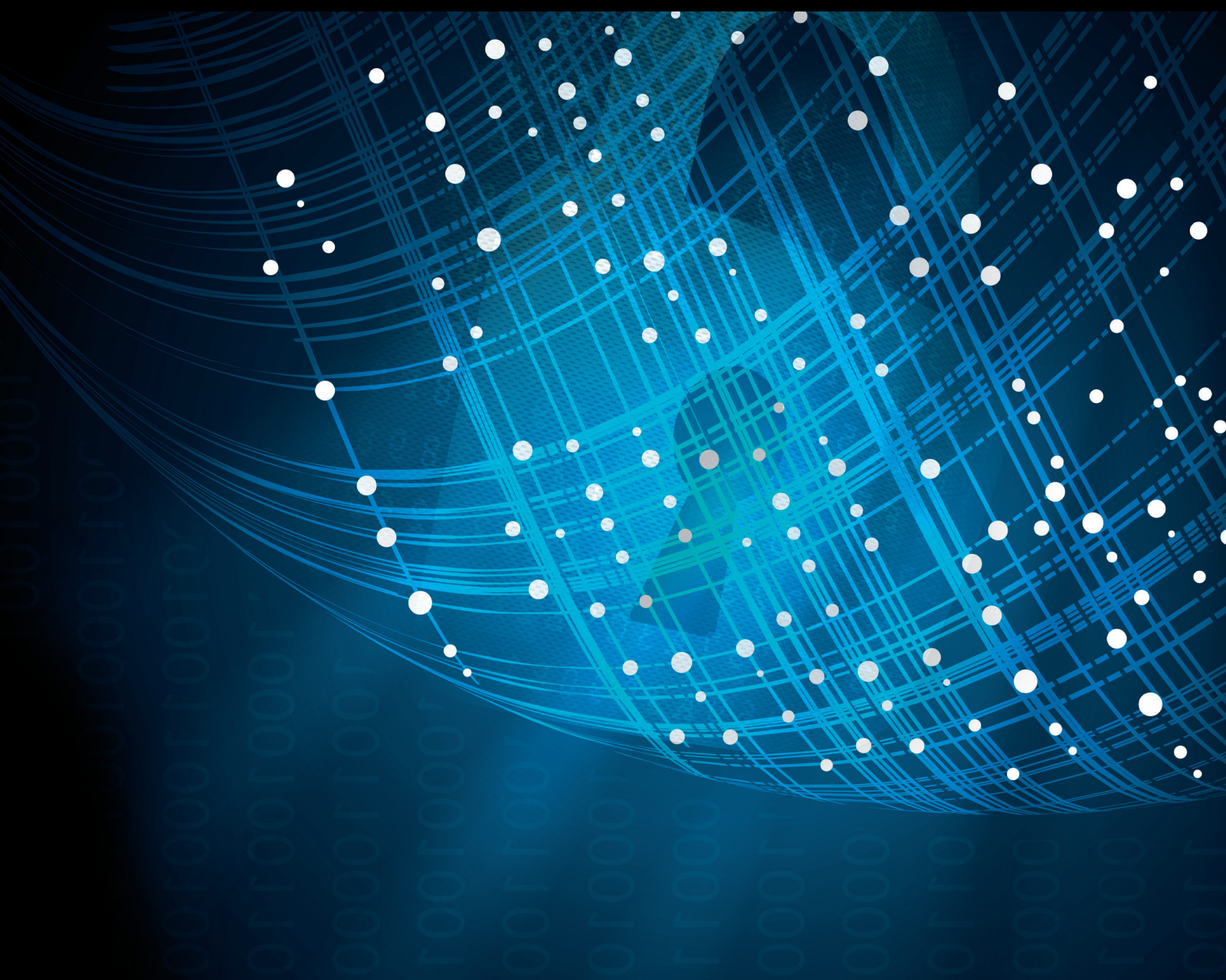


Security and Communication Networks

Theory and Engineering Practice for Security and Privacy of Edge Computing 2021

Lead Guest Editor: Honghao Gao

Guest Editors: Zhiyuan Tan, Wenbing Zhao, and Yuyu Yin





**Theory and Engineering Practice for Security
and Privacy of Edge Computing 2021**

Security and Communication Networks

**Theory and Engineering Practice for
Security and Privacy of Edge Computing
2021**

Lead Guest Editor: Honghao Gao

Guest Editors: Zhiyuan Tan, Wenbing Zhao, and
Yuyu Yin





Copyright © 2022 Hindawi Limited. All rights reserved.

