Lastly, Table 1 illustrates the relation between the stretch factor  $t$  and the number of sectors  $k$  in theory. In SINR-Spanner,  $k$  is the value in the second row given the corresponding  $t$  in the first row. Note that  $t = 1/(1-2\sin(\pi/k))$  is the upper theory bound of the stretch factor for  $YG_k^{R_b}(V)$  with respect to  $G^{R_b}(V)$  so far, maybe a smaller  $k$  is sufficient in practical.

**5.2. The Approximation Ratio of SINR-Spanner Algorithm.** The goal of  $t$ -spanner-SINR problem is to find a suitable  $t$ -spanner under SINR and to minimize the delay in the construction. Now, we try to give the approximation ratio of the SINR-Spanner algorithm. The basic idea of our algorithm is that each node should locally broadcast its ID and coordinates to its neighbors  $R_b$  successfully under SINR. In order to reduce the delay, there should be as many nodes as possible to transmit simultaneously. As we see, in the SINR-Spanner algorithm, the nodes in different proximity region can transmit simultaneously. Now, we consider whether the nodes in a different local broadcasting region can transmit simultaneously, then discuss the approximation ratio of SINR-Spanner.

**Theorem 9.** *The approximation ratio of the algorithm SINR-Spanner is bounded by  $(e/2) \cdot (R_p^2/R_b^2)$ .*

*Proof.* The probability that any node  $u$  transmits as the only transmitting node in its local broad region is

$$C_{\Delta_u^b}^1 \cdot \frac{1}{\Delta_u^b} \cdot \left(1 - \frac{1}{\Delta_u^b}\right)^{\Delta_u^b-1} = \left(1 - \frac{1}{\Delta_u^b}\right)^{\Delta_u^b-1}. \quad (15)$$

Let  $S$  be the total area of wireless nodes distribution. Assume that a node as the only transmitting node in its local broadcasting region can transmit  $R_b$  successfully, the number of nodes transmitting  $R_b$  successfully in one time slot is

$$\frac{S}{\pi R_b^2} \cdot \left(1 - \frac{1}{\Delta_u^b}\right)^{\Delta_u^b-1}. \quad (16)$$

In fact, the assumption cannot be guaranteed by theory and the following simulation, i.e., even though a node is the only transmitting node in its local broadcasting region, the node may not transmit  $R_b$  successfully owing to cumulative interference producing by other simultaneously transmitting nodes. So the solution adopted the above assumption is the low bound for  $t$ -spanner-SINR problem.

From the analysis of SINR-Spanner algorithm, the delay of constructing a  $t$ -spanner under SINR is mainly and inversely proportional to the number of nodes transmitting  $R_b$  successfully in one time slot. Hence, the approximation ratio of the algorithm SINR-Spanner is

$$\begin{aligned} & \frac{S}{\pi R_b^2} \cdot \left(1 - \frac{1}{\Delta_u^b}\right)^{\Delta_u^b-1} / \left\{ \frac{S}{\pi R_p^2} \cdot \left(1 - \frac{1}{\Delta_u^p}\right)^{\Delta_u^p-1} \right\} \\ &= \frac{R_p^2}{R_b^2} \left\{ \left(1 - \frac{1}{\Delta_u^b}\right)^{\Delta_u^b-1} / \left(1 - \frac{1}{\Delta_u^p}\right)^{\Delta_u^p-1} \right\} \\ &\leq \frac{R_p^2}{R_b^2} \cdot \frac{1}{2} / \frac{1}{e} = \frac{e}{2} \cdot \frac{R_p^2}{R_b^2}. \end{aligned} \quad (17)$$

The inequality holds owing to the following:  $\Delta_u^p > \Delta_u^b \geq 2$  for connectivity and  $(1 - (1/x))^{x-1}$  decreases with  $x$  increases when  $x \geq 2$ . When  $x$  is large enough, replacing  $x - 1$  by  $x$  does not cause much error and  $(1 - (1/x))^x \cong 1/e$ .

Since  $R_p$  is at about 2.57 to 6.34 times as  $R_b$  from Theorem 1 and Figure 3, the approximation ratio of SINR-Spanner is a constant.

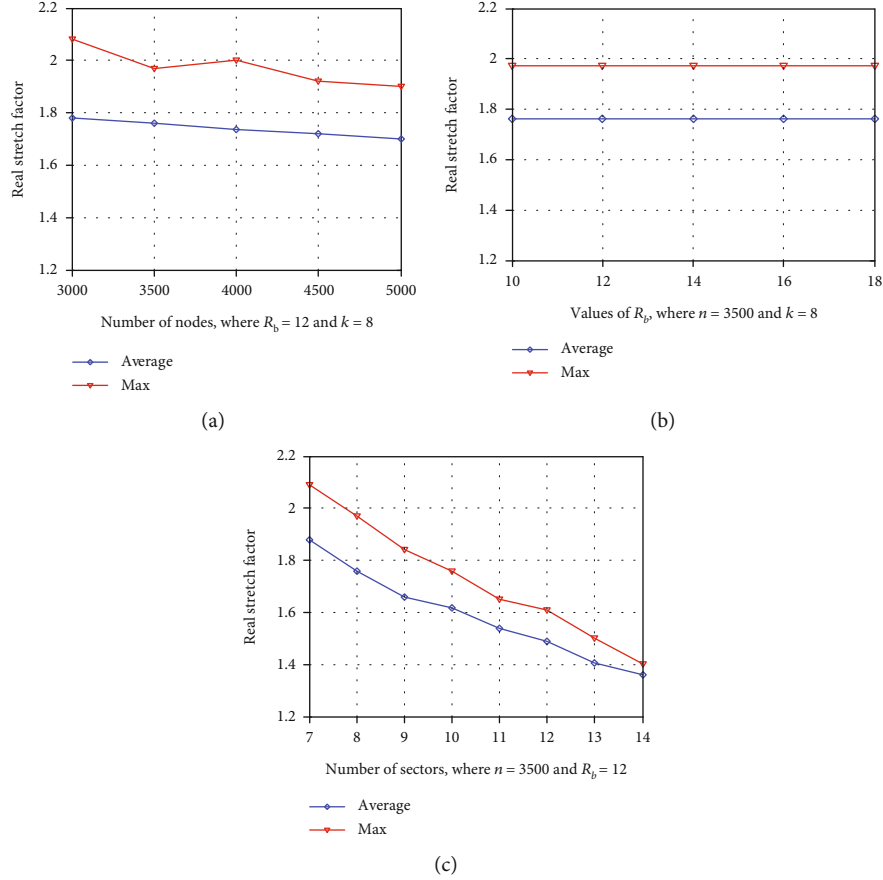
## 6. Simulation

In the previous section, we theoretically prove that the algorithm SINR-Spanner performs well in the worst cases and the resultant graph is the required spanner. In this section, we conduct simulations to investigate the average performance of our algorithm.

Our simulations are coded in the Sinalgo simulation framework [26], which is for testing and validating network algorithms and abstracts from the underlying layers. We consider a square area of 1000 by 1000 and deploy  $n$  nodes within this network region randomly and uniformly, where  $n \in \{3000, 3500, 4000, 4500, 5000\}$ . The local broadcasting range  $R_b$  varies in  $\{10, 12, 14, 16, 18\}$ . The ambient noise  $N = 5 \times 10^{-8}$  mW. Figure 3 has given the ranges of the path loss exponent  $\alpha$ , the threshold  $\beta$ , and  $\varepsilon$ , and the relation between them and the proximity range  $R_p$ .  $R_p$  mainly affects the sending probability, which affects the delay of our

TABLE 1: The stretch factor  $t$  and the number of sectors  $k$  in theory.

$t$	7.6	4.3	3.2	2.7	2.3	2.1	2	1.9	1.8	1.7	1.6	1.5	1.4	1.3	1.2	1.1
$k$	7	8	9	10	11	12	13	14	15	16	17	19	22	28	38	70

FIGURE 6: Influences of  $n$ ,  $R_b$ , and  $k$  on the number of missing edges.

algorithm. After testing various values, no matter what values  $\alpha$ ,  $\beta$ , and  $\varepsilon$  have in the ranges, the variety of the performance and the delay in our algorithm is similar. Therefore, we adopted  $\alpha = 5$ ,  $\beta = 4$ , and  $\varepsilon = 0.8$  in our following reported result. Accordingly, the transmission power  $P = N\beta \cdot (R_b/(1 - \varepsilon))^\alpha$  owing to the equation (2) and (3). The setting of simulation parameters refers to [9, 19]. With the proof of Theorem 8, we know that each node runs  $16\Delta^p + c$  rounds and the algorithm could get the required spanner with high probability. However, the way we adopted was that the algorithm terminates when the resultant graph does not change in 50 continuous timeslots in the simulation, i.e., in 50 continuous time slots no node can find a nearer neighbor within each sector. Over 100 runs of the simulations have been made for each reported average result.

Now, we first explore the stretch factor of the resultant graph (real stretch factor) in Figure 6. In (a), we analyze the influence of the number of nodes. The local broadcasting range was set to  $R_b = 12$ , and the number of sectors was set to  $k = 8$ . The maximum and average real stretch factor slightly reduced with the number of nodes increasing. In

(b), we investigate the impact of  $R_b$  with the number of nodes  $n = 3500$  and the number of sectors  $k = 8$ . The real stretch factor hardly changes with  $R_b$ . In (c), we analyze the influence of the number of sectors  $k$  with  $n = 3500$  and  $R_b = 12$ . The maximum and average real stretch factor decrease with  $k$  increases. When  $k \rightarrow \infty$ , the stretch factor approaches one. From all figures in Figure 6, it can be seen that both the maximum and average real stretch factor is much smaller than the theory value in Table 1 with the same  $k$ . Hence, given the required  $t$ , we can choose a smaller  $k$  according to practical experience. In summary, the stretch performance of the algorithm SINR-Spanner is better than expected.

Due to randomization of SINR-Spanner, the constructed graphs may not be perfect  $YG_k^{R_b}$ ; for example, the connection link to the nearest neighbor in a sector might be missing. But the algorithm performance is guaranteed with high probability, i.e., the probability for all  $n$  nodes transmitting  $R_b$  successfully and all edges in  $YG_k^{R_b}$  being reserved is bounded by  $1 - e^{-n/4}$ . To verify this, we evaluate the number of missing edges in the resultant graph from the corresponding perfect



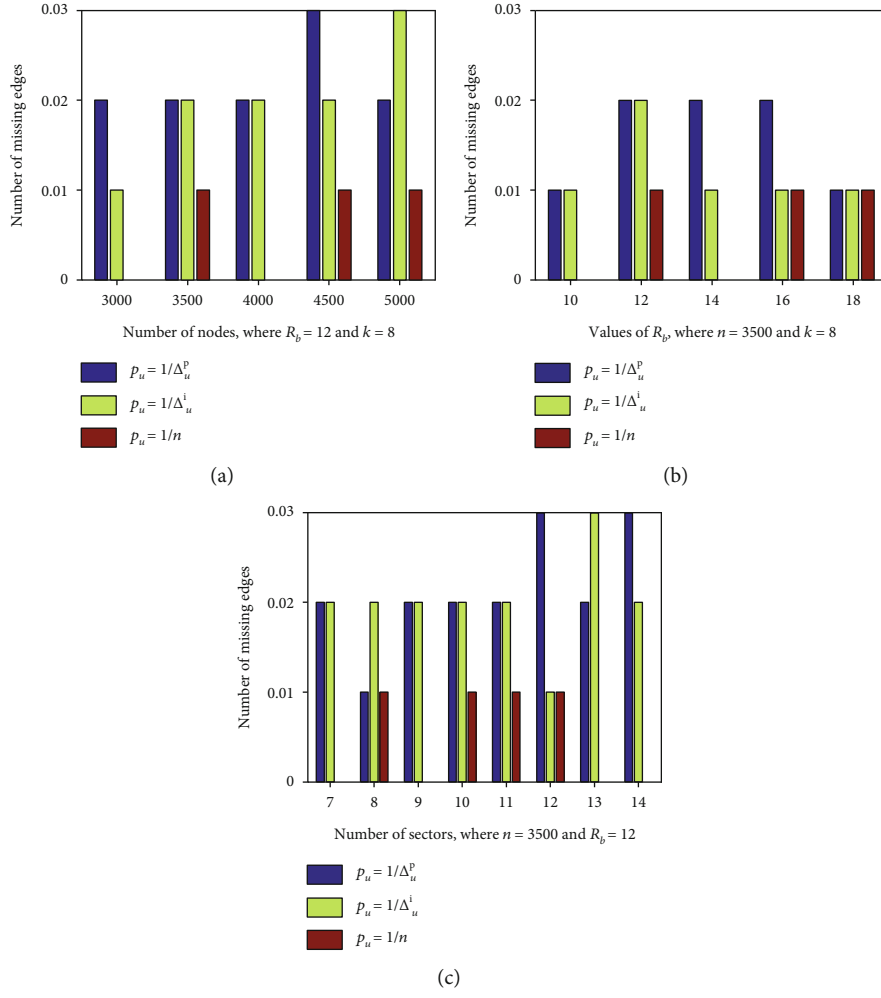


FIGURE 7: Influences of  $n$ ,  $R_b$ , and  $k$  on the number of missing edges.

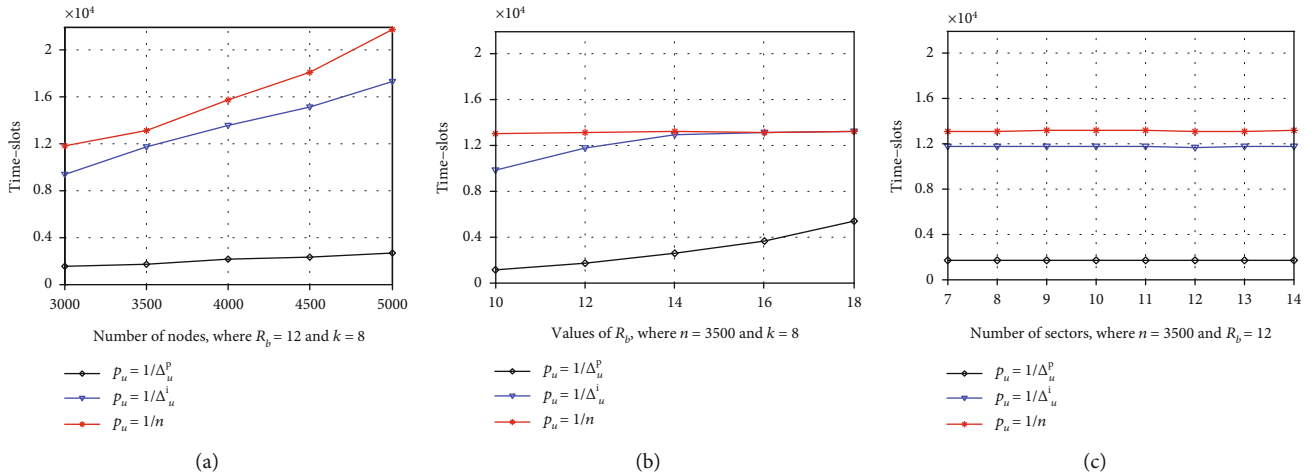


FIGURE 8: Influences of  $n$ ,  $R_b$ , and  $k$  on the delay.

$YG_k^{R_b}$  in Figure 7. With a different number of nodes, different values of  $R_b$ , and different number of sectors, we compare the number of missing edges in three sending probability cases

including  $1/n$ ,  $1/\Delta_u^p$  (SINR-Spanner), and  $1/\Delta_u^l$  (the algorithm SINR-Undirected-YG in previous work [9]). When the sending probability is  $1/\Delta_u^p$ , the number of missing edges is a little

bit more than the other two cases; the reason is that the nodes transmitting at the same time are more and mutual interference is a little bigger. However, the number of missing edges in all three cases is no more than three in total 100 runs, though each run has no less than 3000 nodes and  $O(kn)$  edges. Simulations indicate that the similarity between the resultant graph and the corresponding  $YG_k^{R_b}$  with no-missing edges is close to 100% in all three cases.

We then consider the average delay needed by SINR-Spanner in Figure 8 from the influences of  $n$  in (a),  $R_b$  in (b), and  $k$  in (c), respectively. We still compare the results with three sending probability cases including  $1/n$ ,  $1/\Delta_u^p$  (SINR-Spanner), and  $1/\Delta_u^l$  (the algorithm SINR-Undirected-YG in previous work [9]). Whether the sending probability is  $1/n$ ,  $1/\Delta_u^p$ , or  $1/\Delta_u^l$  in (a), the delay grows with the number of nodes increasing. In (b), the delay increases with  $R_b$  increasing when the sending probability is  $1/\Delta_u^p$  and  $1/\Delta_u^l$ . However, when the sending probability is  $1/n$ , the delay does not change in (b) since it is only related to the number of nodes. In (c), the delay does not vary with  $k$  increasing. In summary, from Figure 8, the delay mainly changes with the change of the sending probability, while the sending probability of  $1/\Delta_u^p$  or  $1/\Delta_u^l$  mainly varies with  $n$  and  $R_b$ . Moreover, the average delay needed by the algorithm in [9] is close to the case where each node transmits with the probability  $1/n$ , and the average delay needed by SINR-Spanner is much smaller than that of previous work [9]. Finally, in theory,  $16\Delta^p + c$  is the delay upper bound of the algorithm SINR-Spanner from Theorem 8 and  $\Delta^p$  is the upper bound by  $n$ , while in the simulation, the delay is much smaller than  $16n + c$  and the algorithm can achieve reliable performance when the algorithm terminates when the resultant graph does not change in 50 continuous time slots.

## 7. Summary

In this paper, we present a randomized and distributed algorithm SINR-Spanner to solve the  $t$ -spanner-SINR problem using small delay in the IoT, which has the following characteristics: (1) being a distributed algorithm, (2) considering the SINR interference model, (3) applying the YG idea, and (4) theory and simulation guaranteed. In future research, the delay performance of the spanner construction algorithm under SINR may be able to be improved by adopting a smaller proximity region. Other methods for spanner construction except YG are also worthy of investigating.

## Data Availability

Our simulations are coded in the Sinalgo simulation framework [26], which is for testing and validating network algorithms and abstracts from the underlying layers. We consider a square area of 1000 by 1000 and deploy  $n$  nodes within this network region randomly and uniformly, where  $n \in \{3000, 3500, 4000, 4500, 5000\}$ .

## Conflicts of Interest

The author(s) declare(s) that they have no conflicts of interest.

## Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grants (12071478, 61972404) and the Natural Science Foundation of Shandong Province under Grants (ZR2019ZD10, F060505)

## References

- [1] Z. Cai and Z. He, "Trading private range counting over big IoT data," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 144–153, Dallas, TX, USA, 2019.
- [2] C. Luo, Y. Hong, D. Li, Y. Wang, W. Chen, and Q. Hu, "Maximizing network lifetime using coverage sets scheduling in wireless sensor networks," *Ad Hoc Networks*, vol. 98, article 102037, 2020.
- [3] X. Zhang and J. Yu, "Spanner construction for topology control in wireless networks," *Ruan Jian Xue Bao/Journal of Software*, vol. 26, no. 4, pp. 904–926, 2015.
- [4] G. Narasimhan and M. Smid, *Geometric Spanner Networks*, Cambridge University Press, New York, 2007.
- [5] R. Klein and M. Kutz, "Computing geometric minimum-dilation graphs is NP-hard," in *Graph Drawing. GD 2006*, M. Kaufmann and D. Wagner, Eds., vol. 4372 of Lecture Notes in Computer Science, pp. 196–207, Springer, Berlin, Heidelberg, 2006.
- [6] X. Li, P. Wan, and Y. Wang, "Power efficient and sparse spanner for wireless ad hoc networks," in *Proceedings Tenth International Conference on Computer Communications and Networks (Cat. No.01EX495)*, pp. 564–567, Scottsdale, AZ, USA, 2001.
- [7] P. Von Rickenbach, R. Wattenhofer, and A. Zöllinger, "Algorithmic models of interference in wireless ad hoc and sensor networks," *IEEE/ACM Transaction on Networking*, vol. 17, no. 1, pp. 172–185, 2009.
- [8] M. M. Halldórsson and T. Tonoyan, "Plain SINR is enough," in *Jul 2019 in Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing*, pp. 127–136, Toronto, Canada, 2019.
- [9] X. Zhang, J. Yu, W. Li, X. Cheng, D. Yu, and F. Zhao, "Localized algorithms for Yao graph-based spanner construction in wireless networks under SINR," *IEEE/ACM Transaction on Networking*, vol. 25, no. 4, pp. 2459–2472, 2017.
- [10] A. Yao, "On constructing minimum spanning trees in  $k$ -dimensional spaces and related problems," *SIAM Journal on Computing*, vol. 11, no. 4, pp. 721–736, 1982.
- [11] I. Althöfer, G. Das, D. Dobkin, D. Joseph, and J. Soares, "On sparse spanners of weighted graphs," *Discrete and Computational Geometry*, vol. 9, no. 1, pp. 81–100, 1993.
- [12] C. Scheideler, "Overlay networks for wireless ad hoc networks," in *Wireless Communications*, P. Agrawal, P. J. Fleming, L. Zhang, D. M. Andrews, and G. Yin, Eds., vol. 143 of The IMA Volumes in Mathematics and its Applications, pp. 237–258, Springer, New York, NY, 2010.
- [13] I. Kanj, "Geometric spanners: recent results and open directions," in *2013 Third International Conference on Communications and Information Technology (ICCIT)*, vol. 82, p. 78, Beirut, Lebanon, 2013.
- [14] K. Kothapalli, C. Scheideler, M. Onus, and A. W. Richa, "Constant density spanners for wireless ad-hoc networks," in

- Proceedings of the 17th annual ACM symposium on Parallelism in algorithms and architectures - SPAA'05*, pp. 116–125, Las Vegas, NV, USA, 2005.
- [15] E. Chlamtác and M. Dinitz, “Lowest-degree  $k$ -spanner: approximation and hardness,” *Theory of Computing*, vol. 12, no. 1, pp. 1–29, 2016.
  - [16] M. A. Abam and M. S. Qafari, “Geometric spanner games,” *Theoretical Computer Science*, vol. 795, pp. 398–407, 2019.
  - [17] P. Bose, R. Fagerberg, A. van Renssen, and S. Verdonschot, “On plane constrained bounded-degree spanners,” *Algorithmica*, vol. 81, no. 4, pp. 1392–1415, 2019.
  - [18] B. Huang, J. Yu, X. Cheng, H. Chen, and H. Liu, “SINR based shortest link scheduling with oblivious power control in wireless networks,” *Journal of Network and Computer Applications*, vol. 77, pp. 64–72, 2017.
  - [19] O. Goussevskaia, T. Moscibroda, and R. Wattenhofer, “Local broadcasting in the physical interference model,” in *Proceedings of the 5th International Workshop on Foundations of Mobile Computing (DialM-POMC'08)*, pp. 35–44, Toronto, Canada, 2008.
  - [20] D. Yu, Q. Hua, Y. Wang, H. Tan, and F. C. M. Lau, “Distributed multiple-message broadcast in wireless ad-hoc networks under the SINR model,” in *Structural Information and Communication Complexity. SIROCCO 2012*, G. Even and M. M. Halldórsson, Eds., vol. 7355 of Lecture Notes in Computer Science, pp. 111–122, Springer, Berlin, Heidelberg, 2012.
  - [21] T. Jurdzinski, D. R. Kowalski, M. Rozanski, and G. Stachowiak, “On setting-up asynchronous ad hoc wireless networks,” in *2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 2191–2199, Kowloon, Hong Kong, 2015.
  - [22] M. M. Halldórsson, Y. Wang, and D. Yu, “Leveraging multiple channels in ad hoc networks,” in *Proceedings of the 2015 ACM Symposium on Principles of Distributed Computing*, pp. 431–440, Donostia-San Sebastián, Spain, 2015.
  - [23] F. Fuchs and R. Prutkin, “Simple distributed  $\Delta + 1$  coloring in the SINR model,” in *Structural Information and Communication Complexity. SIROCCO 2015*, C. Scheideler, Ed., vol. 9439 of Lecture Notes in Computer Science, pp. 149–163, Springer, Cham, 2015.
  - [24] L. Fu, S. C. Liew, and J. Huang, “Effective carrier sensing in CSMA networks under cumulative interference,” in *2010 Proceedings IEEE INFOCOM*, pp. 1–9, San Diego, CA, USA, 2010.
  - [25] A. Blum, J. Hopcroft, and R. Kannan, *Foundations of Data Science*, Cambridge University Press, New York, 2020.
  - [26] Distributed Computing Group, ETH Zurich, “Sinalgo - simulator for network algorithms, version 0.75.3. 2008,” <http://sourceforge.net/projects/>.

## Research Article

# A Survey of Cooperative Jamming-Based Secure Transmission for Energy-Limited Systems

Yuandong Wu and Yan Huo 

*School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing, China*

Correspondence should be addressed to Yan Huo; [yhuo@bjtu.edu.cn](mailto:yhuo@bjtu.edu.cn)

Received 23 November 2020; Revised 25 December 2020; Accepted 7 January 2021; Published 15 January 2021

Academic Editor: Zhuojun Duan

Copyright © 2021 Yuandong Wu and Yan Huo. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Considering the ongoing development of various devices and rich applications in intelligent Internet of Things (IoT) systems, it is a crucial issue to solve secure transmission of legitimate signals for massive data sharing in the systems. Cooperative jamming-based physical layer security is explored to be a complement of conventional cryptographic schemes to protect private information. Yet, this method needs to solve a game between energy consumption and signal secure transmission. In this paper, we summarize the basics of cooperative jamming and universal security metrics. Using the metrics, we study a series of typical cooperative jamming strategies from two aspects, including power allocation and energy harvesting. Finally, we propose open issues and challenges of further works on cooperative jamming in an IoT system with energy constraints.

## 1. Introduction

The popularization of smart devices and corresponding applications in Internet of Things (IoT) systems, such as smart city, intelligent industry, and security surveillance, has penetrated modern life [1]. We heavily rely on these wireless smart devices for private information transmission. The rapid development of mobile computing prompts smart devices to receive wireless signals without restriction. Due to the broadcast nature of wireless channels, legitimate wireless signals are vulnerable to unauthorized receivers. Wiretap, caused by an eavesdropper, is a passive attack and does not interfere with legitimate transceivers. Though a legitimate receiver can receive untampered signals, the privacy leakage of these signals is unacceptable along with more attention to information security [2–4].

Multilayer-based mechanisms have been studied to increase the security and integrity of transmitted signals. These mechanisms, designed by traditional cryptography algorithms, are deployed in the high layers of the open system interconnection model [5–7]. However, the distribution

and management of secret keys between wireless devices remain a challenge for cryptography-based security mechanisms [8]. Moreover, low-end IoT devices with limited computing capability and hardware resources cannot adopt highly complex cryptographic approaches [9, 10]. These increase the probability to eavesdrop on legitimate signals. Therefore, we need to introduce complementary or alternative information security measures for IoT devices and applications. Physical layer security (PLS) was first presented in Wyner's wiretap channel [11] and then extended to a Gaussian degraded wiretap channel in [12] and a general nondegraded wiretap channel in [13]. These works are a vital foundation for the following studies.

PLS exploits physical inherent characteristics of wireless channels to guarantee information security regardless of eavesdropper computing capability. It can provide low-layer protection without compromising the existing cryptographic technique-based security protection. Signal processing techniques such as beamforming, precoding, and diversity approaches contribute to PLS. Besides, cooperative jamming, first proposed in [14], is a mainstream technology

of PLS, whose core idea is to hide legitimate signals within artificial noise (AN). Essentially, the inherent randomness of AN is used to stop eavesdropping to guarantee information security. At the same time, to avoid AN from interfering with legitimate receivers, it should be actively controlled.

Most cooperative jamming schemes interfere with eavesdroppers by AN while exploiting beamforming to cancel interference at destination nodes [15]. This idea should lead to much energy consumption. From the energy perspective, we should focus on not only secure performance but also energy efficiency for such security solutions due to massive deployed devices with low power and limited energy [16]. We summarize three reasons to illustrate why energy efficiency must be concerned in the cooperative jamming design. Firstly, IoT devices are usually designed as small, wireless portable electronics, whose batteries need to be recharged frequently. Next, batteries may pose huge safety risks in some deployments. Finally, it is not environment-friendly to dump billions of waste batteries.

Because energy constraints of low-end IoT devices hinder the application of cooperative jamming, recent works introduced an energy harvesting technology [17] and power allocation strategies to increase energy efficiency. However, there remain significant issues to realize efficient cooperative jamming with energy constraints. For example, current energy harvesting technologies only transfer small amounts of dynamic and unpredictable power for a small wireless device. Thus, in this paper, we need to survey numerous studies of cooperative jamming strategies with energy constraints. Our contributions are as follows.

- (i) We formulate a general cooperative jamming model and present main metrics to measure security levels of signal transmission
- (ii) We systematically review cooperative jamming strategies for limited energy scenarios in terms of optimal power allocation and wireless-powered methods
- (iii) We raise a series of interesting open issues that need to be studied in depth to improve secure energy efficiency for physical layer security

The survey is organized as follows. Section 2 provides a general cooperative jamming model and the corresponding security performance metrics. Next, we present typical cooperative jamming schemes based on power allocation and energy harvesting to cope with energy constraints in a wireless transmission scenario in Section 3. We discuss a few interesting open research issues and the corresponding challenges in Section 4, and the conclusion of our survey will be given in Section 5.

## 2. Basics of Cooperative Jamming Schemes

In this section, we investigate a general cooperative jamming model and summarize typical secrecy metrics of cooperative jamming.

**2.1. A General Cooperative Jamming Model.** A typical wiretap model consists of a pair of transceivers (Alice and Bob) and an illegal passive eavesdropper (Eve) [18]. Eve intends to passively wiretap legitimate signals between transceivers. A traditional method is to broadcast encrypted signals to prevent Eve from wiretapping. However, the cryptographic method cannot satisfy security requirements of resource-constrained scenarios due to limited computational capabilities and insufficient energy. As a result, a physical layer-based solution provides additional protection via exploiting characteristic differences between a legitimate channel and a wiretapping channel.

A cooperative jamming scheme is a typical physical layer-based solution to broadcast artificial noise to block eavesdropping while not degrading the receiving performance of legitimate transceivers. The artificial noise is actively transmitted by the transceiver or a selected jammer, which is defined as self-cooperative jamming and non-self-cooperative jamming, shown in Figure 1. In essence, a transceiver in the self-cooperative jamming mode utilizes multiple antennas to transmit legitimate signals and artificial noise simultaneously while a friendly jammer in the non-self-cooperative jamming mode needs to optimize power allocation and design beamforming vectors to cover legitimate signals.

**2.2. Security Metrics.** Various metrics, i.e., bit error ratio of received signals, secrecy capacity, secrecy outage probability, and intercept probability, are considered to measure security performances of cooperative jamming schemes in different scenarios. We describe these metrics as follows.

**2.2.1. Bit Error Ratio (BER).** It is defined as a ratio of the number of error bits to the number of total transmitted bits in a certain period. It is used in the scenario where it only focuses on the decode error probability at receivers. BER of a receiver is affected by the signal energy per bit, the spectral density of interference and noise, channel fading parameters, and modulation methods. The received BER of an eavesdropper under BPSK modulation, for example, can be represented as follows:

$$p_e^{\text{BPSK}} = \mathcal{Q}\left(\sqrt{\frac{2|h_{\text{AE}}|^2 E_b}{N_0 + |h_{\text{JE}}|^2 N_J}}\right), \quad (1)$$

where  $h_{\text{AE}}$  and  $h_{\text{JE}}$  represent the channel states from Alice and Jammer to Eve, respectively.  $N_0$  is the spectral density of the Gaussian white noise, and  $N_J$  denotes the time-averaged spectral density of jamming signals.  $\mathcal{Q}(\cdot)$  is the complementary distribution function of the standard Gaussian and defined as  $\mathcal{Q}(x) = 1/\sqrt{2\pi} \int_x^{\infty} \exp(-t^2/2) dt$ .

**2.2.2. Secrecy Capacity (SC).** It is firstly proposed in [12] and can be defined as the maximum achievable perfect secrecy rate [19], i.e.,  $C_s = \sup_{p_e < \varepsilon} R_s$ , where  $p_e \triangleq \Pr(W \neq \hat{W})$  is the error probability of message  $W$  and  $\varepsilon > 0$  is a predefined error probability threshold for a given system. Here,  $W$  is the



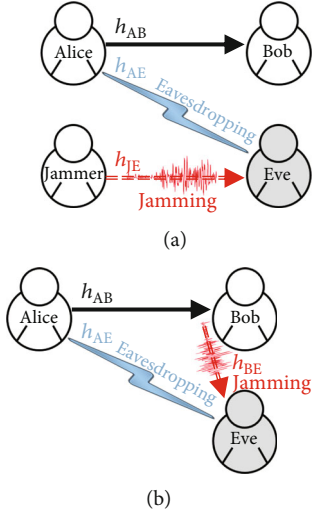


FIGURE 1: Cooperative jamming-based physical layer security.

original messages and  $\bar{W}$  represents the decoded messages at Bob.  $R_s \triangleq H(W)/n$  is the secrecy rate, and  $H(\cdot)$  denotes the entropy of the confidential messages. The secrecy capacity of the general wiretap channel is given by the following expression [20]:

$$C_s = \max_{p(u,x)} I(V; Y) - I(V; Z), \quad (2)$$

where  $I(V; Y)$  and  $I(V; Z)$  are the mutual information of an auxiliary random variable,  $V$ , and the received variable at Bob,  $Y$ , or the received variable at Eve,  $Z$ , when sending  $X$  at Alice, respectively. For a given channel, finding the secrecy capacity is equivalent to finding the joint distribution of  $V$  and  $X$ , i.e.,  $p(v, x)$ ,  $u \in U$ ,  $x \in X$ , which maximizes the difference in (2). As the result, the secrecy capacity for an average power constraint can be calculated as follows:

$$C_s = (C_Y - C_Z)^+ = \left( \frac{1}{2} \log_2(1 + \gamma_B) - \frac{1}{2} \log_2(1 + \gamma_E) \right)^+, \quad (3)$$

where  $\gamma_U$  is the signal-to-interference-plus-noise ratio of  $U \in \{\text{Bob}, \text{Eve}\}$ ,  $(x)^+$  represents  $\max(0, x)$ , and  $C_Y$  and  $C_Z$ , respectively, represent the channel capacities of the main and the wiretap channels. It is used when the state information of both legitimate channels and illegal channels is perfectly known. Note that Eve definitely intercept transmitted signals if the secrecy capacity is negative (i.e., the capacity of a legitimate channel falls below that of a wiretap channel). In this case, signal transmission from Alice to Bob should be insecure [21].

**2.2.3. Secrecy Sum Rate (SSR).** It is used to characterize the sum of the secrecy rate for  $n$  legitimate users when discussing the overall security requirements of a wireless system with several transmitters. It is a metric that optimizes the secrecy rate of the whole system rather than a specific legitimate

channel:

$$R_{\text{sum}} = \sum_{i=1}^n \mathbb{E} R_s^i. \quad (4)$$

**2.2.4. Secrecy Outage Probability (SOP).** The SOP metric is a probability that the instantaneous security capacity is less than a nonnegative target secrecy rate  $R_s$ . It is also named the outage probability of SC. Considering a fading channel with an eavesdropper, SOP is a mainstream metric to analyze secrecy performance [22]. The SOP metric is formulated as follows:

$$P_{\text{out}}(R_s) = \Pr(C_s < R_s). \quad (5)$$

**2.2.5. Connection Outage Probability (COP).** The COP is defined as the probability that the SINR of the legitimate channel falls below the transmission threshold  $\gamma^{\text{th}} = 2^{R_t} - 1$ , where  $R_t$  represents the transmission minimum target rate [23]. It can be expressed as follows:

$$P_{\text{CO}} = \Pr(\gamma_t < \gamma_t^{\text{th}}). \quad (6)$$

**2.2.6. Intercept Probability (IP).** This metric is to describe the probability of an intercept event if the SC falls below zero [24]. Intuitively, it is related to the statistical characteristics of a legitimate channel and a wiretap channel when jamming signals are invalid:

$$P_{\text{int}} = \Pr(C_Y < C_Z). \quad (7)$$

**2.2.7. Secrecy Energy Efficiency (SEE).** The concept of SEE,  $\eta_{\text{SEE}}$ , is defined as a ratio of the secrecy rate to the total power consumption, i.e., the number of securely transmitted bits per unit energy [25]. It is an important metric for a scenario that considers both secure transmission and energy efficiency. We can find an optimal equilibrium between the secrecy rate and the total energy consumption when maximizing this metric:

$$\eta_{\text{SEE}} = \frac{R_s}{P_{\text{tot}}}, \quad (8)$$

where  $P_{\text{tot}}$  is the total power consumption for the complete transmission.

**2.2.8. Secrecy Gap (SG).** The secrecy gap is the SNR difference between a legitimate receiver and an eavesdropper. It can be calculated by a tight bound of the maximal secrecy rate [26]:

$$\Delta\gamma = \gamma_B - \gamma_E. \quad (9)$$

**2.2.9. Worst-Case Secrecy Rate (WCSR).** It is defined as the minimum secrecy rate when there are  $K$  eavesdroppers in

an uncertain region [27], i.e.,

$$C_s = \left( C_Y - \max_{1 \leq k \leq K} C_Z^k \right)^+. \quad (10)$$

In addition, we use WCSR to optimize beamforming vectors, energy covariance at a transmitter, and AN covariance at a receiver, to minimize the legitimate channel capacity  $C_Y$  with power constraint [28],

$$C_s = \left( \min_{h \in \Omega_h} C_Y(h) - C_Z \right)^+, \quad (11)$$

where  $h$  represents the estimated signal fading coefficient affected by the optimized factors mentioned above and  $\Omega_h$  is the value range of  $h$ .

**2.2.10. Secrecy Throughput (ST).** This metric determines the average number of bits of confidential information received per unit time. We assume that the secrecy capacity is  $C_s$ , and a ratio of the transmission duration to the total time-slot is  $(1 - \alpha)$ ; then, the secrecy throughput is calculated as follows [29]:

$$\tau_s = (1 - \alpha)C_s. \quad (12)$$

**2.2.11. Power Consumption (PC).** It is a power constraint to secure signal transmission. We can compare system performance when satisfying the same security requirements. Lower power consumption means higher energy efficiency.

### 3. Cooperative Jamming in Energy-Constraint Scenarios

The stored energy in devices is the key factor to achieve secure signal transmission, especially in an energy-constraint wireless system. Enough energy can ensure the simultaneous transmission of legitimate signals and artificial noise. There are two perspectives to design secure communication strategies with energy constraints, including optimal power allocation and the efficient wireless-powered method. The former focuses on the reasonable utility of limited energy in one period while the latter is aimed at harvesting much energy from wireless environments to support energy consumption.

**3.1. Power Allocation-Based Cooperative Jamming Schemes.** Power allocation is one of the mainstream solutions to the optimization problem of cooperative jamming-based physical layer security in an energy-constraint scenario. The transmit power and jamming power are the main factors to affect secrecy performance and transmission efficiency when sending legitimate signals to a wireless network. An unreasonable power allocation scheme may cause much decoding errors at a legitimate receiver or low secure transmission performance. Therefore, it is important to design a feasible power allocation scheme to ensure the effectiveness and security of signal transmission.

The existing works to design optimal power allocation are based on two assumptions. The first one is that the global channel state information (CSI) is perfectly available to all legitimate nodes, and the second one is that the CSI of eavesdroppers in the given networks is imperfect. According to these assumptions, the authors in [30] first proposed a scheme to determine antenna weights and optimize transmit power for a relay communication scenario with limited total system power. Then, the authors in [31] further studied a secure transmission strategy for a multiantenna amplify-and-forward (AF) wireless network with one eavesdropper. Their strategy exploited artificial noise sent by the receiver to superimpose legitimate signal broadcast to the relay in the first phase and perfectly removed the noise via the self-interference cancellation (SIC) technology at the receiver when in the forwarding phase. Their investigation on jamming power allocation strategy depended on either the known perfect CSI or the known statistical CSI. Similarly, the authors in [32] presented a half jamming power scheme to achieve secure transmission for a two-hop relaying network with four nodes. They provided the optimal percentage of jamming power to minimize SOP under different SNR scenarios.

Although a relay can forward legitimate signals and emit AN to degrade the receiving quality of Eve [43–47], it still has potential secrecy threats for signal transmission. For one thing, numerous eavesdroppers may surround a relay to intercept forwarded signals. In this case, the authors in [48] exploited the relay as a pure cooperative jammer without signal forwarding. They optimized power allocation between information-bearing signals at the transmitter and the AN at the relay to cope with the decreasing SC caused by the correlation between eavesdropping channels and legitimate channels. For another, an untrusted relay may intercept and wiretap confidential signals when forwarding these signals. The work of [49] jointly optimized power allocation for all nodes in an untrusted two-way relay network to maximize SEE subject to power and SC constraints.

In Table 1, we summarize a list of feasible power allocation schemes to achieve cooperative jamming in energy-constraint scenarios. We notice that the known perfect CSI is essential to achieve secure communications through optimal power allocation.