This is a special issue published in "Security and Communication Networks." 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

Roberto Di Pietro, Saudi Arabia

Associate Editors

Jiankun Hu , Australia
Emanuele Maiorana , Italy
David Megias , Spain
Zheng Yan , China

Academic Editors

Saed Saleh Al Rabae , United Arab Emirates
Shadab Alam, Saudi Arabia
Goutham Reddy Alavalapati , USA
Jehad Ali , Republic of Korea
Jehad Ali, Saint Vincent and the Grenadines
Benjamin Aziz , United Kingdom
Taimur Bakhshi , United Kingdom
Spiridon Bakiras , Qatar
Musa Balta, Turkey
Jin Wook Byun , Republic of Korea
Bruno Carpentieri , Italy
Luigi Catuogno , Italy
Ricardo Chaves , Portugal
Chien-Ming Chen , China
Tom Chen , United Kingdom
Stelvio Cimato , Italy
Vincenzo Conti , Italy
Luigi Coppolino , Italy
Salvatore D'Antonio , Italy
Juhriyansyah Dalle, Indonesia
Alfredo De Santis, Italy
Angel M. Del Rey , Spain
Roberto Di Pietro , France
Wenxiu Ding , China
Nicola Dragoni , Denmark
Wei Feng , China
Carmen Fernandez-Gago, Spain
AnMin Fu , China
Clemente Galdi , Italy
Dimitrios Geneiatakis , Italy
Muhammad A. Gondal , Oman
Francesco Gringoli , Italy
Biao Han , China
Jinguang Han , China
Khizar Hayat, Oman
Azeem Irshad, Pakistan

M.A. Jabbar , India
Minho Jo , Republic of Korea
Arijit Karati , Taiwan
ASM Kayes , Australia
Farrukh Aslam Khan , Saudi Arabia
Fazlullah Khan , Pakistan
Kiseon Kim , Republic of Korea
Mehmet Zeki Konyar, Turkey
Sanjeev Kumar, USA
Hyun Kwon, Republic of Korea
Maryline Laurent , France
Jegatha Deborah Lazarus , India
Huaizhi Li , USA
Jiguo Li , China
Xueqin Liang, Finland
Zhe Liu, Canada
Guangchi Liu , USA
Flavio Lombardi , Italy
Yang Lu, China
Vincente Martin, Spain
Weizhi Meng , Denmark
Andrea Michienzi , Italy
Laura Mongioi , Italy
Raul Monroy , Mexico
Naghme Moradpoor , United Kingdom
Leonardo Mostarda , Italy
Mohamed Nassar , Lebanon
Qiang Ni, United Kingdom
Mahmood Niazi , Saudi Arabia
Vincent O. Nyangaresi, Kenya
Lu Ou , China
Hyun-A Park, Republic of Korea
A. Peinado , Spain
Gerardo Pelosi , Italy
Gregorio Martinez Perez , Spain
Pedro Peris-Lopez , Spain
Carla Ràfols, Germany
Francesco Regazzoni, Switzerland
Abdalhossein Rezai , Iran
Helena Rifà-Pous , Spain
Arun Kumar Sangaiah, India
Nadeem Sarwar, Pakistan
Neetesh Saxena, United Kingdom
Savio Sciancalepore , The Netherlands

De Rosal Ignatius Moses Setiadi ,
Indonesia
Wenbo Shi, China
Ghanshyam Singh , South Africa
Vasco Soares, Portugal
Salvatore Sorce , Italy
Abdulhamit Subasi, Saudi Arabia
Zhiyuan Tan , United Kingdom
Keke Tang , China
Je Sen Teh , Australia
Bohui Wang, China
Guojun Wang, China
Jinwei Wang , China
Qichun Wang , China
Hu Xiong , China
Chang Xu , China
Xuehu Yan , China
Anjia Yang , China
Jiachen Yang , China
Yu Yao , China
Yinghui Ye, China
Kuo-Hui Yeh , Taiwan
Yong Yu , China
Xiaohui Yuan , USA
Sherali Zeadally, USA
Leo Y. Zhang, Australia
Tao Zhang, China
Youwen Zhu , China
Zhengyu Zhu , China

Contents

EPPSA: Efficient Privacy-Preserving Statistical Aggregation Scheme for Edge Computing-Enhanced Wireless Sensor Networks

Yunting Tao , Fanyu Kong , Jia Yu, and Qiuliang Xu 


Research Article (12 pages), Article ID 7359134, Volume 2022 (2022)