**3.2. Wireless-Powered Cooperative Jamming.** Although power allocation strategies achieve the optimal secure transmission performance with energy constraints, it is difficult to further increase the SC or decrease SOP by using limited energy. Energy harvesting (EH) is a promising technology to recharge their batteries by converting solar, thermoelectric, or electromagnetic energy into electricity [50]. As this technology realizes the proactive energy replenishment of wireless devices, it has advantages to support further cooperative jamming and achieve a self-sustainable secure communication system [51].

Radio frequency-based energy harvesting (RF-EH) is a feasible method to help wireless devices acquire energy from ambient radio signals. A generalized RF-EH network consists of RF energy sources (e.g., Powercast or even TV Tower),

TABLE 1: An overview of power allocation-based cooperative jamming schemes.

References	Assumptions	Metrics	Contributions
[33]	Perfect CSI	SC	Propose a fast algorithm to obtain asymptotically optimal cooperative jamming.
[34]	Perfect CSI	SC	Improve the SC for a scenario with limited power and a fixed number of antennas.
[35]	Perfect CSI	SC	Prove that the optimal power allocation depends on the global CSI and optimize SC subject to power constraints.
[36]	Perfect CSI	SC	Study the secrecy performance of partial cooperative jamming for single and multiple data transmission scenarios.
[37]	Perfect CSI	SC	Analyze the impact of the distance and the number of eavesdroppers on the secrecy performance for different transmission patterns.
[38]	Unknown CSI	SC	Propose a robust scheme in an unknown CSI scenario and demonstrate the similar secrecy performance between unknown and known CSI.
[39]	Statistical CSI	SOP	Minimize the SOP problem to obtain the optimal power allocation.
[40]	Statistical CSI	SOP	Derive closed-form and asymptotic expressions of the SOP for a dual-hop underlay uplink CRN operating under Nakagami- $m$ fading channels.
[24]	Statistical CSI	IP	Propose a case study of physical layer security for a multiple relay scenario and evaluate the IP in Rayleigh fading environments.
[41]	Perfect CSI	SEE	Propose a beamforming scheme to maximize the SEE-based optimization problem in an underlay CRN cooperative jamming scenario.
[25]	Perfect CSI	SEE	Consider a joint source and relay power allocation scheme to maximize the system SEE.
[26]	Perfect CSI	SG	Demonstrate that a slightly reduced SC sharply decreases the received SNR of an eavesdropper.
[42]	Unknown CSI	WCSR	Optimize the flying trajectories and transmit power of unmanned aerial vehicles to improve the average WCSR of the system.

nodes (end users like sensors), and an information gateway (e.g., relay and base stations). The RF energy sources, whose spectrum to carry electromagnetic signals is from 3 kHz to 300 GHz, are the common infrastructures in daily lives. It attracts much attention as a viable solution to extend the lifetime of energy-constrained wireless networks. Though the fact that RF waves are available almost anywhere, the density in the environment is low. For example, the power density of Wi-Fi is only 1 mW/cm<sup>2</sup>. In addition, the efficiency of energy harvesting is inversely proportional to the signal propagation distance. As a result, it is much more efficient to exploit a dedicated source as well as multiple-antenna techniques to transfer energy [52, 53].

Simultaneous wireless information and power transfer (SWIPT) is an efficient technology to broadcast information and RF energy signals to communicate with information nodes and power energy receivers [54]. Different from traditional energy harvesting methods, SWIPT harvests dedicated RF energy rather than other environmental energy. Using alternative patterns of information transmission and energy transfer, it prolongs the lifetime for an energy-constrained system with hardware limitations. In particular, three modes are designed to implement SWIPT in a practical scenario, i.e., the time switching (TS) mode, the power splitting (PS) mode, and the antenna switching (AS) mode, which are intuitively compared in Figure 2. The first mode exploits an orthogonal time-slot to receive signals and energy alternately by periodical switching antennas between an EH receiver and an information decoder. The second one splits received signals into two individual streams with different power levels. Last, the

AS mode assigns a part of antennas for decoding signals while using the rest of the antennas to harvesting energy.

The SWIPT technology is usually used in a relay node to extend transmission ranges and provide additional services, e.g., cooperative jamming-based secure transmission. The relay node with SWIPT ensures legitimate signal forwarding and AN transmission via continuous energy replenishment. In particular, the existing works on SWIPT-based secure transmission include scenarios of static relay communications and unmanned aerial vehicle- (UAV-) enabled dynamic relay communications.

For static relay communications, the authors of [66] analyzed the impact of the number of antennas of the source, relay, and destination nodes on the secure performance of cooperative jamming for different multiantenna models. Then, the authors in [67] proposed an accumulate-then-transmit communication protocol. They employed a multi-antenna power beacon to establish a secure wireless link for energy-constrained sources. In [68], the authors studied an RF-EH power splitting technique for a multiuser multiple-input-single-output interference channel. They designed beamforming vectors and the power allocation strategy to minimize the total transmitted power subject to the quality of service requirements and energy constraints. Similarly, the authors in [69] employed power splitting to design a robust secure transmission scheme for a multiple-input-single-output channel to minimize the WCSR under transmit power constraints and additional worst-case EH constraints.

Yet, the above schemes are based on the half-duplex signal transmission that cannot receive and transmit signals

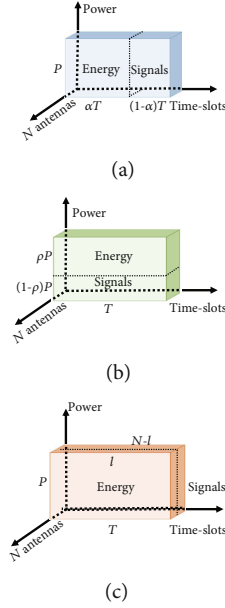


FIGURE 2: The typical SWIPT modes.

simultaneously. To improve energy efficiency, some studies proposed full-duplex-based cooperative jamming methods because a jammer can broadcast AN and harvest energy simultaneously. A three-part energy-constrained SWIPT system with full-duplex self-jamming was proposed in [70]. They apply the TS SWIPT technology at the destination to extend battery lifetime. The source transmits the energy-bearing signals to the destination using maximal ratio transmission (MRT) to increase harvested energy in the EH phase. Based on their analysis, they derived the closed-form expressions of SOP and ST and then provided the optimal duration allocation and the maximum ST. Coincidentally, a wireless-powered full-duplex jammer in a four-node system is introduced in [71]. The authors employed the accumulate-and-jam protocol and discussed the impact of antenna allocation at the jammer on secure performance. They believed that increasing the number of antennas used for energy harvesting can enhance security when a source sends legitimate signals with low power.

For dynamic relay communications, relay nodes are deployed based on physical layer characteristics, such as channel state information (CSI), received signal strength (RSS), channel phase response, and channel impulse response (CIR). In [72], the authors considered a novel scenario that has no direct link between transceivers due to heavy shadow fading. They employed an energy-constrained UAV-enabled mobile relay to receive information and harvest energy simultaneously. The UAV exploits PS and TS protocols while the full-duplex destination can simultaneously receive forwarded signals from UAV and transmit AN signals to confuse eavesdroppers without perfect CSI. Their scheme can achieve a significant improvement in the max-min SC compared to the benchmark schemes.

Table 2 lists wireless-powered cooperative jamming schemes for energy-constrained systems.

## 4. Open Issues and Challenges

In this section, we first discuss a few interesting open research issues and novel technologies to improve energy efficiency and then present challenges to be solved.

### 4.1. Open Research Issues

**4.1.1. The Optimal Friendly Jammer Selection.** The optimal jammer selection leads to the best secure performance (the maximal SC or the minimal SOP) with the same energy consumption. The optimal jammer performs better than the other candidate jammers under energy constraints. Therefore, optimal jammer selection is an effective method to improve energy efficiency. In [73], the authors considered a wireless network with multiple sources and multiple relay nodes. Each relay node is equipped with a rechargeable battery. A novel minimum bottleneck matching algorithm and a suboptimal relay selection algorithm are proposed for the group lifetime maximization policy. For an EH-enabled secondary system in cooperative cognitive radio-based IoT, the authors of [74] presented a Vickrey auction-based relay selection strategy. This strategy can select an SU from several EH-enabled candidate SUs as a relay node while the unselected SUs keep harvesting energy. Moreover, works of [75, 76] demonstrate that joint power allocation and relay selection schemes can obtain better secrecy performance than the conventional jamming power allocation. Based on the existing studies, we note that it is a fundamental issue to select the optimal relay and jammer from a set of candidate nodes to extend the lifetime and improve the energy efficiency of a secure transmission system.

**4.1.2. Intermittent Friendly Jamming.** The optimal design of friendly jamming schemes is the core issue to achieve the best secure transmission performance and energy efficiency. Traditional continuous friendly jamming schemes can maximize SC or minimize SOP under the given energy constraints. However, these algorithms may waste energy to broadcast AN even though there is no legitimate signal transmission. Thus, some researchers studied intermittent jamming schemes to cope with issues of low SEE. Different from continuous jamming, an intermittent jammer transmits jamming signals on demand [77, 78]. Despite energy constraints, we can exploit intermittent jamming to ensure secure transmission and energy efficiency for it utilizes the idle duration of legitimate signal transmission to keep sleeping and harvest energy to improve SEE. The intermittent jammer can theoretically strike a tradeoff between the jamming effectiveness and energy savings by appropriately adjusting durations of transmission and sleeping and, finally, increase the lifetime of devices in an energy-constraint IoT system.

Take an intermittent jamming strategy proposed in [79] as an example. Different from traditional continuous jamming strategies, the intermittent jamming strategy proposed in this article is aimed at increasing the system security by shortening the jamming time but strengthening the jamming power. They compared the BER of intermittent jamming strategies and continuous jamming strategies and developed



TABLE 2: An overview of energy-constrained wireless-powered cooperative jamming.

References	Scenarios/assumptions	Metrics	Contributions
[29]	PS-based full duplex jamming/imperfect CSI	ST	Prove that a PS-based scheme outperforms a TS-based scheme for a delay-tolerant transmission mode and performs better for delay-constrained transmission only in specific scenario.
[55]	SWIPT-based AF half-duplex relay/perfect CSI	SC	Maximize SC subject to transmit power constraints by optimizing the transmit beamforming matrix of an AF relay and the covariance matrix of AN.
[56]	EH half-duplex relay/perfect CSI	SOP	Obtain a closed-form near-optimal TS ratio and the SOP exact expression for an EH-based jammer-assisted wireless sensor network.
[57]	SWIPT-based AF half-duplex relay/imperfect CSI	WCSR	Maximize WCSR by jointly optimizing the CB and the CJ covariance matrix along with the PS ratios for a relay with static power splitting and dynamic power splitting scenarios.
[58]	EH half-duplex jammer/imperfect CSI	ST	Achieve the best throughput subject to secrecy outage probability constraints by optimizing rate parameters.
[59]	SWIPT-based AF half-duplex relay/imperfect CSI	WCSR	Jointly optimize the AN covariance matrices at harvest-and-jam helpers and the AF relay beamforming matrix to maximize the WCSR.
[60]	SWIPT-based full-duplex relay/perfect CSI	SC	Study optimal power allocation in a secure OFDM-based SWIPT system with the help of a wireless-powered friendly jammer.
[61]	SWIPT-based full-duplex relay/imperfect CSI	PC	Prove that secure performance of the robust beamforming design is better than nonrobust ones for a practical multiradio wireless mesh network.
[62]	SWIPT-based full-duplex self-jamming/perfect CSI	COP, SOP, ST	Analyze COP, SOP, reliable-secure probability, and ST when multiple noncollusion eavesdroppers intercept confidential signals.
[63]	Half duplex destination-based-jamming SWIPT/imperfect CSI	SC	Design an AN-aided multicell coordinated beamforming scheme for SWIPT-enabled centralized and distributed manners by minimizing the total required power.
[64]	SWIPT-based AF half-duplex relay/imperfect CSI	SOP	Investigate the SOP for a TS-based SWIPT and destination-aided-jamming system with an untrustworthy AF relay.
[65]	EH full-duplex relay/imperfect CSI	SC and SOP	Propose a full-duplex jammer protocol whose key feature is that both relay and jammer are powered by source transmissions.

a new metric to jointly measure security requirements and energy cost, formulated an optimization problem with respect to the jamming duration proportion and jamming power, and examined the feasibility of intermittent jamming for different modulation methods. Accordingly, intermittent jamming is a feasible scheme to satisfy the requirements of secure performance and energy constraints. After solving the issues of when to jam and how to jam, it will surely become one of the practical cooperative jamming solutions.

*4.1.3. Unknown CSI of an Eavesdropper.* Almost all the existing cooperative jamming schemes are based on the assumptions of available perfect CSI or statistical CSI of all nodes in a wireless system. Yet, it is difficult to estimate the CSI of an eavesdropper perfectly especially when it is in the passive wiretapping mode. As a result, the performance with energy constraints in a practical scenario may be worse than its theoretical performance. Thus, the authors of [80] employed the space power synthesis technology to design a multijammer-based model to minimize synthetic jamming power at a legitimate receiver while satisfying predefined interference temperature in other locations. Although this scheme can securely transmit signals for an unknown CSI scenario within a fixed small area, multijammer-based cooperative jamming for a large-scale scenario may highly waste energy, which is difficult to achieve in an energy-limited system. As a result, future studies should consider how to design a cooperative

jamming scheme for an unknown CSI scenario with energy constraints.

#### *4.1.4. Cooperative Jamming for Intelligent Reflecting Surface.*

Intelligent reflecting surface (IRS) is a promising technology to engineer the radio signal propagation in wireless networks. IRS can dynamically alter a wireless channel to enhance communication performance via tuning massive reflecting elements. Different from the AF technology that uses energy to transmit signals, IRS only reflects signals by passive elements rather than generating new signals via a transmitter module. Thus, IRS adapts to an energy-constrained scenario well. In [81], the authors studied an IRS-assisted multiple-input-single-output system with cooperative jamming. They designed jamming beamforming matrices and the IRS phase-shift matrix to maximize energy efficiency. Considering the changeable CSI, the authors of [82] formulated a secure energy efficiency maximization problem subject to available power and the lowest rate constraints. Intuitively, IRS is envisioned to have abundant applications in future wireless networks. We need to consider issues such as how to integrate IRS into existing wireless systems, how to balance between signal transmission and energy consumption, and how many reflecting elements should be introduced.

*4.1.5. Polar Code-Based Secure Transmission.* The polar code has been regarded as a candidate technology for forward-



error-correction (FEC) in the 5G air interfaces due to its excellent encoding/decoding capability and high reliability. Because using the polar code is able to improve the reliability of legitimate signals, a friendly jammer can consume less energy to ensure the transmission. Therefore, we can guarantee secure transmission by an energy-limited friendly jammer. For a discrete memoryless multiple-access wiretap channel, the authors in [83] proved that any feasible rate pair is achievable under strong secrecy with a low-complexity polar coding scheme. In essence, the reason for using polar codes to ensure physical layer security is that polarization creates a series of independent linear deterministic multiple access channels. These channels make it possible to design a resolvability-based code and thus achieve strong secure transmission. In [84], the authors minimized the number of cooperative helpers to fulfill a feasible SC requirement. They employed Tal-Sharov-Vardy implementation of polar codes to implement secure polar coding for a two-user Gaussian wiretap channel. Note that many modules and applications of a digital wireless communication system have the polarization effect that can improve ST and the received signal quality. Thus, it is one of the urgent issues to jointly optimize physical layer technologies with polar codes of future wireless communications to achieve optimal transmission performance.

*4.2. Challenges of Future Works.* Although the existing works on cooperative jamming with energy constraints have made progress, there are still many challenges unsolved.

Firstly, the study in [40] proved that a friendly jammer cannot contribute to the enhancement of system security in the presence of an important number of eavesdroppers. The reason is that cooperative jamming is to ensure that the average legitimate channel state is better than the wiretap channel state. Yet, multiple eavesdroppers may collude to achieve a better wiretap channel than a legitimate channel. As a result, the number, location, power, and social attributes [85] of selected jammers should be appropriately designed to protect from collusion eavesdropping.

Next, most current studies focus on static system models. Yet, a practical scenario with mobile nodes, such as intelligent industry or smart home, causes a dynamic wireless channel [86], which leads to inaccurate prediction or even difficult to predict. This indicates that the assumption of a perfect/statistical channel state is unrealistic. In addition, a mobile scenario results in wireless-powered nodes without sufficient energy supply [87]. The Doppler shift causes the mismatch between a cooperative node and a receiver, which impacts the performance of cooperative jamming cancellation [88]. Thus, one crux to use cooperative jamming in a practical application is how to design secure transmission for legitimate signals using various characteristics of changeable wireless transmission scenarios.

Finally, recent works merely design the management of harvested energy but ignore feasible scheme design to decide when to switch a relay as a transceiver or to keep idle. Besides, researches on SWIPT-based remote communications remain vacant. The battery power may be insufficient due to low harvesting efficiency caused by long distances.

## 5. Conclusion

In this article, we investigate cooperative jamming schemes for physical layer security for an IoT system with energy constraints. Our work starts with the necessity of physical layer security and introduces the basic knowledge and security metrics of cooperative jamming. Next, considering limited energy scenarios, we discuss the typical security optimization strategies from two aspects of power allocation and energy harvesting. In essence, the power allocation-based secure transmission focuses on the effective utilization of device energy while the energy harvesting is aimed at employing external energy to recharge. We believe that a feasible cooperative jamming scheme should exploit these two methods to jointly optimize so as to deal with the bottleneck of energy shortage in an IoT system. Finally, we propose related open issues as well as challenges to study cooperative jamming with novel technologies in the future for an IoT system with limited energy.

## Data Availability

The data used to support the findings of this study are included within the article.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant 2019JBZ001, in part by the Beijing Natural Science Foundation under Grant 4202054, and in part by the National Natural Science Foundation of China under Grant 61871023 and Grant 61931001.

## References

- [1] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.
- [2] J. Mao, S. Zhu, X. Dai, Q. Lin, and J. Liu, "Watchdog: detecting ultrasonic-based inaudible voice attacks to smart home systems," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8025–8035, 2020.
- [3] X. Zheng, Z. Cai, and Y. Li, "Data linkage in smart internet of things systems: a consideration from a privacy perspective," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 55–61, 2018.
- [4] X. Zheng, Z. Cai, J. Yu, C. Wang, and Y. Li, "Follow but no track: Privacy preserved profile publishing in cyber-physical social systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1868–1878, 2017.
- [5] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2018.