Multiagent Reinforcement Learning for Task Offloading of Space/Aerial-Assisted Edge Computing

Yanlong Li, Lei Liang, Jielin Fu , and Junyi Wang

Research Article (10 pages), Article ID 4193365, Volume 2022 (2022)

Comparison of Blackhole and Wormhole Attacks in Cloud MANET Enabled IoT for Agricultural Field Monitoring

Tauqeer Safdar Malik, Muhammad Nasir Siddiqui, Muhammad Mateen, Kaleem Razzaq Malik, Song Sun, and Junhao Wen 



Research Article (18 pages), Article ID 4943218, Volume 2022 (2022)

Multinode Data Offloading for Urban Wireless Sensor Networks Based on Fog Computing: A Multiarmed Bandit Approach

Yuchen Shan, Hui Wang , and Chenxiang Zhang

Research Article (17 pages), Article ID 2965081, Volume 2022 (2022)

Protecting Location Privacy in IoT Wireless Sensor Networks through Addresses Anonymity

Qiong Zhang  and Kewang Zhang 





Research Article (12 pages), Article ID 2440313, Volume 2022 (2022)

A Power Transformer Fault Prediction Method through Temporal Convolutional Network on Dissolved Gas Chromatography Data

Mengda Xing , Weilong Ding , Han Li , and Tianpu Zhang 

Research Article (11 pages), Article ID 5357412, Volume 2022 (2022)

A Blockchain-Based Privacy Preservation Scheme in Mobile Medical

Haiying Wen , Meiyang Wei , Danlei Du , and Xiangdong Yin 




Research Article (11 pages), Article ID 9889263, Volume 2022 (2022)

Healthcare Big Data Privacy Protection Model Based on Risk-Adaptive Access Control

Rong Jiang, Shanshan Han, Mingyue Shi, Tilei Gao , and Xusheng Zhao


Research Article (12 pages), Article ID 3086516, Volume 2022 (2022)

A Method of the Active and Passive Event Service Based on the Sensor Web

Lan Liu , Jingjing Fan, Chengfan Li , and Xuefeng Liu 

Research Article (11 pages), Article ID 2578744, Volume 2022 (2022)

PACAM: A Pairwise-Allocated Strategy and Capability Average Matrix-Based Task Scheduling Approach for Edge Computing

Feng Hong, Tianming Zhang , Bin Cao, and Jing Fan

Research Article (14 pages), Article ID 6430612, Volume 2022 (2022)

GTF: An Adaptive Network Anomaly Detection Method at the Network Edge

Renjie Li , Zhou Zhou , Xuan Liu , Da Li , Wei Yang , Shu Li , and Qingyun Liu 

Research Article (12 pages), Article ID 3017797, Volume 2021 (2021)

BEvote: Bitcoin-Enabled E-Voting Scheme with Anonymity and Robustness

Ning Lu, Xin Xu, Chang Choi , Tianlong Fei, and Wenbo Shi

Research Article (14 pages), Article ID 9988646, Volume 2021 (2021)

A Novel Video Copyright Protection Scheme Based on Blockchain and Double Watermarking

Jingjing Zheng , Shuhua Teng , Peirong Li , Wei Ou , Donghao Zhou , and Jun Ye 

Research Article (16 pages), Article ID 6493306, Volume 2021 (2021)

Joint Design of Beamforming and Edge Caching in Fog Radio Access Networks

Wenjing Lv, Rui Wang , Jun Wu , Zhijun Fang, and Songlin Cheng 

Research Article (8 pages), Article ID 1935453, Volume 2021 (2021)

Research Article

EPPSA: Efficient Privacy-Preserving Statistical Aggregation Scheme for Edge Computing-Enhanced Wireless Sensor Networks

Yunting Tao ¹, Fanyu Kong ¹, Jia Yu,² and Qiuliang Xu ¹

¹School of Software, Shandong University, Jinan 250101, China

²College of Computer Science and Technology, Qingdao University, Qingdao 266071, China

Correspondence should be addressed to Fanyu Kong; fanyukong@sdu.edu.cn

Received 29 November 2021; Accepted 1 April 2022; Published 2 May 2022

Academic Editor: Yuyu Yin

Copyright © 2022 Yunting 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.

In edge computing-enhanced wireless sensor networks (WSNs), multidimensional data aggregation can optimize the utilization of computation resources for data collection. How to improve the efficiency of data aggregation has gained considerable attention in both academic and industrial fields. This article proposes a new efficient privacy-preserving statistical aggregation scheme (EPPSA) for WSNs, in which statistical data can be calculated without exposing the total number of sensor devices to control center. The EPPSA scheme supports multiple statistical aggregation functions, including arithmetic mean, quadratic mean, weighted mean, and variance. Furthermore, the EPPSA scheme adopts the modified Montgomery exponentiation algorithms to improve the aggregation efficiency in the edge aggregator. The performance evaluation shows that the EPPSA scheme gets higher aggregation efficiency and lower communication load than the existing statistical aggregation schemes.

1. Introduction

In recent years, wireless sensor networks (WSNs) have achieved an accelerated increase in deployment. WSNs are widely utilized in scenarios such as smart homes [1], vehicular ad hoc networks [2–4], industrial Internet of Things [5], and monitoring environments [6–8]. The sensor devices in WSNs are responsible for sensing real-time data and transmitting the sensed data to control center for data analysis and intelligent control. In a variety of WSN applications, some computations are too time-consuming for sensor devices. Edge computation is an effective solution for resource-limited sensor devices to gain edge devices' assistance, such as data aggregation and neural network models [9]. With the edge computation devices deployed near the target area, the computing load in WSN sensor devices could be distributed to the edge devices. With the help of edge computation devices, cloud data centers provide various services for numbers of applications [10–13].

To reduce data redundancy and communication delay, data aggregation has become one of the most practical techniques, which can be used in edge computing-enhanced

WSNs. Usually, a gateway is an ideal edge device to perform data aggregation operations due to its high computational capability, and mobile edge computing (MEC) also provides an emergent paradigm that brings computation close to mobile sensors [14]. It is worth noting that data aggregation at edge gateways may suffer from some potential security risks [15]. Firstly, the data may be captured or falsified during the delivery process, considering WSNs are usually deployed in an unattended environment. Secondly, adversaries can invade the edge gateway for stealing users' private data. The traditional security approaches cannot be directly applied to edge computing-enhanced WSN data aggregation, since they may be conflicted with aggregation function [16]. Furthermore, due to the dynamic and heterogeneous characteristics of WSN devices, there exists difficulty for the sensed data to be collected, encrypted, used, and stored in accordance with the users' preferences [17, 18].

To solve the above problems, homomorphic encryption algorithms have been considered to construct privacy-preserving single-dimensional aggregation schemes [19–21]. Furthermore, researchers proposed several multidimensional privacy-preserving data aggregation schemes, the core

idea of which is to construct a conversion mechanism between multidimensional data and large integers [19, 20, 22–33]. These researches are centered on how to reduce computation costs and communication load while collecting and transmitting the data. Lu et al. [26] proposed an efficient privacy-preserving data aggregation (EPPA) scheme in smart grids. Merging multidimensional data by super-increasing sequence of large primes, Lu et al.'s scheme is more efficient than the one-dimensional data aggregation schemes. Using a polynomial method, Shen et al. [27] constructed a user-level polynomial to store multidimensional values in a single data space based on Horner's rule. Fault tolerance can be used to enhance the security and robustness of a data aggregation scheme. In [32], Mohammadali et al. presented a homomorphic privacy-preserving data aggregation scheme with the fault tolerance property, so it can keep data secure even if the aggregator is malicious or curious.

Most secure data aggregation schemes only consider summation-based aggregation since the underlying additive homomorphic encryption only supports the modular addition operations. In practice, various types of statistics (e.g., mean, variance and standard deviation) might often need to be supported for data application [34]. Therefore, it is necessary to design multifunctional secure data aggregation scheme supporting various data statistics. Zhang et al. [35] proposed a multifunctional secure data aggregation scheme (MODA). This scheme offers the building blocks for multifunctional aggregation by encoding raw data into well-defined vectors. Peng et al. [36] introduced a multifunctional aggregation scheme supporting diversified aggregation functions, including linear, polynomial, and continuous functions. Both of the above schemes implement the statistical functions computed by control center. For example, in [36], the ciphertext sum is generated in the edge device and the mean is calculated using the decrypted sum by control center. Thus, the total number of sensor devices is required to transmit to control center for calculating the mean by sum/total number.

In lots of WSN application scenarios (e.g., industrial monitoring), the total number of sensor devices represents industrial scale which should be kept secret. Smart factories use WSNs and edge computation to create new production forms with better efficiency and flexibility. The total number of sensor devices usually represents industrial production scale in a smart factory. Usually, control center is a third-party service from the cloud or a regulatory agency from the government side. Trade secrets can be learned and used by rivals if the scale of a factory's production is disclosed. Therefore, it is necessary to compute statistical aggregation functions without exposing the total number of WSN sensor devices. In such a scenario, the control center could use statistical data for scientific analysis and intelligent decision-making but would not have any data about the industrial production scale of the smart factory.