- [6] Y. Jia, Y. Chen, X. Dong, P. Saxena, J. Mao, and Z. Liang, "Man-in-the-browser-cache: persisting HTTPS attacks via browser cache poisoning," *Computer & Security*, vol. 55, pp. 62–80, 2015.
- [7] Z. Cai and Z. He, "Trading private range counting over big iot data," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 144–153, Dallas, TX, USA, 2019.
- [8] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.
- [9] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial iots," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.
- [10] Y. Liang, Z. Cai, J. Yu, Q. Han, and Y. Li, "Deep learning based inference of private information using embedded sensors in smart devices," *IEEE Network*, vol. 32, no. 4, pp. 8–14, 2018.
- [11] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [12] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.
- [13] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.
- [14] R. Negi and S. Goel, "Secret communication using artificial noise," in *VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference*, pp. 1906–1910, Dallas, TX, USA, 2005.
- [15] M. Dehghan, D. L. Goeckel, M. Ghaderi, and Z. Ding, "Energy efficiency of cooperative jamming strategies in secure wireless networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 9, pp. 3025–3029, 2012.
- [16] Z. Cai and Q. Chen, "Latency-and-coverage aware data aggregation scheduling for multihop battery-free wireless networks," *IEEE Transactions on Wireless Communications*, 2020.
- [17] G. Zhang, J. Xu, Q. Wu, M. Cui, X. Li, and F. Lin, "Wireless powered cooperative jamming for secure ofdm system," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 2, pp. 1331–1346, 2018.
- [18] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming strategies for physical layer security," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 148–153, 2018.
- [19] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.
- [20] A. Yener and S. Ulukus, "Wireless physical-layer security: lessons learned from information theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814–1825, 2015.
- [21] Y. Zou, X. Wang, and W. Shen, "Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack," in *2013 IEEE International Conference on Communications (ICC)*, pp. 2183–2187, Budapest, Hungary, 2013.
- [22] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *2006 IEEE International Symposium on Information Theory*, pp. 356–360, Seattle, WA, USA, 2006.
- [23] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of csi feedback delays," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6259–6274, 2016.
- [24] Y. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42–48, 2015.
- [25] D. Wang, B. Bai, W. Chen, and Z. Han, "Achieving high energy efficiency and physical-layer security in AF relaying," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 740–752, 2016.
- [26] K. Fytrakis, N. Kolokotronis, K. Katsanos, and N. Kalouptsidis, "Optimal cooperative strategies for phy security maximization subject to SNR constraints," *IEEE Access*, vol. 8, pp. 119312–119323, 2020.
- [27] L. Tang and Q. Li, "Wireless power transfer and cooperative jamming for secrecy throughput maximization," *IEEE Wireless Communications Letters*, vol. 5, no. 5, pp. 556–559, 2016.
- [28] Z. Deng, Y. Gao, C. Cai, and W. Li, "Optimal transceiver design for swipt system with full-duplex receiver and energy-harvesting eavesdropper," *Physical Communication*, vol. 26, pp. 1–8, 2017.
- [29] R. Ma, H. Wu, J. Ou, S. Yang, and Y. Gao, "Power splitting-based SWIPT systems with full-duplex jamming," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9822–9836, 2020.
- [30] L. Dong, H. Zhu, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *2009 IEEE/SP 15th Workshop on Statistical Signal Processing*, pp. 417–420, Cardiff, UK, 2009.
- [31] K. Park, T. Wang, and M. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1741–1750, 2013.
- [32] Y. Choi and J. H. Lee, "Power allocation for cooperative jamming in amplify-and-forward relaying network with eavesdropper," in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, pp. 1–5, Glasgow, UK, 2015.
- [33] J. Yang, S. Salari, I. Kim, D. I. Kim, S. Kim, and K. Lim, "Asymptotically optimal cooperative jamming for physical layer security," *Journal of Communications and Networks*, vol. 18, no. 1, pp. 84–94, 2016.
- [34] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 5013–5022, 2011.
- [35] L. Dong, H. Yousefi'zadeh, and H. Jafarkhani, "Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper," in *2011 IEEE International Conference on Communications (ICC)*, pp. 1–5, Kyoto, Japan, 2011.
- [36] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4871–4884, 2011.
- [37] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, 2010.
- [38] P. Siyari, M. Krunz, and D. N. Nguyen, "Distributed power control in single-stream MIMO wiretap interference networks with full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 67, no. 3, pp. 594–608, 2019.
- [39] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: optimal power allocation and secrecy outage analysis,"

- IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7495–7505, 2017.
- [40] M. Bouabdellah, F. el Bouanani, and M.-S. Alouini, “A PHY layer security analysis of uplink cooperative jamming-based underlay CRNs with multi-eavesdroppers,” *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 2, pp. 704–717, 2020.
- [41] Y. Wen, T. Jing, Y. Huo, Z. Li, and Q. Gao, “Secrecy energy efficiency optimization for cooperative jamming in cognitive radio networks,” in *2018 International Conference on Computing, Networking and Communications (ICNC)*, pp. 795–799, Maui, HI, USA, 2018.
- [42] Y. Li, R. Zhang, J. Zhang, S. Gao, and L. Yang, “Cooperative jamming for secure UAV communications with partial eavesdropper information,” *IEEE Access*, vol. 7, pp. 94593–94603, 2019.
- [43] G. Zheng, L. Choo, and K. Wong, “Optimal cooperative jamming to enhance physical layer security using relays,” *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, 2011.
- [44] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff, “Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer,” *IEEE Transactions on Vehicular Technology*, vol. 64, no. 5, pp. 1833–1847, 2015.
- [45] L. Chen, S. Han, W. Meng, C. Li, and M. Berhane, “Power allocation for single-stream dual-hop full-duplex decode-and-forward mimo relay,” *IEEE Communications Letters*, vol. 20, no. 4, pp. 740–743, 2016.
- [46] J. Li, A. P. Petropulu, and S. Weber, “On cooperative relaying schemes for wireless physical layer security,” *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4985–4997, 2011.
- [47] C. Yuan, X. Tao, N. Li, W. Ni, R. P. Liu, and P. Zhang, “Analysis on secrecy capacity of cooperative non-orthogonal multiple access with proactive jamming,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2682–2696, 2019.
- [48] S. Xu, S. Han, W. Meng, Z. Li, C. Li, and C. Zhang, “Improving secrecy for correlated main and wiretap channels using cooperative jamming,” *IEEE Access*, vol. 7, pp. 23788–23797, 2019.
- [49] D. Wang, B. Bai, W. Chen, and Z. Han, “Secure green communication via untrusted two-way relaying: a physical layer approach,” *IEEE Transactions on Communications*, vol. 64, no. 5, pp. 1861–1874, 2016.
- [50] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. M. Leung, and Y. L. Guan, “Wireless energy harvesting for the Internet of Things,” *IEEE Communications Magazine*, vol. 53, no. 6, pp. 102–108, 2015.
- [51] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, “Wireless networks with RF energy harvesting: a contemporary survey,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 757–789, 2015.
- [52] L.-G. Tran, H.-K. Cha, and W.-T. Park, “RF power harvesting: a review on designing methodologies and applications,” *Micro and Nano Systems Letters*, vol. 5, no. 1, pp. 1–14, 2017.
- [53] H. Chen, C. Zhai, Y. Li, and B. Vucetic, “Cooperative strategies for wireless-powered communications: an overview,” *IEEE Wireless Communications*, vol. 25, no. 4, pp. 112–119, 2018.
- [54] J. Huang, C.-C. Xing, and C. Wang, “Simultaneous wireless information and power transfer: technologies, applications, and research challenges,” *IEEE Communications Magazine*, vol. 55, no. 11, pp. 26–32, 2017.
- [55] H. Xing, Z. Chu, Z. Ding, and A. Nallanathan, “Harvest-and-jam: improving security for wireless energy harvesting cooperative networks,” in *2014 IEEE Global Communications Conference*, pp. 3145–3150, Austin, TX, USA, 2014.
- [56] G. Hu and Y. Cai, “Analysis and optimization of wireless-powered cooperative jamming for sensor network over Nakagami-m fading channels,” *IEEE Communications Letters*, vol. 23, no. 5, pp. 926–929, 2019.
- [57] H. Xing, K. Wong, A. Nallanathan, and R. Zhang, “Wireless powered cooperative jamming for secrecy multi-AF relaying networks,” *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 7971–7984, 2016.
- [58] W. Liu, X. Zhou, S. Durrani, and P. Popovski, “Secure communication with a wireless-powered friendly jammer,” *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 401–415, 2016.
- [59] H. Xing, K.-K. Wong, Z. Chu, and A. Nallanathan, “To harvest and jam: a paradigm of self-sustaining friendly jammers for secure AF relaying,” *IEEE Transactions on Signal Processing*, vol. 63, no. 24, pp. 6616–6631, 2015.
- [60] M. Liu and Y. Liu, “Power allocation for secure swipt systems with wireless-powered cooperative jamming,” *IEEE Communications Letters*, vol. 21, no. 6, pp. 1353–1356, 2017.
- [61] L. Li, X. Zhao, S. Geng, Y. Zhang, and L. Zhang, “Robust beamforming design for SWIPT-based multi-radio wireless mesh network with cooperative jamming,” *Information*, vol. 11, no. 3, p. 138, 2020.
- [62] X. X. Tang, W. Yang, Y. Cai, W. Yang, and Y. Huang, “Security of full-duplex jamming SWIPT system with multiple non-colluding eavesdroppers,” in *2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC)*, pp. 66–69, Macau, 2017.
- [63] Y. Lu, K. Xiong, P. Fan, Z. Zhong, and K. B. Letaief, “Coordinated beamforming with artificial noise for secure SWIPT under non-linear EH model: centralized and distributed designs,” *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1544–1563, 2018.
- [64] E. N. Egashira, E. E. B. Olivo, D. P. M. Osorio, and H. Alves, “Secrecy performance of untrustworthy AF relay networks using cooperative jamming and SWIPT,” in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1–6, Istanbul, Turkey, 2019.
- [65] Z. Mobini, M. Mohammadi, and C. Tellambura, “Wireless-powered full duplex relay and friendly jamming for secure cooperative communications,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 621–634, 2019.
- [66] K. Cao, B. Wang, H. Ding, and J. Tian, “Adaptive cooperative jamming for secure communication in energy harvesting relay networks,” *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1316–1319, 2019.
- [67] Y. Bi and A. Jamalipour, “Accumulate then transmit: toward secure wireless powered communication networks,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6301–6310, 2018.
- [68] S. Timotheou, I. Krikidis, G. Zheng, and B. Ottersten, “Beamforming for MISO interference channels with QoS and RF energy transfer,” *IEEE Transactions on Wireless Communications*, vol. 13, no. 5, pp. 2646–2658, 2014.
- [69] Q. Zhang, X. Huang, Q. Li, and J. Qin, “Cooperative jamming aided robust secure transmission for wireless information and



- power transfer in MISO channels,” *IEEE Transactions on Communications*, vol. 63, no. 3, pp. 906–915, 2015.
- [70] X. Tang, Y. Cai, Y. Deng, Y. Huang, W. Yang, and W. Yang, “Energy-constrained SWIPT networks: enhancing physical layer security with FD self-jamming,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 212–222, 2019.
- [71] Y. Bi and H. Chen, “Accumulate and jam: towards secure communication via a wireless-powered full-duplex jammer,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1538–1550, 2016.
- [72] W. Wang, X. Li, M. Zhang et al., “Energy-constrained UAV-assisted secure communications with position optimization and cooperative jamming,” *IEEE Transactions on Communications*, vol. 68, no. 7, pp. 4476–4489, 2020.
- [73] S. Gupta and R. Bose, “Energy-aware relay selection and power allocation for multiple-user cooperative networks,” in *2016 IEEE Wireless Communications and Networking Conference*, pp. 1–7, Doha, Qatar, 2016.
- [74] Y. Huo, M. Xu, X. Fan, and T. Jing, “A novel secure relay selection strategy for energy-harvesting-enabled internet of things,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, 18 pages, 2018.
- [75] Y. Choi and J. H. Lee, “A new cooperative jamming technique for a two-hop amplify-and-forward relay network with an eavesdropper,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 12447–12451, 2018.
- [76] D. Li, X. Zhang, and Y. Shang, “Joint physical network coding and destination aided cooperative jamming for secure wireless sensor networks,” in *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, pp. 1–5, Nanjing, China, 2016.
- [77] O. Besson, P. Stoica, and Y. Kamiya, “Direction finding in the presence of an intermittent interference,” *IEEE Transactions on Signal Processing*, vol. 50, no. 7, pp. 1554–1564, 2002.
- [78] Z. Cai, S. Ji, J. He, and A. G. Bourgeois, “Optimal distributed data collection for asynchronous cognitive radio networks,” in *2012 IEEE 32nd International Conference on Distributed Computing Systems*, pp. 245–254, Macau, China, 2012.
- [79] Q. Gao, Y. Huo, T. Jing, L. Ma, Y. Wen, and X. Xing, “An intermittent cooperative jamming strategy for securing energy-constrained networks,” *IEEE Transactions on Communications*, vol. 67, no. 11, pp. 7715–7726, 2019.
- [80] L. Huang, X. Fan, Y. Huo, C. Hu, Y. Tian, and J. Qian, “A novel cooperative jamming scheme for wireless social networks without known csi,” *IEEE Access*, vol. 5, pp. 26476–26486, 2017.
- [81] Q. Wang, F. Zhou, R. Q. Hu, and Y. Qian, “Energy-efficient beamforming and cooperative jamming in irs-assisted miso networks,” in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–7, Dublin, Ireland, 2020.
- [82] Q. Wu and R. Zhang, “Intelligent reflecting surface enhanced wireless network: joint active and passive beamforming design,” in *2018 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, Abu Dhabi, United Arab Emirates, 2018.
- [83] R. A. Chou and A. Yener, “Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming,” *IEEE Transactions on Information Theory*, vol. 64, no. 12, pp. 7903–7921, 2018.
- [84] M. Hajimomeni, K. Kim, H. Aghaeinia, and I.-M. Kim, “Cooperative jamming polar codes for multiple-access wiretap channels,” *IET Communications*, vol. 10, no. 4, pp. 407–415, 2016.
- [85] X. Zheng, Z. Cai, J. Li, and H. Gao, “Location-privacy-aware review publication mechanism for local business service systems,” in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, pp. 1–9, Atlanta, GA, USA, 2017.
- [86] W. Trappe, “The challenges facing physical layer security,” *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16–20, 2015.
- [87] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, “Security and privacy in smart city applications: challenges and solutions,” *IEEE Communications Magazine*, vol. 55, no. 1, pp. 122–129, 2017.
- [88] W. Guo, H. Zhao, W. Ma, C. Li, Z. Lu, and Y. Tang, “Effect of frequency offset on cooperative jamming cancellation in physical layer security,” in *2018 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–5, Abu Dhabi, United Arab Emirates, 2018.

## Research Article

# Emotional Dialogue Generation Based on Conditional Variational Autoencoder and Dual Emotion Framework

Zhenrong Deng,<sup>1</sup> Hongquan Lin,<sup>2</sup> Wenming Huang ,<sup>2</sup> Rushi Lan,<sup>3</sup> and Xiaonan Luo<sup>4</sup>

<sup>1</sup>Guangxi Key Laboratory of Image and Graphic Intelligent Processing, Guilin 541004, China

<sup>2</sup>School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004, China

<sup>3</sup>School of Computer Science & Engineering, South China University of Technology, Guangzhou 510006, China

<sup>4</sup>National and Local Joint Engineering Research Center of Satellite Navigation and Location Service, Guilin University of Electronic Technology, Guilin 541004, China

Correspondence should be addressed to Wenming Huang; 995456524@qq.com

Received 19 August 2020; Revised 2 November 2020; Accepted 5 December 2020; Published 28 December 2020

Academic Editor: Yaguang Lin

Copyright © 2020 Zhenrong Deng et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

An excellent dialogue system needs to not only generate rich and diverse logical responses but also meet the needs of users for emotional communication. However, despite much work, these two problems have not been solved. In this paper, we propose a model based on conditional variational autoencoder and dual emotion framework (CVAE-DE) to generate emotional responses. In our model, latent variables of the conditional variational autoencoder are adopted to promote the diversity of conversation. A dual emotion framework is adopted to control the explicit emotion of the response and prevent the conversation from generating emotion drift indicating that the emotion of the response is not related to the input sentence. A multiclass emotion classifier based on the Bidirectional Encoder Representations from Transformers (BERT) model is employed to obtain emotion labels, which promotes the accuracy of emotion recognition and emotion expression. A large number of experiments show that our model not only generates rich and diverse responses but also is emotionally coherent and controllable.

## 1. Introduction

With the development of privacy protection and incentive technology in the Internet of Things and mobile social networks driven by artificial intelligence, intelligent dialogue systems have entered our daily lives [1–4]. The enormous demands of privacy protection for dialogue systems have promoted the accuracy of speech recognition and semantic understanding, greatly improving the experience of human-machine dialogue. At the same time, people have put forward increasing requirements for intelligent dialogue systems to produce more human-like dialogues. As an important part of human intelligence, emotional intelligence is defined as the ability to perceive, integrate, understand, and regulate emotions [5]. Thus, machines will be able to communicate at the human level only when they have the ability to perceive and express emotions.

Currently, deep neural networks have been successfully applied in various applications [6–9]. In dialogue generation

tasks, the sequence to sequence (Seq2Seq) model [10] is a commonly used model. It is mainly based on the language ability learned from a large number of corpora to conduct dialogue and on the powerful calculation ability and abstraction ability to automatically summarize and extract valuable knowledge and features from massive data. In an open-domain dialogue system, there are multiple reasonable replies to a given query from a user. This phenomenon is called “one-to-many” diversity. However, for the dialogue system based on the Seq2Seq model and the maximum likelihood estimation (MLE) objective, the characteristics of the model determine the general utterance with a greater probability of its tendency to respond, such as “I don’t know” and “Yes.”

To generate more informative and meaningful responses, much work has been carried out in the open-domain dialogue [11–13]. These methods focus on the consistency of the conversation content rather than on emotion. Based on the past progress of dialogue systems, Zhou et al. [14] first integrated emotional factors into large-scale dialogue generation



using embedding of emotional tags, internal memory networks, and external memory networks. Subsequently, Asghar et al. [15] used emotion word embedding and emotion-based objective functions to improve performance. Zhou et al. [16] proposed to use the emoticon-rich Twitter corpus as a data set for emotional dialogue generation. However, the above work only considers the characteristics of target emotions and not the emotion of the input sentence, with the hope that the machine generates corresponding emotional responses; this will lead to the phenomenon of emotional drift, that is, the emotional response is incoherent and inconsistent with the emotion of the input sentence.

The generation of emotional dialogue needs to consider two main factors: one is the content of the generated response, and the other is the emotion of the generated response. In addition to avoiding the generation of a large number of general replies and increase the diversity of replies, it is necessary to consider the connection between the output emotion and the emotion of the user's input sentence, as well as the controllability of the output emotion. For example, if the user is sad, we can generate comforting words to make the user feel better.

The contributions of our work are summarized as follows:

- (1) We propose a dual-emotional framework for emotional dialogue generation, which comprehensively considers the impact of the emotion of the input sentence and the target emotion on emotional response in order to make our emotional response consistent with the user's emotion and ensure that the emotional response is controllable
- (2) We combine the conditional variational autoencoder [17] with the dual emotion framework to train an emotional generation system, and experiments prove that our model has strong performance
- (3) A multiclass emotion classifier based on the BERT [18] model is employed to obtain emotion labels, which improves the accuracy of emotion recognition and emotion expression.

The rest of the paper is organized as follows. In "Related Work," we outline the related work on emotional conversational agents. Then, we describe the proposed model in "Proposed Model." "Experiment" provides the experimental results. Finally, we summarize this article and propose directions for the future work in "Conclusion."

## 2. Related Work

With the popularity of social media, massive quantities of dialogue data can be accumulated and saved, allowing researchers to solve the problems of dialogue systems in a purely data-driven manner. Vinyals et al. [19] applied the Seq2Seq model in machine translation for dialogue generation for the first time, using an encoder to encode input sentences and generating a reply through a decoder. Bahdanau et al. [20] proposed an attention mechanism and applied it to the field of machine translation to improve the accuracy

of machine translation. Shang et al. [21] first built a corpus based on Sina Weibo and used a Seq2Seq model that introduced an attention mechanism to implement a single-round dialogue generation system.

Depending on the dialogue object and the dialogue scene, some work introduces latent variables, samples the distribution of latent variables, and then decodes the distribution to generate responses based on latent variables. Cao et al. [22] proposed a single-round dialogue generation model based on latent variables, including random variables  $z$  of the variational autoencoder in the decoder. Serban et al. [23] introduced the method of latent variables into a hierarchical dialogue model. The latent variables can be either topics or emotions. Zhao et al. [13] constructed a dialogue model based on a conditional variational autoencoder model using multiple semantic intentions as conditions.

Emotion perception is an indispensable part of a successful and intelligent dialogue system. Zhou et al. [14] proposed the emotional chat machine (ECM), which first focuses on how to generate a response with a specific emotion. ECM uses emotion embedding, internal memory network, and external memory network, but it considers neither the influence of the input sentence content on the decoder output nor the influence of the input sentence emotion on the emotional response. We believe that to learn higher-level dialogue skills and logic from a real corpus, a more elaborate mechanism is needed to capture the relationship between the utterance and emotional response. Therefore, we focus on the extraction and expression of the content and emotions of input sentences and produce more human-like emotional responses.

In terms of emotional dialogue research, [16] is most similar to our work, but they mainly focus on emotions in the Twitter corpus to train emotional chat robots, and their work did not further consider the emotional characteristics of the input sentences. Sun et al. [24] proposed a model that takes a sequence containing an emotion category of the input sentence and an emotion category of the output response as input. Xu et al. [25] proposed a dual-attention mechanism that pays attention to the content and emotion of input statements. Song et al. [26] proposed an emotion dialogue system that can express the desired emotion explicit or implicitly. Li et al. [27] used generative adversarial networks to generate emotional responses. Su et al. [28] proposed a stylistic dialogue generation system, which is achieved by adopting an information-guided reinforcement learning strategy.

## 3. Proposed Model

*3.1. Task Definition and Model Overview.* Our task is defined as follows: given a post  $x = (x_1, x_2, \dots, x_m)$ , input emotion label  $E_x$ , and target emotion label  $E_y$ , the goal is to generate a response  $y = (y_1, y_2, \dots, y_n)$ . The input emotion label  $E_x$  is obtained through the multiemotion classifier,  $x_i$  is the token of the input sentence, and  $y_i$  is the token of the output sentence. The response not only is consistent with the post in terms of both content and emotion but also corresponds to the target emotion.

An overview of CVAE-DE is given in Figure 1.  $E_y$  is the emotion label of the response,  $E_x$  is the emotion label of the post, vector  $v_y$  represents the text features of the response, vector  $v_x$  represents the text features and emotion features of the post, vector  $e_y$  represents the emotion features of the response, and vector  $c$  is obtained by concatenation of  $v_x$  and  $e_y$ . In the training process,  $E_x$  and  $E_y$  are obtained from the BERT emotion classifier, post  $x$  and  $E_x$  are encoded by the post encoder to obtain  $v_x$ ,  $E_y$  obtains vector  $e_y$  through a full connection network, and  $v_x$  is concatenated with  $e_y$  to obtain vector  $c$ . Then,  $c$  and  $v_y$  are fed to the prior/recognition network, and the hidden variable  $z$ , which is sampled from the recognition network, is fed to the decoder. In the inference process, the response does not exist,  $E_y$  is directly given by the user,  $z$  is sampled from the prior probability distribution  $p(z | c)$ , and we use an attention mechanism between the encoder and the decoder. Finally, the decoder will generate an emotional response that matches the post in content, is coherent with the post emotion, and corresponds to the target emotion based on attention memory, as well as  $c$  and  $z$ .

**3.2. Multiemotion Classifier Based on the BERT Model.** Most existing models use word2vec or Glove to obtain pretrained word vectors. However, the word vectors trained by these models are a type of static encoding. The same word is the same expression in different contexts, and it does not solve the problem of polysemy, in which words have different meanings in different contexts. In response to this problem, this paper trains a multiemotion classifier based on the BERT model [18]. BERT is a new language representation model that can not only obtain the rich grammatical and semantic features of the corpus text but also solve the problem of traditional language feature representation ignoring word polysemy, ultimately improving the accuracy of emotion classification. The structure of the BERT model is shown in Figure 2.

The most important part of the BERT model is the bidirectional Transformer encoder [29] encoding structure, which uses the encoder structure in the Transformer model as the feature extractor. The encoder is composed of a self-attention mechanism and a feed-forward neural network, abandoning the RNN's cyclic network structure [30], and completely uses an attention-based mechanism to model a segment of text. The attention mechanism in the encoder is called self-attention, and its core idea is to calculate the relationship between each word in a sentence and other words to adjust the importance of each word in order to obtain a context-related word vector. The encoder structure is shown in Figure 3.

In the experiments in this article, the pretrained Chinese model "BERT-Base, Chinese" released by Google is used to train our classifier; it uses a 12-layer Transformer with a hidden size of 768, a multihead attention parameter of 12, and a total model size of 110 MB. First, we load the pretrained model, and then, we use the emotion classification data set to fine-tune our model. Finally, the final model will be employed in the CVAE-DE model as our multiemotion classifier.

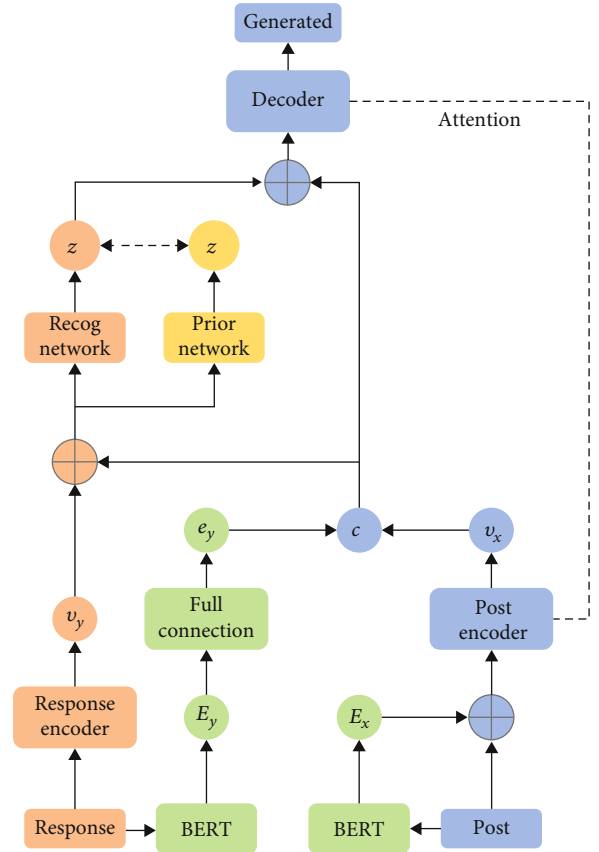


FIGURE 1: Overview of CVAE-DE. The blue part represents a Seq2Seq model based on the attention mechanism, which is the basis of our model. The orange and gold parts represent the conditional variational autoencoder model. The green part represents the dual emotion frame.

**3.3. Sequence to Sequence Model Based on the Attention Mechanism.** The basis of our model is a Seq2Seq model based on the attention mechanism [21]. The encoder and decoder of the model are implemented by GRU [31]. The role of the encoder is to map the post  $x = (x_1, x_2, \dots, x_m)$  to the hidden feature state  $h = (h_1, h_2, \dots, h_m)$ . For moment  $t$ ,  $h_t$  is defined as follows:

$$r_t = \delta(W_r x_t + U_r h_{t-1} + b_r), \quad (1)$$

$$z_t = \delta(W_z x_t + U_z h_{t-1} + b_z), \quad (2)$$

$$\tilde{h}_t = \tanh(W_h x_t + U_h (r_t * h_{t-1}) + b_h), \quad (3)$$

$$h_t = (1 - z_t)h_{t-1} + z_t \tilde{h}_t, \quad (4)$$

where the initial hidden state  $h_0$  is zero vector,  $r_t$  represents the reset gate,  $z_t$  represents the update gate,  $\delta$  is the sigmoid activation function, and  $W_r, W_z, W_h, U_r, U_z, U_h, b_r, b_z, b_h$  are training parameters. The sigmoid activation function can map the data to  $[0, 1]$  to determine the gating signal. The update door has two functions: the forgetting function and memory function. It can not only selectively forget the historical information that is not related to the original

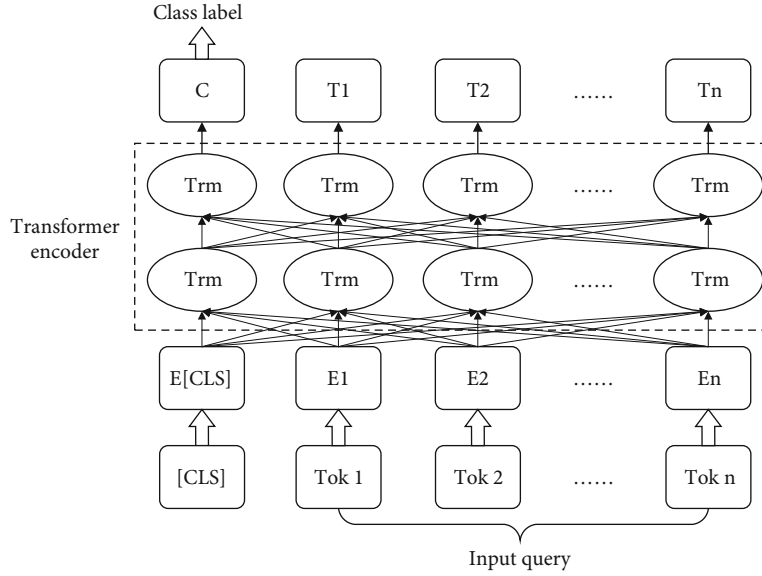


FIGURE 2: Fine-tuning BERT on emotion classification tasks.

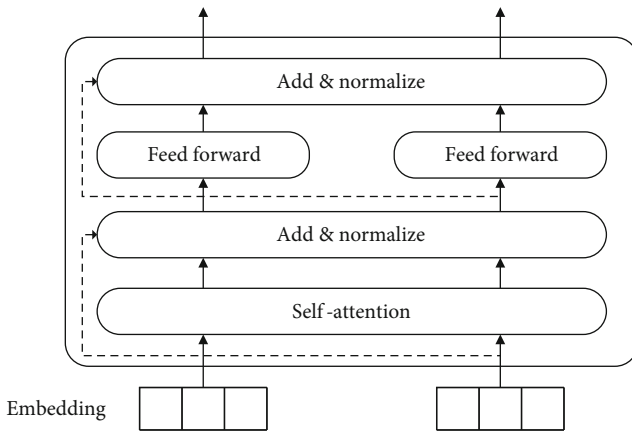


FIGURE 3: Transformer Encoder for feature extraction.

hidden state but also selectively remember the candidate hidden state and retain the long short-term information that is strongly dependent on the current moment. The above equations can be written as  $h_t = GRU(h_{t-1}, x_t)$ .

The current state of the decoder can be updated according to the state  $s_{t-1}$  at the previous time, the output  $y_{t-1}$  of the decoder at the previous time, and the context vector  $vc_t$  at the current time. The probability distribution of the words output by the decoder is

$$p(y_t | y_1, y_2, \dots, y_{t-1}, x) = g(y_{t-1}, s_t, vc_t), \quad (5)$$

$$s_t = GRU(s_{t-1}, [y_{t-1}, vc_t]), \quad (6)$$

where  $g$  is the maxout activation function, the context vector  $vc_t$  is the result of using the attention mechanism to weight

the encoder state sequence  $h$ , and typically, we use Bahdanau attention [20], which is defined as:

$$e_{tj} = v_a^T \tanh(W_a s_{t-1} + U_a h_j), \quad (7)$$

$$\alpha_{tj} = \frac{\exp(e_{tj})}{\sum_{k=1}^m \exp(e_{tk})}, \quad (8)$$

$$vc_t = \sum_{j=1}^m \alpha_{tj} h_j, \quad (9)$$

where  $v_a$ ,  $W_a$ , and  $U_a$  are the attention parameters that need to be learned. The attention mechanism is in fact a weighted sum of the hidden states of the encoder, which can dynamically capture the dependence of the decoder on the input utterance. The objective function of the Seq2Seq model based on the attention mechanism can be expressed as

$$p(y | x) = \prod_{t=1}^n p(y_t | y_1, y_2, \dots, y_{t-1}, vc_t). \quad (10)$$

**3.4. Conditional Variational Autoencoder Model.** The variational autoencoder (VAE) is a generative network structure based on the variational Bayesian inference proposed by Kingma et al. [32]. The VAE has been used to establish two probability density distribution models: one model, called the inference network, involves generating a variational probability distribution of hidden variables according to the variational inference of the original input data; and the other model, called the generation network, involves restoring the approximate probability distribution of the original data according to the generated variational probability distribution of hidden variables. In this model, a prior distribution  $p(z)$  is added to the hidden variable  $z$ , which often follows the standard Gaussian distribution, so that the model can generate samples that are closer to the original data

distribution. The goal of the variational autoencoder is to maximize the probability  $p(y)$  under the premise of sampling by  $z$ , which can be expressed as

$$p(y) = \int p(y|z)p(z)dz. \quad (11)$$

The VAE introduces a recognition model  $q_\phi(z|y)$  in the inference network to replace the undetermined true posterior distribution  $p_\theta(z|y)$ . To make  $q_\phi(z|y)$  approximately equal to  $p_\theta(z|y)$ , the VAE uses the  $KL$  divergence to measure the similarity between the two distributions and minimizes the  $KL$  divergence. In this case, the objective function of the model can be expressed as

$$L(\theta, \phi; y) = -KL(q_\phi(z|y)||p_\theta(z)) + \mathbb{E}_{q_\phi(z|y)}[\log p_\theta(z|y)], \quad (12)$$

where  $\phi$  is the parameter of the inferred network,  $\theta$  is the parameter of the generated network,  $KL(q_\phi(z|y)||p_\theta(z))$  indicates the  $KL$  divergence between the prior distribution  $p_\theta(z)$  of  $z$  and the posterior distribution  $q_\phi(z|y)$  of the model encoder, and  $\mathbb{E}_{q_\phi(z|y)}[\log p_\theta(y|z)]$  represents the reconstruction loss of the data samples by the decoder  $p_\theta(y|z)$ . The model's decoder learning goal is to restore the real data as much as possible, and the goal of the variational autoencoder becomes to maximize its objective function, which can be achieved by minimizing the first term on the right side of Equation (12), that is, making  $q_\phi(z|y)$  of the hidden variable  $z$  approximate  $p_\theta(z)$ .

The traditional VAE belongs to an unsupervised model. Although it can generate similar output data based on the input, it cannot control its orientation to generate specific types of data. For this purpose, Makhzani et al. [17] proposed a conditional variational autoencoder (CVAE) model. Based on the Seq2Seq model, we introduce the latent variable  $z$  in the CVAE model. For a given input utterance, multiple appropriate responses may exist, and each response corresponds to a potential variable configuration that does not appear in the input utterance. CVAE is trained by maximizing the conditional likelihood variational lower bound of  $y$  for a given  $c$  situation.

$$p(y|c) = \int p(y|z,c)p(z|c)dz. \quad (13)$$

In our model, the decoder is used to approximate  $p_D(y|z,c)$ , the prior network is used to approximate  $p_P(z|c)$ , and the recognition network is used to approximate the real posterior  $p_R(z|y,c)$ .  $\theta_D$ ,  $\theta_P$ , and  $\theta_R$  are the parameters of their networks. The objective function is given by

$$L(\theta_D, \theta_P, \theta_R; y, c) = -KL(q_R(z|y,c)||p_P(z|c)) + \mathbb{E}_{q_R(z|y,c)}[\log p_D(y|z,c)]. \quad (14)$$

In addition, as described by Bowman et al. [33], it is

difficult to encode useful information in hidden variables by directly combining the RNN decoder and the variational autoencoder in the field of text generation. Because the RNN-based decoder is a general function approximator, which has a strong ability to model sequence information, it can learn the representation without hidden variables information in the decoding process. The hidden variables lose their function, and VAE mathematically degenerates into a simple Seq2Seq model. Therefore, training a Seq2Seq dialogue generation model based on CVAE needs to balance the reconstruction loss and  $KL$  loss. In our experiments, we use the techniques of  $KL$  annealing, early stop, and bag loss to balance the reconstruction loss and  $KL$  loss. The bag of words loss is added to the training objective function on the previous basis, and the objective function is rewritten as

$$L' = L + L_{bow}. \quad (15)$$

**3.5. Dual Emotion Framework.** To make the emotional responses more coherent, we add an emotion label of the post to the input of the post encoder. The input becomes  $[E_x; x]$ , enabling our model to mine the emotional information of the post and make the emotional response compatible with the post emotion. The estimated probability of the model can be rewritten as

$$p(y|E_x, x) = \prod_{t=1}^n p(y_t|y_1, y_2, \dots, y_{t-1}, E_x, x). \quad (16)$$

To make our emotional responses more human-like, we stitch the target emotion vector  $e_y$  into the vector  $c$  to control the emotion replied by decoder. The vector  $c$  becomes  $[e_y; v_x]$ . Thus, we can choose different emotions to reply to the users, and even affect the user's emotion. For example, when the user is unhappy, we can make the user happy by outputting a response with a happy emotion.

**3.6. Summary of the CVAE-DE Model.** In this section, we introduce the mathematical derivation and structural framework of the model. The goal of our model is to generate dialogue responses that are rich in content, diverse in form, and rich in emotion. To improve our model's ability to understand emotion and improve the accuracy of emotion recognition, we use the BERT model as the emotion classifier. At the same time, to prevent the Seq2Seq model from generating a large number of general responses, we introduce the hidden variables of the conditional variational autoencoder to enable our model to generate rich and diverse responses. Finally, to make the emotion contained in the responses more natural and appropriate, we design a dual emotion framework that considers not only the controllability of the output emotion but also the continuity of the emotion with the input sentence.

## 4. Experiment

**4.1. Data Preparation and Implementation Details.** We use different data sets to train the multiemotion classifier and



dialogue generation model. The multiemotion classifier is trained with the Weibo corpus data with emotion labels, which are derived from the Chinese Weibo emotion recognition task in NLPCC 2013 and the Chinese Weibo text emotion analysis task in NLPCC 2014. After sorting and filtering, the data set has a total of 40133 sentences, each of which contains an emotion label, which are divided into six categories: Null, Like, Sad, Disgust, Anger, and Happiness. The dialogue generation model is trained with the data set that is derived from the emotion dialogue generation task in NLPCC 2017. The data set contains 1119207 pieces of training data, each including an original sentence and a response sentence.

In the training of the multiemotion classifier, we divide the data set into a training set, a validation set, and a test set, with a ratio of 36133:2000:2000. We train the classifier on the basis of the pretrained Chinese model “BERT-Base, Chinese” released by Google.

In the training of the dialogue generation model, the ratio of the training set, validation set, and test set is 1099239:9984:9984. Our vocabulary size is set to 40000, the word embedding vector and the emotion label embedding vector are both set to 128, the encoder and decoder use 128 hidden units of RNN layer, and the latent variable size is set to 268. We randomly initialize all of the parameters of the model and set the batch size to 128.

**4.2. Baselines.** In the experiments, we compare CVAE-DE with the following baselines:

**Seq2Seq:** A standard Seq2Seq model with attention method that is widely used as a baseline in the conversation generation task [21].

**ECM:** A Seq2Seq model that uses the emotion category embeddings, internal and external memory mechanisms to generate emotional responses [14].

**CVAE:** A conditional variational autoencoder model that takes the target emotion label as input to formulate latent variable [16].

**CVAE-MTDA:** A conditional variational autoencoder model with a dual-attention mechanism used to ensure that specific emotional responses are coherent with the content and the emotion of the input [25].

**EDGAN:** A model based on generative adversarial networks with multiple generators for generating responses with specific emotion and a multiclass discriminator [27].

**4.3. Evaluation Indicators.** In this paper, we introduce the evaluation metrics for the following two aspects.

**4.3.1. Multiemotion Classifier.** Emotion classification accuracy is used as the evaluation index of the emotion classifier. For comparison, we train a variety of emotion classifiers, including RNN [30], LSTM [34], and Bi-LSTM [35].

**4.3.2. Dialogue Generation Model.** The evaluation indicators of the dialogue generation model are mainly divided into the categories of automatic evaluation and manual evaluation. Since there is no correct answer in the open-domain dialogue generation, the bilingual evaluation (BLUE) algorithm [36] is not suitable for the evaluation of the dialogue generation model [37]. Therefore, according to the perplexity

TABLE 1: Accuracy of emotion classifiers.

Model	Accuracy
RNN [30]	56.2%
LSTM [34]	59.7%
Bi-LSTM [35]	62.1%
BERT [18]	65.1%

TABLE 2: Objective evaluation with perplexity and accuracy.

Model	Perplexity	Accuracy
Seq2Seq [21]	67.2	0.205
ECM [14]	66.1	0.724
CVAE [16]	37.2	0.675
CVAE-MTDA [25]	34.6	0.692
EDGAN [27]	62.8	0.716
CVAE-DE	33.5	0.749

TABLE 3: Diversity scores for the CVAE-DE and the baselines. Distinct-1 and Distinct-2 are the ratios of distinct unigrams and bigrams in the generated responses.

Model	Distinct-1	Distinct-2
Seq2Seq [21]	0.0045	0.0353
ECM [14]	0.0062	0.0396
CVAE [16]	0.0256	0.2635
CVAE-MTDA [25]	0.0287	0.2712
EDGAN [27]	0.0273	0.2658
CVAE-DE	0.0308	0.2836
Target responses	0.0952	0.5897

TABLE 4: Manual evaluation of the generated responses in terms of content and emotion.

Model	Content	Emotion
Seq2Seq [21]	1.258	0.154
ECM [14]	1.286	0.422
CVAE [16]	1.302	0.392
CVAE-MTDA [25]	1.325	0.405
EDGAN [27]	1.314	0.416
CVAE-DE	1.337	0.437

[38], the accuracy of emotion expression, and the Distinct-1 and Distinct-2 methods [11], the responses generated by our model are automatically evaluated.

**Perplexity:** Defined by Eq. (17) where  $S$  is the generated sentence,  $L$  is the length of the sentence, and  $p(w_i)$  is the probability of the  $i$ -th word. A lower PPL score corresponds to a better model, more natural response, and smoother sentence.

$$PPL(S) = \sqrt[L]{\prod_{i=1}^L \frac{1}{p(w_i | w_1, w_2, \dots, w_{i-1})}}. \quad (17)$$



TABLE 5: Sample responses generated by CVAE-DE and other baseline models. For each input sequence, a generated example response is listed for each emotion category.