In this article, we propose the first privacy-preserving statistical aggregation scheme without revealing the total number of sensor devices to control center for edge

computing-enhanced WSNs. The contributions of this article can be summarized as follows:

- (i) We construct an efficient privacy-preserving statistical aggregation scheme based on the Paillier additive homomorphic encryption scheme and the ECDSA digital signature scheme, called EPPSA. The EPPSA scheme supports multiple statistical aggregation functions, including arithmetic mean, quadratic mean, weighted mean, and variance.
- (ii) In the EPPSA scheme, the mean values can be calculated by the edge device and control center cooperatively, while control center does not know the total number of sensor devices. Firstly, the edge device computes the mean value in ciphertext since it has calculated the sum of the data in ciphertext.. Secondly, after receiving the mean in ciphertext, control center calculates the correct mean by using the modified extended Euclidean algorithm to process the decrypted mean. The EPPSA scheme avoids calculating sum/total number and the total number of WSN sensor devices can be kept secret to control center.
- (iii) In the EPPSA scheme, we propose three modified Montgomery exponentiation algorithms to improve the aggregation efficiency in the edge device. Our idea is to avoid converting the data between the Montgomery domain and residue domain frequently during the whole process. The ciphertext data in the Montgomery domain can be aggregated by Montgomery multiplications, which are more efficient than ordinary modular multiplications.
- (iv) We implement the EPPSA scheme and compare it with the existing schemes. Compared with [28], the EPPSA scheme gets 62.5% aggregation performance improvement for 1024 bits modulus. Compared with [36], the EPPSA scheme gets 50% and 33% communication load decrease on arithmetic mean and variance statistics, respectively.

The rest of this article is organized as follows: In Section 2, the problem formulation is presented. In Section 3, the related preliminaries are reviewed. In Section 4, the proposed EPPSA data aggregation scheme is given. In Section 5, the secure analysis is given. In Section 6, the performance evaluation and comparison are presented. Finally, Section 7 concludes this article.

2. Problem Formulation

In this section, the formalized system model, the security requirements, and design goals are presented.

2.1. System Model. In the EPPSA scheme, a WSN system is comprised of four parts, namely trusted authority (TA), control center (CC), edge aggregator (EA), and sensor device (SD). The system describes a three-level topological structure, as shown in Figure 1.

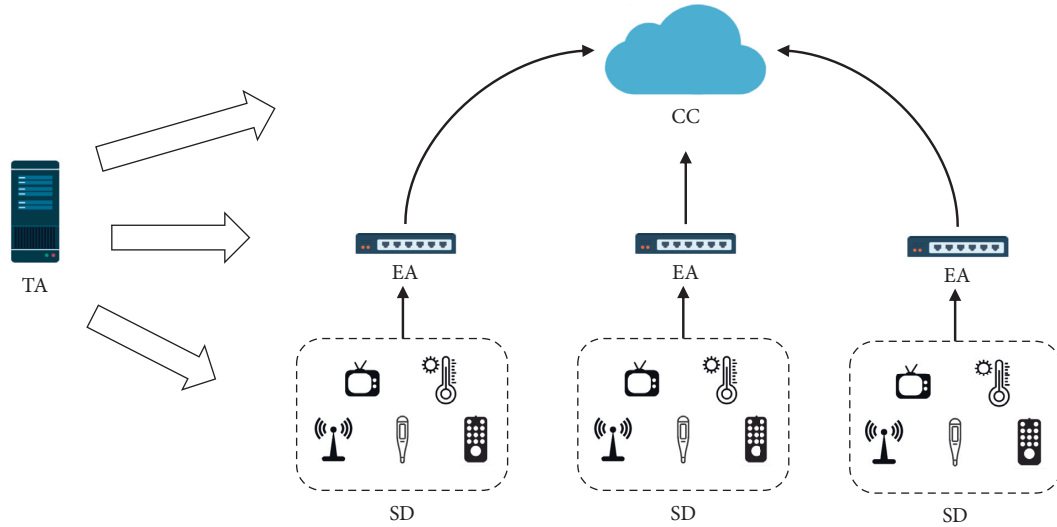


FIGURE 1: System model.