Post	Model	Response (original)	Response (translated)	
港澳游很好玩啊!	Seq2Seq [21]	哈哈, 是啊, 我也想去。	Haha, yeah, I want to go too.	
	Like	嗯, 我喜欢旅游。	Well, I like traveling.	
	Sad	唉, 可惜我去不了	Oh, it's a pity I cannot go.	
	ECM [14]	Disgust	我觉得太贵了。	I think it is too expensive.
	Angry	难道你们觉得好玩?	Do you guys find it fun?	
	Happy	哈哈, 太好笑了。	Haha, it's so fun.	
	Like	不错哦, 我也很想去, 我的兴趣就是去各地旅游!	Not bad, I also want to go, my hobby is to travel everywhere!	
Traveling in Hong Kong and Macau is fun!	Sad	很郁闷, 我还要加班, 只能等下次去马尔代夫了。	Very depressed, I have to work overtime and can only wait for the next time I go to the Maldives.	
	CVAE-DE	Disgust	这个旅游实在是无聊的, 还需要港澳通行证。	This tour is really boring and requires a Hong Kong and Macau pass.
	Angry	你们都不告诉我, 难道我是空气?	You do not tell me, am I the air?	
	Happy	哈哈, 收获很多, 太开心了。	Haha, I have gained a lot, so happy.	
	Seq2Seq [21]	哈哈, 是啊, 我也觉得。	Haha, yeah, I think too.	
	Like	我喜欢这个发型。	I like this hairstyle.	
	Sad	很郁闷, 我也觉得不好。	Very depressed, I also feel bad.	
你换发型了?	ECM [14]	Disgust	换发型很无聊啊!	Changing hair style is boring!
	Angry	我不喜欢理发。	I do not like haircuts.	
	Happy	哈哈, 剪了短发。	Haha, I cut my hair short.	
	Like	新发型是蛮爽的哦! 我就是喜欢这种风格!	The new hairstyle is pretty cool! I just like this style!	
	Sad	太恐怖了, 我只是想换, 但是没有勇气。	It's horrible, I just want to change, but I do not have the courage.	
	CVAE-DE	Disgust	无聊啊, 换了一个不喜欢的发型。	Bored, changed to a hairstyle that I do not like.
	Angry	难道你不喜欢我的发型?	Do not you like my hairstyle?	
Have you changed your hair style?	Happy	哈哈, 这个发型, 你会爱上我的。	Haha, with this hairstyle, you will fall in love with me.	
	Seq2Seq [21]	是啊, 下雨了。	Yes, it's raining	
	Like	我喜欢这种天气。	I like this weather.	
	Sad	估计会被淋湿的。	It is estimated that it will get wet.	
	ECM [14]	Disgust	下雨太难受了。	The rain is too uncomfortable.
	Angry	我还不能出门。	I cannot go out yet.	
	Happy	哈哈, 已经凉快了。	Haha, it's already cool.	
Is it raining in Shanghai?	Like	在上海, 天气预报不错, 下雨很凉快耶~	In Shanghai, the weather forecast is good, and the rain is very cool ~	
	Sad	可惜最近完全没有下雨, 是一个干旱的季节。	It is a pity that it has not rained at all recently, it is a dry season.	
	CVAE-DE	Disgust	是的, 上海的天气太热了!	Yes, the weather in Shanghai is too hot!
	Angry	没啊!我说过不会的, 你们不相信。	No! I said no, you do not believe it.	
	Happy	哈哈, 估计大暴雨就要来了。	Hahaha, it is estimated that the heavy rain is coming.	

Distinct-1 and Distinct-2: Used to judge whether the model will generate a large number of universal and repetitive responses, which can reflect the diversity of responses. The definition is given in Equation (18) where  $\text{Count}(\text{unique ngram})$  is the number of unigrams/bigrams that are not repeated in the responses and  $\text{Count}(\text{word})$  is the total number of unigrams/bigrams in the responses. A

larger value of Distinct-1 and Distinct-2 indicates a higher diversity of the generated responses.

$$\text{Distinct}(n) = \frac{\text{Count}(\text{unique ngram})}{\text{Count}(\text{word})}. \quad (18)$$

**Manual Evaluation:** To better understand the quality of the generated response in terms of content and emotion, we invite 4 volunteers to evaluate the results of our generation models. The reviewer scores of the generated response are based on content and emotion. The content scores are mainly based on whether the response is appropriate and natural or whether it may be generated by people; it is a widely accepted measurement standard by researchers and was proposed by Shang et al. [21]. The emotion scores are mainly based on whether the emotion of response meets the given target emotion. The content scores are divided into 0 point, 1 point, and 2 points. The emotion scores are divided into 0 point and 1 point.

**4.4. Experimental Results and Analysis.** (1) **Classification Accuracy of the Multiemotion Classifier:** As shown in Table 1, the classifier based on the BERT model has the highest accuracy, reaching 65.1%. The higher the accuracy of the emotion classifier is, the more accurate the emotion label is, and the higher the accuracy of the emotion expression. Therefore, we will use a classifier based on the BERT model to generate the emotion labels.

(2) **Perplexity and Accuracy of Emotion Expression:** As shown in Table 2, CVAE-DE obtains better score than all of the other models in perplexity and emotion expression accuracy. The best score in emotion expression accuracy indicates that the dual emotion framework can generate a response that is closer to the emotional response in the real human conversation corpus than the other models. The emotional responses of CVAE-DE model are not only controlled by the target emotion but also affected by the emotion of the input sentence. As communicated in real life, the responding party is not only controlled by their own emotion but also affected by the emotion expressed by the other party. The emotion accuracy of Seq2Seq is quite low because it generates the same response with different emotion types.

(3) **Distinct-1 and Distinct-2:** It is observed from Table 3 that the CVAE-DE model is far superior to the pure Seq2Seq model in response diversity. The CVAE-based models can enjoy the superiority of stochastic sampling from probabilistic latent variable, enabling them to generate various and meaningful responses, while pure Seq2Seq models tend to generate monotonous responses.

(4) **Manual Evaluation:** From the results shown in Table 4, CVAE-DE outperforms other models in content and emotion. This result indicates that CVAE-DE can generate high-quality emotional responses without sacrificing the grammatical correctness and logic of the content.

(5) **Case Study:** In Table 5, we show some example responses generated by CVAE-DE and other baselines. For a given post, there are a variety of proper responses with different emotion types. Intuitively, different people generate different emotion types for the same post.

It is observed that the CVAE-DE model generates emotional responses on every emotion type, while Seq2Seq with attention chooses a random emotion type for response. Compared with ECM, our model can produce responses with richer content, more diverse forms, and greater emo-

tional accuracy. When fed with different target emotions, the CVAE-DE model uses different emotional words to control expressions.

Although our model has achieved a relatively satisfactory performance compared to that of other models, there are still some limitations. Our model is mainly limited to some coarse-grained emotional labels, including like, sadness, and anger. Such coarse-grained classification labels make it difficult to capture the nuances of human emotion. Therefore, our future work direction may be to train our model to make it easier to capture the nuances of human emotions by building a corpus with fine-grained emotional labels.

## 5. Conclusion

In this paper, we propose an emotional dialogue generation model, CVAE-DE, to produce high-quality responses with multiple emotion types. An emotion classifier based on the BERT model is used to classify a variety of emotions, which to a certain extent improves the problem of previous methods obtaining a low classification accuracy of emotion categories. To enable the model to produce more rich and diverse responses, we introduce a conditional variable auto-encoder on the basis of the Seq2Seq model based on the attention mechanism. At the same time, to enable the model to generate coherent and controllable emotional responses, we propose a dual-emotional framework. The experimental results show that the model proposed in this paper can produce high-quality responses with specific emotions.

In future work, we will use more complex generation models to further improve the quality of generated responses and use a corpus with fine-grained emotion classification labels to enrich the emotion of responses. At the same time, we will also explore the application of the method in this article to multiple rounds of dialogue, using contextual information to infer the user's emotional information, rather than the emotional information specified by the user. This will be a challenging task because it depends on the topic, contextual information, and the user's emotions.

## Data Availability

We use different data sets to train the multiemotion classifier and dialogue generation model. The multiemotion classifier is trained with the Weibo corpus data with emotion labels, which are derived from the Chinese Weibo emotion recognition task in NLPCC 2013 and the Chinese Weibo text emotion analysis task in NLPCC 2014. After sorting and filtering, the data set has a total of 40133 sentences, each of which contains an emotion label, which are divided into six categories: Null, Like, Sad, Disgust, Anger, and Happiness. The dialogue generation model is trained with the data set that is derived from the emotion dialogue generation task in NLPCC 2017. The data set contains 1119207 pieces of training data, each including an original sentence and a response sentence. All researchers can access the data at the following site: [https://www.biendata.xyz/ccf\\_tcci2018/datasets](https://www.biendata.xyz/ccf_tcci2018/datasets).

## Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

## Acknowledgments

This work was partially supported by the National Natural Science Foundation of China (Nos. 6202780103, 61772149, 61762028, and U1701267), Guangxi Science and Technology Project (Nos. AB20238013, ZY20198016, 2019GXNSFFA245014), and Guangxi Key Laboratory of Image and Graphic Intelligent Processing Project (No. GIIP2003).

## References

- [1] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2018.
- [2] Y. Lin, Z. Cai, X. Wang, and F. Hao, "Incentive mechanisms for crowdblocking rumors in mobile social networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9220–9232, 2019.
- [3] Y. Lin, X. Wang, F. Hao et al., "Dynamic control of fraud information spreading in mobile social networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–14, 2019.
- [4] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cybe physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.
- [5] P. Salovey and J. Mayer, "What is emotional intelligence? Emotional development and emotional intelligence: implications for educators," *New York: Basic Books. Senge, PM (1998). Sharing Knowledge. Executive Excellence*, vol. 15, no. 6, pp. 11–12, 1997.
- [6] R. Lan, L. Sun, Z. Liu, H. Lu, C. Pang, and X. Luo, "Madnet: a fast and lightweight network for single-image super resolution," *IEEE Transactions on Cybernetics*, pp. 1–11, 2020.
- [7] B. Li, R. Liu, J. Cao, J. Zhang, Y.-K. Lai, and X. Liu, "Online low-rank representation learning for joint multi-subspace recovery and clustering," *IEEE Transactions on Image Processing*, vol. 27, no. 1, pp. 335–348, 2017.
- [8] Y. Wang, Y. Gao, Y. Li, and X. Tong, "A worker-selection incentive mechanism for optimizing platform-centric mobile crowdsourcing systems," *Computer Networks*, vol. 171, pp. 107–144, 2020.
- [9] R. Lan, Y. Zhou, Z. Liu, and X. Luo, "Prior knowledge-based probabilistic collaborative representation for visual recognition," *IEEE Transactions on Cybernetics*, vol. 50, no. 4, pp. 1498–1508, 2020.
- [10] I. Sutskever, O. Vinyals, and Q. V. Le, "Sequence to sequence learning with neural networks," in *Proceedings of the 27th International Conference on Neural Information Processing Systems*, vol. 2, pp. 3104–3112, Cambridge, MA, United States, 2014.
- [11] J. Li, M. Galley, C. Brockett, J. Gao, and B. Dolan, "A diversity-promoting objective function for neural conversation models," in *Proceedings of the 2016 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*, pp. 110–119, San Diego, California, 2016.
- [12] C. Xing, W. Wu, Y. Wu et al., "Topic aware neural response generation," in *Proceedings of the Thirty-First AAAI Conference on Artificial Intelligence*, pp. 3351–3357, San Francisco, California, USA, 2017.
- [13] T. Zhao, R. Zhao, and M. Eskenazi, "Learning discourse-level diversity for neural dialog models using conditional variational autoencoders," in *Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pp. 654–664, Vancouver, Canada, 2017.
- [14] H. Zhou, M. Huang, T. Zhang, X. Zhu, and B. Liu, "Emotional chatting machine: emotional conversation generation with internal and external memory," in *Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence*, pp. 730–739, New Orleans, Louisiana, USA, 2018.
- [15] N. Asghar, P. Poupart, J. Hoey, X. Jiang, and L. Mou, "Affective neural response generation," in *European Conference on Information Retrieval*, pp. 154–166, Springer, 2018.
- [16] X. Zhou and W. Y. Wang, "Mojitalk: Generating emotional responses at scale," in *Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pp. 1128–1137, Melbourne, Australia, 2018.
- [17] A. Makhzani, J. Shlens, N. Jaitly, I. Goodfellow, and B. Frey, "Adversarial autoencoders," 2015, <https://arxiv.org/abs/1511.05644>.
- [18] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "Bert: pre-training of deep bidirectional transformers for language understanding," in *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers)*, pp. 4171–4186, Minneapolis, Minnesota, 2019.
- [19] O. Vinyals and Q. Le, *A neural conversational model*, ICML Deep Learning Workshop, 2015.
- [20] D. Bahdanau, K. Cho, and Y. Bengio, "Neural machine translation by jointly learning to align and translate," in *3rd International Conference on Learning Representations, ICLR*, San Diego, USA, 2015.
- [21] L. Shang, Z. Lu, and H. Li, "Neural responding machine for short-text conversation," in *Proceedings of the 53rd Annual Meeting of the Association for Computational Linguistics and the 7th International Joint Conference on Natural Language Processing (Volume 1: Long Papers)*, pp. 1577–1586, Beijing, China, 2015.
- [22] K. Cao and S. Clark, "Latent variable dialogue models and their diversity," in *Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics: Volume 2, Short Papers*, pp. 182–187, Valencia, Spain, 2017.
- [23] I. V. Serban, A. Sordoni, Y. Bengio, A. Courville, and J. Pineau, "Building end-to-end dialogue systems using generative hierarchical neural network models," in *Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence*, pp. 3776–3783, Phoenix, Arizona, USA, 2016.
- [24] X. Sun, X. Peng, and S. Ding, "Emotional human-machine conversation generation based on long short-term memory," *Cognitive Computation*, vol. 10, no. 3, pp. 389–397, 2018.
- [25] W. Xu, X. Gu, and G. Chen, "Generating emotional controllable response based on multi-task and dual attention framework," *IEEE Access*, vol. 7, pp. 93734–93741, 2019.

- [26] Z. Song, X. Zheng, L. Liu, M. Xu, and X.-J. Huang, “Generating responses with a specific emotion in dialog,” in *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*, pp. 3685–3695, Florence, Italy, 2019.
- [27] Y. Li and B. Wu, “Emotional dialogue generation with generative adversarial networks,” in *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, vol. 1, pp. 868–873, Chongqing, China, 2020.
- [28] Y. Su, D. Cai, Y. Wang et al., “Stylistic dialogue generation via information-guided reinforcement learning strategy,” 2020, <https://arxiv.org/abs/2004.02202>.
- [29] A. Vaswani, N. Shazeer, N. Parmar et al., “Attention is all you need,” in *Proceedings of the 31st International Conference on Neural Information Processing Systems*, pp. 6000–6010, Red Hook, NY, United States, 2017.
- [30] T. Mikolov, M. Karafiát, and L. Burget, “Recurrent neural network based language model,” in *Eleventh Annual Conference of the International Speech Communication Association*, pp. 1045–1048, Makuhari, Chiba, Japan, 2010.
- [31] K. Cho, B. van Merriënboer, C. Gulcehre et al., “Learning phrase representations using rnn encoder–decoder for statistical machine translation,” in *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, pp. 1724–1734, Doha, Qatar, 2014.
- [32] D. P. Kingma and M. Welling, “Auto-encoding variational bayes,” in *International Conference on Learning Representations*, Banff, Canada, 2014.
- [33] S. Bowman, L. Vilnis, O. Vinyals, A. Dai, R. Jozefowicz, and S. Bengio, “Generating sentences from a continuous space,” in *Proceedings of the 20th SIGNLL Conference on Computational Natural Language Learning*, pp. 10–21, Berlin, Germany, 2016.
- [34] S. Hochreiter and J. Schmidhuber, “Long short-term memory,” *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.
- [35] A. Graves, S. Fernández, and J. Schmidhuber, “Bidirectional lstm networks for improved phoneme classification and recognition,” in *International Conference on Artificial Neural Networks*, pp. 799–804, Springer, 2005.
- [36] K. Papineni, S. Roukos, T. Ward, and W.-J. Zhu, “Bleu: a method for automatic evaluation of machine translation,” in *Proceedings of the 40th Annual Meeting of the Association for Computational Linguistics*, pp. 311–318, USA, 2002.
- [37] C.-W. Liu, R. Lowe, I. V. Serban, M. Noseworthy, L. Charlin, and J. Pineau, “How not to evaluate your dialogue system: an empirical study of unsupervised evaluation metrics for dialogue response generation,” in *Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing*, pp. 2122–2132, Austin, Texas, 2016.
- [38] Y. Bengio, R. Ducharme, P. Vincent, and C. Jauvin, “A neural probabilistic language model,” *Journal of Machine Learning Research*, vol. 3, pp. 1137–1155, 2003.



## Research Article

# Service Recommendation with High Accuracy and Diversity

Shengqi Wu <sup>1</sup>, Huaizhen Kou <sup>1</sup>, Chao Lv,<sup>2,3</sup> Wanli Huang <sup>1</sup>, Lianyong Qi,<sup>1,4</sup>  
and Hao Wang <sup>5</sup>

<sup>1</sup>School of Computer Science, Qufu Normal University, Rizhao, China

<sup>2</sup>China Telecom Smart Home Competence Center, China

<sup>3</sup>E-Surfing Smart Home Technology Co., Ltd., China

<sup>4</sup>State Key Laboratory for Novel Software Technology, Nanjing, China

<sup>5</sup>Department of Computer Science, Norwegian University of Science and Technology, Gjøvik, Norway

Correspondence should be addressed to Wanli Huang; wanlih1983@126.com and Hao Wang; hawa@ntnu.no

Received 4 August 2020; Revised 24 October 2020; Accepted 25 November 2020; Published 17 December 2020

Academic Editor: Yaguang Lin

Copyright © 2020 Shengqi Wu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In recent years, the number of web services grows explosively. With a large amount of information resources, it is difficult for users to quickly find the services they need. Thus, the design of an effective web service recommendation method has become the key factor to satisfy the requirements of users. However, traditional recommendation methods often tend to pay more attention to the accuracy of the results but ignore the diversity, which may lead to redundancy and overfitting, thus reducing the satisfaction of users. Considering these drawbacks, a novel method called DivMTID is proposed to improve the effectiveness by achieving accurate and diversified recommendations. First, we utilize users' historical scores of web services to explore the users' preferences. And we use the TF-IDF algorithm to calculate the weight vector of each web service. Second, we utilize cosine similarity to calculate the similarity between candidate web services and historical web services and we also forecast the ranking scores of candidate web services. At last, a diversification method is used to generate the top- $K$  recommended list for users. And through a case study, we show that DivMTID is an effective, accurate, and diversified web service recommendation method.

## 1. Introduction

In recent years, web services have developed rapidly and are playing an increasingly important role in E-commerce and virtual reality applications. With the increasing of Internet web services' numbers, people have more access to Internet information anytime and anywhere. However, people need to deal with a large amount of information resources, which makes it difficult for people to quickly find valuable services which they are interested in. In other words, the selection process is complicated in the age of big data [1–4]. Therefore, precise recommendation of web services is the key issue in service computing. As we all know, the recommender system has been widely used in many applications, such as <https://Amazon.com>, <https://TiVo.com>, and <https://Netflix.com> [5]. And web service recommendation is a process of actively

identifying suitable web services and recommending them to users. The most common method is traditional collaborative filtering [6].

As we all know, collaborative filtering usually explores users' preferences basing on users' historical usage records and then recommends the most appropriate service items to users automatically [7]. However, this method mainly focuses on improving the accuracy of recommendation, which may lead to the redundancy of services in a limited list of top- $K$  recommendations. Worse, the recommendation results may reduce users' satisfaction and are not conducive to exploring users' potential preferences for other services. For example, it is assumed that there is a certain service category with similar or related functions that match the interests of users and has better quality of services than other categories of services. Ordinary service recommendation



methods may only recommend this category of services to users in the final recommended list, but from users' points of view, recommendation services with similar functions are redundant, and this phenomenon is called overfitting. Accordingly, the recommender system should also pay attention to the diversity of service recommendations while ensuring a high accuracy of recommendation results. In this manner, other categories of services that users may be interested in can be included in the top- $K$  recommended list [3, 8].

Fortunately, diversification methods can not only avoid redundancy but also expand the range of users' choices, which is beneficial to avoid the uncertainty in the prediction of users' preferences [9]. However, there is a trade-off between accuracy and diversity [10] because high accuracy may often be obtained by safely recommending users the most popular and appropriate items, which can clearly lead to the reduction of diversity. And on the contrary, higher diversity can be achieved by trying to uncover and recommend highly idiosyncratic or personalized items with less data for each user, which will be more difficult to predict. And it may lead to the decrease of recommendation accuracy. Therefore, it is crucial for recommender systems to provide an optimal list of recommendations that takes into account both accuracy and diversity and to keep a balance between them [11–14]. This is also the main research direction of this paper. The main contributions of this paper are listed below:

- (i) A new web service recommendation method which pays attention to both accuracy and diversity is proposed
- (ii) Providing users with the list of top- $K$  service recommendations, our method improves the disadvantages of traditional service recommendation methods and effectively solves the problem of overfitting
- (iii) Our method weighs well the double indicators of accuracy and diversity in order to achieve the best recommendation effect and improve users' satisfaction

The remainder of this paper is organized as follows. Section 2 describes a scenario of web service recommendation, and based on that, the main motivation and research content of this paper are further described. Section 3 presents the framework and specific steps of the proposed web service recommendation method (named DivMTID). Section 4 introduces a case study, where a specific case is solved by DivMTID. Section 5 summarizes this paper, draws conclusions, and expounds future work.

## 2. Research Scenario and Motivation

In this section, the research scenario and motivation of this paper are described. All the work we have done is based on the research scenario and motivation.

*2.1. Research Scenario.* Here, we use Figure 1 to describe the research scenario in this paper. Suppose that a website has many different types of modules (entertainment, military, sports, life, finance, cars, games, films, shopping, etc.), and there are many different web services under each module. Assume that there are  $M$  web services used by a user under all modules, and they are recorded as  $WS_{u1}, WS_{u2}, \dots, WS_{uM}$ . For each module, they are recorded as  $WS_{u1}, WS_{u2}, \dots, WS_{ux}$  ( $x$  is a variable). Meanwhile, there are  $N$  candidate web services recorded as  $WS_1, WS_2, \dots, WS_N$  in the set of candidate services. And each web service is described by the Web Service Description Language (which is called the WSDL document). In order to describe it exhaustively, the symbols mentioned in this paper and their meanings are shown in Table 1.

*2.2. Motivation.* In this subsection, we utilize the example in Figure 2 to demonstrate the motivation of our proposal. It is assumed that the recommender system intends to recommend a list of web services to a user. In this condition, to recommend appropriate web services to the user, the similarity between historical web services and candidate web services should be calculated first. And then the system generates the top- $K$  recommended list to the user. However, in the process of similarity calculation and recommendation calculation, we will face the following challenges:

When calculating the similarity between historical web services and candidate web services, it is necessary to establish the relationship between historical records and the candidate service set. However, an effective method to predict the relative score of candidate service objects and filter the candidate web services is needed.

As the diversity of the recommended list is frequently neglected, the web services in the list may be similar to each other, which may lead to overfitting and failure to explore users' potential preferences and finally reduce the users' satisfaction.

Considering the above issues, a novel web service recommendation method named DivMTID is proposed, which will achieve the accuracy and diversity of recommendation results, and it will be presented in detail in the following sections.

## 3. A Diversified Service Recommendation Method Based on TF-IDF

Under the research scenario of Section 2, this paper proposes a new web service recommendation method named DivMTID, which is based on the TF-IDF algorithm. It utilizes cosine similarity and combines WSDL documents to calculate the ranking score of each candidate service and then uses the diversity algorithm to select the best web services from candidate services to set the top- $K$  service recommended list. Meanwhile, it takes into account the accuracy and diversity of recommendation results. Table 2 lists the basic framework of DivMTID, which includes four steps.

*3.1. Step 1: Explore Users' Preferences Approximately.* In step 1, we first make an approximate positioning of users'

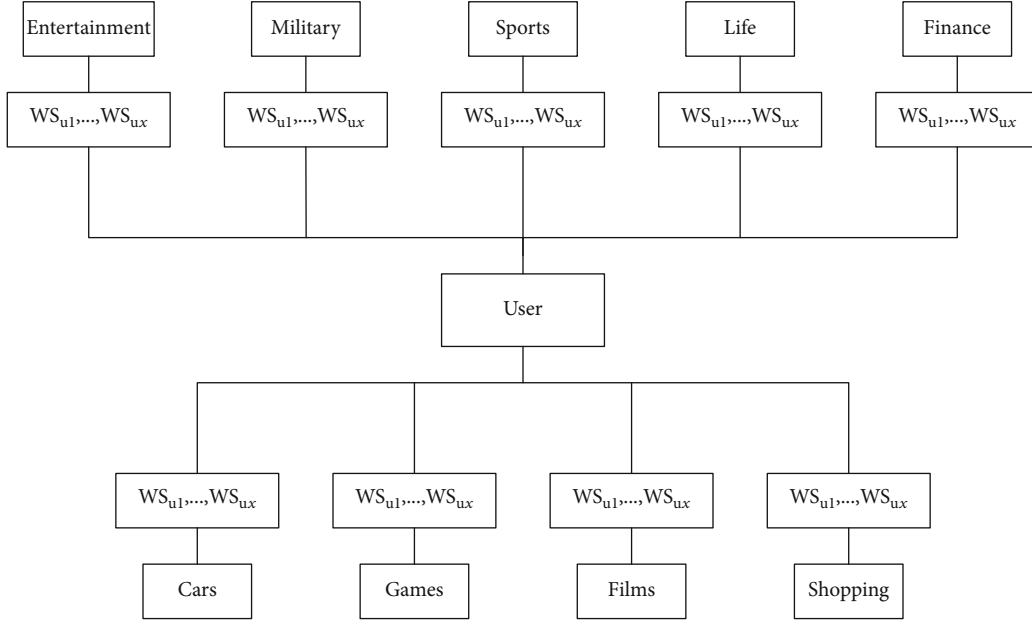


FIGURE 1: Research scenario.

TABLE 1: Symbols and their meanings.

Symbol	Meaning
$WS_{ui}$	Web service $i$ used in a user's history
$WS_j$	Candidate web service $j$
$WSDL_i$	The WSDL documentation of web service $i$
$M$	The number of web services used in a user's history
$N$	The number of candidate web services
$r_i$	A user's rating of web service $i$ used in history
$M_j$	Degree of a user's preference for module $j$
$a, b$	Threshold setting
$t_j$	The $j$ -th word in the corpus
$\omega$	The weight vector of web service
$\text{CosSim}_{i,j}$	The similarity level of web service $i$ and web service $j$
$\text{Score}_j$	The predicted ranking score of candidate web service $j$

preferences according to users' historical score records. In order to give more effectively personalized service recommendations, we need to figure out what users like and why they like it. In other words, using more effective preference representation methods may make recommendation algorithms exhibit higher performance. In most service recommendation methods, a user's score on web service can only represent the user's opinion on a service, but the user's preferences cannot be fully determined by a score record. However, a user's historical score records can be used to make an approximate positioning of the user's preferences. We can use the rating scores of web services to establish correlations with metadata and break the common limitation of expressing preferences with only one score.

For example, under the scenario described in Section 2, if a user rated 5 for all the web services under the module of military and rated 2 for all the web services under the module of finance, then the recommender system should infer that the user prefers the military module and should recommend more candidate web services about the military than finance.

We can establish the correlation between history scores and the information of the metadata module in equation (1), which utilizes score records for web services to calculate a user's preference degree for each module.

$$M_j = \frac{\sum_{i=r_{\min}}^{r_{\max}} (r_i \times n_{r_{\text{service-rated}}})}{n_{r_{\text{service-used}}}}. \quad (1)$$

In equation (1),  $M_j$  represents the degree of a user's preference for module  $j$ .  $r_i$  represents a user's historical rating scores for the used web services.  $n_{r_{\text{service-rated}}}$  represents the number of web services which rated  $r_i$  under the metadata module  $j$ , and  $n_{r_{\text{service-used}}}$  represents the number of all the used web services by the user under the metadata module  $j$ .

We can calculate the user's preference degree for the modules in equation (1) and make an approximate positioning of the user's preference. A threshold " $a$ " is set here, and the module with a calculated result greater than " $a$ " is defined as the user's preference module. For example, in the scenario of Section 2, we set a threshold 3. After calculation, if the modules with a result greater than 3 are military, finance, cars, and shopping, then the top- $K$  recommended list should mainly consist of web services under these modules, which means that the modules below the threshold are automatically filtered out. At last, we put all the web services belonging to the preference modules together to form a set  $P$ . The above is the content of step 1, its pseudocode can be described by Algorithm 1.

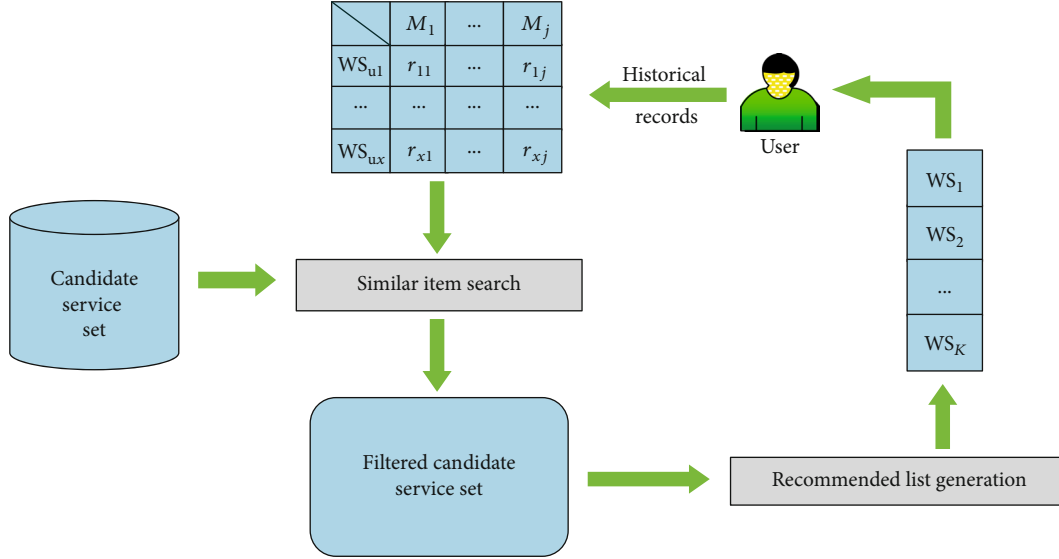


FIGURE 2: A motivating example.

TABLE 2: The basic framework of DivMTID.

<p>Step 1: explore users' preferences approximately</p> <p>By establishing the relationship between a user's history score records and the information of the metadata module, the preference degree of each module is calculated, and the user's preferences is approximately explored.</p> <p>Step 2: calculate TF-IDF weight vectors of web services</p> <p>Using the TF-IDF algorithm, the importance of words in the corpus to web services is calculated and finally represented by the TF-IDF weight vector in order to make a distinction among web services.</p> <p>Step 3: predict the ranking scores of candidate services</p> <p>The similarity between candidate web services and historically used web services is calculated by using cosine similarity, and the ranking score values of candidate web services are predicted.</p> <p>Step 4: create a diversified web service recommended list</p> <p>According to different index numbers, <math>K</math> different web services are selected to form multiple recommended lists. Then, it needs to calculate the list-diversity value of each list, and the list with the highest value becomes the web service recommended list that is finally recommended to the user.</p>
---

3.2. Step 2: Calculate TF-IDF Weight Vectors of Web Services. The task of step1 in DivMTID is to determine users' preferences, filtering out the web services under all modules with low history rating scores. It saves a lot of time for the subsequent recommendation algorithm to run. However, step 1 cannot exactly determine what kind of services users like, what characteristics the web services with high scores have, and how to select the best web services from so many candidate services. Step 2 is designed to solve these problems. It is assumed that step 1 filtered out  $L$  web services together.

As is mentioned, each web service in set  $P$  has a corresponding WSDL document, the same as candidate services. Then, all meaningful words in the WSDL documents of all services can form a corpus. After that, a well-known TF-

**Input:**

$WS_{u1}, WS_{u2}, \dots, WS_{uM}$ : web services used by a user.  
 $r_1, r_2, \dots, r_M$ : the rating scores.  
 $a$ : the threshold.

**Output:**

$P$ : a set.

```

1. for  $j = 1$  to  $g$  do // assume there are  $g$  modules
2.    $n_{r_{service-used}} = \text{count}(WS_{ui})$ 
3.   for  $r = r_{min}$  to  $r_{max}$  do
4.      $n_{r_{service-rated}} = \text{count}(WS_{ui})$ 
5.      $n_{r_{service-rated}} * r$ 
6.   end for
7.   Calculate  $M_j$  according to equation (1)
8.   if  $M_j \geq a$ 
9.     then add  $\{WS_{ui} \mid WS_{ui} \in j\}$  to  $P$ 
10.  end if
11. end for
12. return  $P$ 

```

ALGORITHM 1: Explore users' preferences approximately.

IDF algorithm [8, 15] is used to assess the importance of words in the corpus for each web service. The importance is proportional to the number of times that words appear in the document and inversely proportional to the frequency of words appearing in the corpus. The explanation is as follows.

$tf$  represents the word frequency, indicating the frequency of a word appearing in a WSDL document. It can be described in

$$tf(t_j, WSDL_i) = \frac{\text{freq}(t_j, WSDL_i)}{|WSDL_i|}. \quad (2)$$

$t_j$  represents the  $j$ -th word in the corpus and  $WSDL_i$  represents the WSDL document of the  $i$ -th web service.  $\text{Freq}(t_j,$

**Input:**  
 $WS_{u1}, WS_{u2}, \dots, WS_{u(M-L)}$ : web services in set P.  
 $WS_1, WS_2, \dots, WS_N$ : candidate web services.

**Output:**  
 $\omega_i$ : weight vectors of services in set P.  
 $\omega_j$ : weight vectors of candidate services.

1. Count ( $|WSDL_i|$ )
2. **for**  $i = u1$  to  $u(M-L)$  **do**
3.   **for**  $j = 1$  to  $nd$  //assume there are  $n$  words in the corpus
4.     **if**  $t_j \in WSDL_i$
5.       **then**  $\text{freq}(t_j, WSDL_i)$
6.        Count  $|WSDL_i|$
7.        Count  $|\{WSDL_i : t_j \in WSDL_i\}|$
8.        Calculate  $\omega_i$  according to equation (4)
9.     **end if**
10.   **end for**
11. **end for**
12.  $\omega_i = (\omega_{i1}, \omega_{i2}, \dots, \omega_{in})$
13. Calculate candidate services' TF-IDF weight vectors  $\omega_j$
14. **return**  $\omega_i, \omega_j$

ALGORITHM 2: Calculate TF-IDF weight vectors of web services.

$WSDL_i$ ) represents the number of times that  $t_j$  appears in the  $WSDL_i$  document, and  $|WSDL_i|$  represents the number of words that appear in the  $WSDL_i$  document. So we can also get the equation  $|WSDL_i| = \sum_j \text{freq}(t_j, WSDL_i)$ .

$\text{idf}$  represents the inverse document frequency. It is expressed by the ratio of the total number of all WSDL documents and the number of documents containing the word. We can calculate the logarithm of the quotient in

$$\text{idf}(t_j, WSDL_i) = \log_2 \frac{|WSDL|}{|\{WSDL_i : t_j \in WSDL_i\}|}. \quad (3)$$

$|WSDL|$  represents the total number of WSDL documents. And  $|\{WSDL_i : t_j \in WSDL_i\}|$  represents the total number of documents containing word  $t_j$ .

we use TF-IDF to assess the importance of words in a corpus for a web service. If a word appears with high frequency in a WSDL document of a web service and appears with low frequency in other WSDL documents of services, then we suppose that the word has a high importance and representativeness for this web service, which can be used to classify and distinguish different services.

Since WSDL documents are generally short, this paper chooses to give higher weight to the  $\text{idf}$  value to normalize the inherent bias with

$$\omega = \text{tf}(t_j, WSDL_i) * \text{idf}^2(t_j, WSDL_i). \quad (4)$$

The common way to implement TF-IDF is to give the same weight to word frequency and the inverse document frequency. However, this paper gives higher weight to  $\text{idf}$  in order not only to standardize the inherent deviation of the  $\text{tf}$  measurement in short documents but also to better exclude

**Input:**  
 $\omega_i, \omega_j$ : weight vectors of services.  
 $r_i$ : the rating scores.  
 $b$ : the threshold.

**Output:**  
 $Y$ : a set.

1. **for**  $j = 1$  to  $N$  **do**
2.   **for**  $i = 1$  to  $M-L$  **do**
3.     Calculate  $\text{CosSim}_{ij}$  according to equation (5)
4.      $r_i * \text{CosSim}_{ij}$
5.   **end for**
6.   Calculate  $\text{Score}_j$  according to equation (6)
7.   **if**  $\text{Score}_j > b$
8.     **then** add  $WS_j$  to  $Y$
9.   **end if**
10. **end for**
11. **return**  $Y$

ALGORITHM 3: Predict the ranking scores of candidate services.

the common words that frequently appear in web services in the corpus [16]. In this way, it can improve the classification and differentiation ability among web services and so improve the accuracy of a user's preferences.  $\omega$  represents the calculation result. It is the TF-IDF weight of word  $t_j$  to web services, which means the importance of word  $t_j$  for web services. Utilizing all the words in the corpus, we calculate the TF-IDF weight of a web service by equation (4) to form the weight vector of a certain web service. We candidate the TF-IDF weight vectors of all web services in the set P, denoted as  $\omega_i, i = u1, u2, \dots, u(M-L)$ . Similarly, for all candidate web services, their TF-IDF weight vectors are also calculated and denoted as  $\omega_j, j = 1, 2, \dots, N$ . The above is

<p><b>Input:</b>  <math>Y</math>: set <math>Y</math>.  <math>K</math>: the length of recommended list  <math>\text{CosSim}_{i,j}</math>: the similarity between service <math>i</math> and service <math>j</math>.</p> <p><b>Output:</b>  a diversified web service recommended list</p> <ol style="list-style-type: none"> <li>1. <math>f =  Y  // f</math> denotes the number of web services in the set <math>Y</math></li> <li>2. <math>\text{Sort}(Y)</math></li> <li>3. Create indexes for <math>f</math> web services</li> <li>4. <b>for</b> <math>j = 1</math> to <math>CK f \text{do} // K &lt; f</math></li> <li>5. Form a list with <math>K</math> web services according to different index numbers</li> <li>6. Calculate list-diversity according to equation (7)</li> <li>7. <b>end for</b></li> <li>8. <b>return</b> the list with the highest list-diversity value</li> </ol>
---

ALGORITHM 4: Create a diversified web service recommended list.

the content of step 2; its pseudocode can be described by Algorithm 2.

*3.3. Step 3: Predict the Ranking Scores of Candidate Services.* In order to evaluate the similarity between two web services, we use the TF-IDF weight vector of web services to calculate their cosine similarity [17] and define the similarity level between two web services as  $\text{CosSim}_{i,j}$ . The reason that we choose cosine similarity to measure the distance between different services is twofold: (1) cosine similarity is not limited to dimension volume; (2) cosine similarity has higher accuracy and is intuitive enough to describe the similarity calculation. The value of  $\text{CosSim}_{i,j}$  is calculated in

$$\text{CosSim}_{i,j} = \cos(\omega_i, \omega_j) = \frac{\omega_i \cdot \omega_j}{|\omega_i| \times |\omega_j|}. \quad (5)$$

In equation (5),  $|\omega_i|$  and  $|\omega_j|$  is the Euclidean length of the weight vector  $\omega_i$  and  $\omega_j$ . Besides,  $\omega_i \cdot \omega_j$  is their dot product. Cosine similarity can be used to effectively evaluate the similarity degree between two vectors, so we can also evaluate the similarity between two web services. After that, we calculate  $\text{CosSim}_{i,j}$  of candidate web services by combining each candidate web service and every web service in set  $P$  to get their value of cosine similarity in order.

We can get the similarity between the candidate web services and a user's history web services according to the value of  $\text{CosSim}_{i,j}$ , so that we can calculate the ranking score of each candidate web service (defined as  $\text{Score}_j$ ) in

$$\text{Score}_j = \lambda \sum_{i=1}^{M-L} r_i \times \text{CosSim}_{i,j}. \quad (6)$$

In equation (6),  $\lambda$  is the parameter and  $r_i$  is users' rating on history web services. The aim of multiplying users' rating and the value of  $\text{CosSim}_{i,j}$  is to give  $\text{CosSim}_{i,j}$  a different weight. After that, we carry on the accumulation, and we can obtain the ranking score of each candidate service. At last, we sort

TABLE 3: The user's history rating records.

	Entertainment	Military	Sports
Web <sub>u1</sub>	Null	2	4
Web <sub>u2</sub>	2	3	5
Web <sub>u3</sub>	Null	1	3
Web <sub>u4</sub>	3	2	5
Web <sub>u5</sub>	4	1	3
	Life	Finance	Cars
Web <sub>u1</sub>	4	1	Null
Web <sub>u2</sub>	4	1	4
Web <sub>u3</sub>	5	Null	3
Web <sub>u4</sub>	3	5	2
Web <sub>u5</sub>	3	Null	1
	Games	Films	Shopping
Web <sub>u1</sub>	2	5	1
Web <sub>u2</sub>	1	3	2
Web <sub>u3</sub>	1	3	2
Web <sub>u4</sub>	1	3	3
Web <sub>u5</sub>	2	5	Null

the score and set a threshold " $b$ ." All the candidate web services with a ranking score greater than " $b$ " form a set  $Y$ . And the web services in the top- $K$  recommended list are selected from this set. The above is the content of step 3; its pseudocode can be described by Algorithm 3.

*3.4. Step 4: Create a Diversified Web Service Recommended List.* The purpose of setting threshold " $b$ " is to ensure the accuracy of the top- $K$  recommended list, which is usually recommended to the user by selecting the first  $K$  services from high value to low value according to  $\text{Score}_j$ . Although it ensures the high accuracy of the recommendation results, it leads to the decrease of the diversity. Besides, it may cause the problem of overfitting, which is not conducive to exploring the potential preferences of users [18–21]. Therefore, we need a method which can balance accuracy and diversity.



TABLE 4: The user's module preference degree.

	Entertainment	Military	Sports
$M_j$	1.8	1.8	4.0
	Life	Finance	Cars
$M_j$	3.8	1.4	2.0
	Games	Films	Shopping
$M_j$	1.4	3.8	1.6

TABLE 5: The WSDL documents of web services in set P.

	Sports	Life	Films
$Web_{u1}$	Shooting	Marriage	Ang Lee
	Video	Marriage	Ang Lee
	Long	Article	Ang Lee
	Slow	Long	Article
$Web_{u2}$	Shooting	Marriage	Hollywood
	Video		Article
	Short	Picture	
	Fast		Long
$Web_{u3}$	Gymnastics	Cooking	Ang Lee
		Video	Video
	Picture	Short	Long
		Fast	Slow
$Web_{u4}$	Shooting	Cooking	Action movie
	Shooting	Cooking	
	Article	Cooking	Picture
	Long	Picture	
$Web_{u5}$	Gymnastics	Cooking	Hollywood
	Video	Cooking	Video
	Long	Cooking	Short
	Slow	Article	Fast

Step 4 provides a solution to how to make the recommendations more diverse while ensuring a high accuracy at the same time.

First, we set up an index of all candidate web services in the set  $Y$  and select  $K$  services according to different index numbers to form multiple recommended lists. Then, we define the diversity of web services in recommended lists as the list-diversity and each recommended list's list-diversity is calculated in equation (7). Finally, we select the recommended list with the highest list-diversity value as the top- $K$  recommended list to recommend to users.

$$\text{List-diversity} = 1 - \frac{2}{N(N-1)} \sum_{i,j \in Y, i \neq j} \text{CosSim}_{i,j}. \quad (7)$$

The list-diversity means the average dissimilarity between each pair of web services in a recommended list. In equation (7),  $Y$  represents the set  $Y$  and  $N = |Y|$ .  $\text{CosSim}_{i,j}$

TABLE 6: The WSDL documents of candidate web services.

	Candidate services
$Web_1$	Ang Lee, article, long
$Web_2$	Cooking, cooking, picture
$Web_3$	Shooting, video, short, fast
$Web_4$	Marriage, video, long, slow
$Web_5$	Diving, diving, picture
$Web_6$	Gymnastics, article, long
$Web_7$	Hollywood, picture
$Web_8$	Hollywood, video, short, fast
$Web_9$	Action movie, article
$Web_{10}$	Shooting, shooting, article, long

represents the similarity of every two candidate web services in a list. The above is the content of step 4, its pseudocode can be described by Algorithm 4 (set the length of recommended list is  $K$ ).

#### 4. Case Study

In order to introduce the specific steps of DivMTID, and also to further illustrate the effectiveness of DivMTID, a case study is provided in this section.

Suppose that there are nine existing modules including entertainment, military, sports, life, finance, cars, games, films, and shopping. We assume that there are five different web services under each module and there are ten candidate web services. A user rated the web services he has used (rating values between 1 and 5, no rating value is recorded as null which equals to 0). Table 3 is the user's history rating records. Now, our work is providing the user with a top- $K$  web service recommended list. We set the threshold " $a$ " to 3.

**4.1. Step 1: Explore Users' Preferences Approximately.** We use equation (1) to calculate the user's preference degree for each module and make an approximate positioning of the user's preference. After the calculation, we get the preference degree values  $M_j$ , and the results are shown in Table 4.

Because we have set the threshold " $a$ " to 3, the modules containing sports, life, and films whose  $M_j$  greater than 3 are the user's approximate preference modules. The web services under these three modules form a set  $P$ .

**4.2. Step 2: Calculate TF-IDF Weight Vectors of Web Services.** After approximately exploring the user's preferences, we calculate the weight vectors of web services utilizing the WSDL documents of all services in the set  $P$  and the WSDL documents of all candidate services. Table 5 shows the WSDL documents of all web services in the set  $P$ , and Table 6 shows the WSDL documents of all candidate services.

A corpus containing all meaningful words from the WSDL documents of all services in the set  $P$  and the WSDL documents of all candidate services is made (shooting, gymnastics, diving, marriage, cooking, Ang Lee, Hollywood, action movie, video, article, picture, long, short, fast, and

slow). Then, we calculate the weight vector of each web service according to equation (4).

The sports module:

$$\begin{aligned}
\vec{\omega}_{u1} &= (1.35, 0, 0, 0, 0, 0, 0, 0, 0, 0.54, 0, 0, 0.44, 0, 0, 1.75), \\
\vec{\omega}_{u2} &= (1.35, 0, 0, 0, 0, 0, 0, 0, 0, 0.54, 0, 0, 0, 1.35, 1.35, 0), \\
\vec{\omega}_{u3} &= (0, 4.68, 0, 0, 0, 0, 0, 0, 0, 0, 1.69, 0, 0, 0, 0, 0), \\
\vec{\omega}_{u4} &= (2.69, 0, 0, 0, 0, 0, 0, 0, 0, 0.54, 0, 0.44, 0, 0, 0, 0), \\
\vec{\omega}_{u5} &= (0, 2.34, 0, 0, 0, 0, 0, 0, 0, 0.54, 0, 0, 0.44, 0, 0, 1.75).
\end{aligned} \tag{8}$$

The life module:

$$\begin{aligned}
\vec{\omega}_{u1} &= (0, 0, 0, 4.68, 0, 0, 0, 0, 0, 0.54, 0, 0.44, 0, 0, 0, 0), \\
\vec{\omega}_{u2} &= (0, 0, 0, 4.68, 0, 0, 0, 0, 0, 0, 1.69, 0, 0, 0, 0, 0), \\
\vec{\omega}_{u3} &= (0, 0, 0, 0, 1.75, 0, 0, 0, 0, 0.54, 0, 0, 0, 1.35, 1.35, 0), \\
\vec{\omega}_{u4} &= (0, 0, 0, 0, 5.24, 0, 0, 0, 0, 0, 0.84, 0, 0, 0, 0, 0), \\
\vec{\omega}_{u5} &= (0, 0, 0, 0, 5.24, 0, 0, 0, 0, 0.54, 0, 0, 0, 0, 0, 0),
\end{aligned} \tag{9}$$

The films module:

$$\begin{aligned}
\vec{\omega}_{u1} &= (0, 0, 0, 0, 0, 7.01, 0, 0, 0, 0.54, 0, 0, 0, 0, 0, 0), \\
\vec{\omega}_{u2} &= (0, 0, 0, 0, 0, 0, 2.31, 0, 0, 0.72, 0, 0.58, 0, 0, 0, 0), \\
\vec{\omega}_{u3} &= (0, 0, 0, 0, 0, 2.34, 0, 0, 0.54, 0, 0, 0.44, 0, 0, 1.75, 0), \\
\vec{\omega}_{u4} &= (0, 0, 0, 0, 0, 0, 0, 6.64, 0, 0, 1.69, 0, 0, 0, 0, 0), \\
\vec{\omega}_{u5} &= (0, 0, 0, 0, 0, 0, 1.75, 0, 0.54, 0, 0, 0, 1.35, 1.35, 0, 0).
\end{aligned}$$

The candidate services:

$$\begin{aligned}
\vec{\omega}_1 &= (0, 0, 0, 0, 0, 3.09, 0, 0, 0, 0.72, 0, 0.58, 0, 0, 0, 0), \\
\vec{\omega}_2 &= (0, 0, 0, 0, 4.66, 0, 0, 0, 0, 0, 1.12, 0, 0, 0, 0, 0), \\
\vec{\omega}_3 &= (1.35, 0, 0, 0, 0, 0, 0, 0, 0.54, 0, 0, 0, 1.35, 1.35, 0, 0), \\
\vec{\omega}_4 &= (0, 0, 0, 2.34, 0, 0, 0, 0, 0.54, 0, 0, 0.44, 0, 0, 1.75, 0), \\
\vec{\omega}_5 &= (0, 0, 14.36, 0, 0, 0, 0, 0, 0, 0, 1.12, 0, 0, 0, 0, 0), \\
\vec{\omega}_6 &= (0, 3.11, 0, 0, 0, 0, 0, 0, 0.72, 0, 0.58, 0, 0, 0, 0, 0), \\
\vec{\omega}_7 &= (0, 0, 0, 0, 0, 0, 3.5, 0, 0, 0, 1.69, 0, 0, 0, 0, 0), \\
\vec{\omega}_8 &= (0, 0, 0, 0, 0, 0, 1.75, 0, 0.54, 0, 0, 0, 1.35, 1.35, 0, 0), \\
\vec{\omega}_9 &= (0, 0, 0, 0, 0, 0, 0, 6.64, 0, 1.09, 0, 0, 0, 0, 0, 0), \\
\vec{\omega}_{10} &= (2.69, 0, 0, 0, 0, 0, 0, 0, 0, 0.54, 0, 0.44, 0, 0, 0, 0).
\end{aligned} \tag{10}$$

**4.3. Step 3: Predict the Ranking Scores of Candidate Services.** According to equation (5), the cosine similarity of the TF-IDF weight vectors is calculated sequentially for each candidate web service with each historically used web service in the set P, and the  $\text{CosSim}_{i,j}$  value of each candidate service is obtained. Then, the ranking score of each candidate web

TABLE 7: The ranking scores of candidate web services.

	Web <sub>3</sub>	Web <sub>8</sub>	Web <sub>4</sub>	Web <sub>2</sub>	Web <sub>1</sub>
Score <sub>j</sub>	15.685	13.166	11.253	9.834	8.311
	Web <sub>7</sub>	Web <sub>6</sub>	Web <sub>10</sub>	Web <sub>9</sub>	Web <sub>5</sub>
Score <sub>j</sub>	7.052	6.234	5.801	3.347	0.275

TABLE 8: The list-diversity and the rank of recommended list.

Recommended list	List-diversity	Rank
Web <sub>3</sub> , Web <sub>8</sub> , Web <sub>4</sub>	0.930	10
Web <sub>3</sub> , Web <sub>8</sub> , Web <sub>2</sub>	0.938	8
Web <sub>3</sub> , Web <sub>8</sub> , Web <sub>1</sub>	0.938	8
Web <sub>3</sub> , Web <sub>4</sub> , Web <sub>2</sub>	0.996	4
Web <sub>3</sub> , Web <sub>4</sub> , Web <sub>1</sub>	0.993	7
Web <sub>3</sub> , Web <sub>2</sub> , Web <sub>1</sub>	1.000	1
Web <sub>8</sub> , Web <sub>4</sub> , Web <sub>2</sub>	0.996	4
Web <sub>8</sub> , Web <sub>4</sub> , Web <sub>1</sub>	0.994	6
Web <sub>8</sub> , Web <sub>2</sub> , Web <sub>1</sub>	1.000	1
Web <sub>4</sub> , Web <sub>2</sub> , Web <sub>1</sub>	0.997	3

service is calculated by equation (6), and it is shown in Table 7.

We set the threshold “ $b$ ” to 8 and make all candidate web services with a ranking score higher than 8 form a set Y. It is shown that the web services which are in set Y contain Web<sub>3</sub>, Web<sub>8</sub>, Web<sub>4</sub>, Web<sub>2</sub>, and Web<sub>1</sub>.

**4.4. Step 4: Create a Diversified Web Service Recommended List.** Suppose the value of  $K$  is 3. Then, we need to build a diversified recommended list containing 3 web services for the user. Step 4 establishes an index of all candidate web services in the set Y, and three web services are selected according to different index numbers to form multiple recommended lists. The list-diversity of each recommended list is calculated by equation (7). Finally, the recommended list with the highest list-diversity value is selected as the top-3 recommended list recommended to the user. The results are shown in Table 8.

As shown in Table 8, we can see that there are two recommended lists ranked first. If two lists have the same ranking value that indicates the same diversity, we need to consider accuracy to further rank them. In other words, we need to compare the sum of every candidate service’s ranking score through Step 3. And the list that has a higher ranking score sum of candidate services is preferred. As a consequence, we choose the list including Web<sub>3</sub>, Web<sub>2</sub>, and Web<sub>1</sub> as the top-3 web service recommended list.

## 5. Conclusions and Future Work

This paper presents a new web service recommendation method called DivMTID. This method first uses users’ history ratings about web services to approximately explore users’ preferences. Second, it uses the TF-IDF algorithm to calculate the weight vectors of each web service. Third, it uses the cosine similarity to calculate the similarity between

candidate web services and historical services in order to estimate the ranking scores of candidate services. Finally, list-diversity is used to generate the top- $K$  recommended list. DivMTID takes the accuracy and diversity index of web service recommendation into account and achieves high diversity of recommendation results while ensuring high accuracy. It comprehensively balances the influence of accuracy and diversity on recommendation results, avoiding the appearance of recommendation redundancy and solving the problem of overfitting. DivMTID is an effective, accurate, and diverse service recommendation method, which is worth popularizing and using.

However, the specific influence of this method in many aspects of the recommender system is not measured. Therefore, in the future work, we will do more experiments about this method's influence on each index of the recommender system.

In addition, we will take the time and space factors into consideration to improve the algorithm from many aspects, such as privacy [22–25]. We will also further improve the performance and effectiveness of the algorithm [26–28] by combining some new approaches such as Blockchain and Edge Computing [29–32].

## Data Availability

Our study does not need any data set. And all the data used to support the findings of this study are included within the article.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (No. 61872219), the Natural Science Foundation of Shandong Province (ZR2019MF001), and the Open Project of the State Key Laboratory of Novel Software Technology (No. KFKT2020B08).

## References

- [1] B. Alhijawi and Y. Kilani, "The recommender system: a survey," *International Journal of Advanced Intelligence Paradigms*, vol. 15, no. 3, p. 1, 2020.
- [2] L. Qi, H. Xiang, W. Dou, C. Yang, Y. Qin, and X. Zhang, "Privacy-preserving distributed service recommendation based on locality-sensitive hashing," *IEEE International Conference on Web Services*, pp. 49–56, 2017.
- [3] L. Qi, W. Dou, C. Hu, Y. Zhou, and J. Yu, "A context-aware service evaluation approach over big data for cloud applications," *IEEE Transactions on Cloud Computing*, vol. 8, no. 2, pp. 338–348, 2020.
- [4] C. Zhou, A. Li, A. Hou et al., "Modeling methodology for early warning of chronic heart failure based on real medical big data," *Expert Systems with Applications*, vol. 151, article 113361, 2020.
- [5] P. Pirasteh, D. Hwang, and J. J. Jung, "Exploiting matrix factorization to asymmetric user similarities in recommendation systems," *Knowledge-Based Systems*, vol. 83, no. 1, pp. 51–57, 2015.
- [6] X. Wu, B. Cheng, and J. Chen, "Collaborative filtering service recommendation based on a novel similarity computation method," *IEEE Transactions on Services Computing*, vol. 10, no. 3, pp. 352–365, 2017.
- [7] L. Qi, Q. He, F. Chen et al., "Finding all you need: web APIs recommendation in web of things through keywords search," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 5, pp. 1063–1072, 2019.
- [8] G. Kang, M. Tang, J. Liu, X. Liu, and B. Cao, "Diversifying web service recommendation results via exploring service usage history," *IEEE Transactions on Services Computing*, vol. 9, no. 4, pp. 566–579, 2016.
- [9] J. Li, T. Cai, K. Deng, X. Wang, T. Sellis, and F. Xia, "Community-diversified influence maximization in social networks," *Information Systems*, vol. 92, article 101522, 2020.
- [10] M. Kunaver and T. Požrl, "Diversity in recommender systems – a survey," *Knowledge-Based Systems*, vol. 123, pp. 154–162, 2017.
- [11] A. Gogna and A. Majumdar, "Balancing accuracy and diversity in recommendations using matrix completion framework," *Knowledge-Based Systems*, vol. 125, pp. 83–95, 2017.
- [12] T. Yu, J. Guo, W. Li, H. J. Wang, and L. Fan, "Recommendation with diversity: an adaptive trust-aware model," *Decision Support Systems*, vol. 123, article 113073, 2019.
- [13] Y. Wang, Z. Cai, Z.-H. Zhan, B. Zhao, X. Tong, and L. Qi, "Walrasian equilibrium-based multiobjective optimization for task allocation in mobile crowdsourcing," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 4, pp. 1033–1046, 2020.
- [14] Y. Wang, Z. Cai, Z.-H. Zhan, Y.-J. Gong, and X. Tong, "An optimization and auction-based incentive mechanism to maximize social welfare for mobile crowdsourcing," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 3, pp. 414–429, 2019.
- [15] A. Guo and T. Yang, "Research and improvement of feature words weight based on TF-IDF algorithm," in *2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference*, pp. 415–419, Chongqing, China, 2016.
- [16] D. Kim, D. Seo, S. Cho, and P. Kang, "Multi-co-training for document classification using various document representations: TF-IDF, LDA, and Doc2Vec," *Information Sciences*, vol. 477, pp. 15–29, 2019.
- [17] Y. Liu, Q. Xu, and Z. Tang, "Research on text classification method based on PTF-IDF and cosine similarity," in *2019 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS)*, pp. 205–208, Shanghai, China, 2019.
- [18] L. Wang, X. Zhang, R. Wang, C. Yan, H. Kou, and L. Qi, "Diversified service recommendation with high accuracy and efficiency," *Knowledge-Based Systems*, vol. 204, article 106196, 2020.
- [19] J. Moody and D. H. Glass, "A novel classification framework for evaluating individual and aggregate diversity in top-N recommendations," *ACM Transactions on Intelligent Systems and Technology*, vol. 7, no. 3, pp. 1–21, 2016.
- [20] L. Wang, X. Zhang, T. Wang et al., "Diversified and scalable service recommendation with accuracy guarantee," *IEEE Transactions on Computational Social Systems*, pp. 1–12, 2020.

- [21] Y. Zuo, M. Gong, J. Zeng, L. Ma, and L. Jiao, "Personalized recommendation based on evolutionary multi-objective optimization," *IEEE Computational Intelligence Magazine*, vol. 10, no. 1, pp. 52–62, 2015.
- [22] Z. Cai, X. Zheng, and J. Yu, "A differential-private framework for urban traffic flows estimation via taxi companies," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6492–6499, 2019.
- [23] J. Wang, Z. Cai, and J. Yu, "Achieving personalized  $k$ -anonymity based content privacy for autonomous vehicles in CPS," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4242–4251, 2020.
- [24] Y. Wang, Z. Cai, X. Tong, Y. Gao, and G. Yin, "Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems," *Computer Networks*, vol. 135, pp. 32–43, 2018.
- [25] T. Liu, Y. Wang, Y. Li, X. Tong, L. Qi, and N. Jiang, "Privacy protection based on stream cipher for spatio-temporal data in IoT," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 7928–7940, 2020.
- [26] X. Xia, F. Chen, Q. He, J. Grundy, M. Abdelrazek, and H. Jin, "Cost-effective app data distribution in edge computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 1, pp. 31–44, 2020.
- [27] Y. Wang, Q. He, D. Ye, and Y. Yang, "Formulating criticality-based cost-effective fault tolerance strategies for multi-tenant service-based systems," *IEEE Transactions on Software Engineering*, vol. 44, no. 3, pp. 291–307, 2018.
- [28] L. Lin, T.-T. Goh, and D. Jin, "How textual quality of online reviews affect classification performance: a case of deep learning sentiment analysis," *Neural Computing and Applications, Springer London*, vol. 32, pp. 4387–4415, 2020.
- [29] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, "Blockchain empowered arbitrable data auditing scheme for network storage as a service," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 289–300, 2020.
- [30] Q. He, G. Cui, X. Zhang et al., "A game-theoretical approach for user allocation in edge computing environment," *IEEE Transactions on Parallel and Distributed Systems*, vol. 31, no. 3, pp. 515–529, 2020.
- [31] L. Yu, H. Shen, Z. Cai, L. Liu, and P. Calton, "Towards bandwidth guarantee for virtual clusters under demand uncertainty in multi-tenant clouds," *IEEE Transactions on Parallel and Distributed Systems*, vol. 29, no. 2, pp. 450–465, 2018.
- [32] T. Zhu, T. Shi, J. Li, Z. Cai, and X. Zhou, "Task scheduling in deadline-aware mobile edge computing systems," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4854–4866, 2019.