- (i) TA is a trusted third party, which is responsible for generating and distributing the secret keys to all the system participants. In the phase of system initialization, TA sets the ECDSA key pairs into the sensor devices, edge devices, and control center. TA distributes the Paillier public key to the sensor devices, edge devices, and the Paillier private key to control center separately by sending digital envelopes over the Internet.
- (ii) CC is a powerful service controller of a WSN sensing system. According to special application requirements, CC is responsible for analyzing the data statistics, for example, data mining. CC is assumed to be honest-but-curious. It means that CC attempts to mine valuable information while performing its specified tasks.
- (iii) EA is a wireless receiving equipment that is deployed at the edge of the WSN. EA is responsible for collection, aggregation, and transmission of sensor data. EA collects encrypted data from sensor devices, aggregates the data, and transmits the aggregated data to CC. EA is a high-performance computing device so that it can perform computationally expensive processes.
- (iv) SD is deployed at the intended area and is responsible for sensing and communication. SDs automatically sense and encrypt the particular data before sending them to EA. For example, ambient temperature sensors record the real-time temperature in an intelligent agricultural system and report the encrypted data to CC via EA.

2.2. Security Requirements. In our system model, EA and CC are curious about SD's privacy data, but they cannot collude with each other. Moreover, there is an adversary α assumed to have the capability to eavesdrop on data during their

transit. To protect data against internal and external attacks, the following security requirements should be fulfilled:

- (i) *Data confidentiality.* Even though data from SDs or EA is eavesdropped on by α during their transit, they cannot be identified. EA cannot infer the privacy information of SDs while aggregating statistical data. When CC receives the statistics data, for example, mean, variance, it cannot identify the individual data or number of SDs.
- (ii) *Authentication.* It should be guaranteed that the data are generated by legitimate SD entities. Otherwise, malicious operations from α , for example, replay attack, may undermine the accuracy of the statistics. Similarly, the aggregate data should be guaranteed to be generated by a legitimate EA.
- (iii) *Data integrity.* Accuracy and completeness of data in transmission should be guaranteed. When an adversary α forges or modifies the data, the malicious operations should be detected by the receiver.

2.3. Design Goal. Our design goal is to design an efficient privacy-preserving statistical aggregation scheme. The following design goals should be achieved:

- (i) *Security.* The proposed scheme should satisfy the secure requirements mentioned above. The security goal is to prevent individual data and statistical data from being stolen by the adversary. In order to achieve this security goal, both internal and external behavior should be detected.
- (ii) *Efficiency.* The proposed scheme should consider computation cost and communication load. On one hand, it is necessary to use lightweight encryption and signing primitives. On the other hand, methods should be adopted to reduce the consumption of aggregate computation.

- (iii) *Statistical aggregation.* A series of data statistical functions should be supported by the proposed scheme. In an actual scenario, statistics of measurement indicators, such as mean, weighted mean, and variance, are essential for analysis. Meanwhile, except for statistics, the CC should not get any other information.

3. Preliminaries

3.1. The Paillier Cryptosystem. The Paillier cryptosystem is a widely used public key encryption scheme with additive homomorphic property [37] and is standardized by International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) in 2019 [38]. The Paillier cryptosystem consists of three parts, namely key generation, encryption, and decryption, which are described in Scheme 1.

The security of the Paillier encryption algorithm is based on the integer factoring problem. When choosing the parameter g , it is necessary to judge whether n is divisible by the order of g . This can be efficiently checked by testing whether $\gcd(L(g^\lambda \bmod n^2), n) = 1$, where function $\gcd(\cdot)$ is the greatest common divisor function.

The Paillier cryptosystem has several interesting homomorphic properties, which are associated with the statistics given below:

$$\text{Dec}(\text{Enc}(d_1)\text{Enc}(d_2) \bmod n^2) = d_1 + d_2 \bmod n. \quad (1)$$

3.2. Mean Value Computation on Ciphertext of Paillier Cryptosystem. Shah et al. [39] proposed a solution for noninteger mean value computation in the homomorphic encrypted domain. This method can be adopted by statistical aggregation scheme in WSNs. Let (d_1, d_2, \dots, d_m) be a set of numbers. The mean value, denoted by d_{mean} , is the sum of the values divided by the total number of elements, $d_{\text{mean}} = \sum_{i=1}^m d_i/m$. In practice, the mean d_{mean} may result in integer or float value. Using the homomorphic property of the Paillier cryptosystem given in (2), the mean can be calculated in the encrypted domain.

$$\text{Enc}(d_{\text{mean}}) = \left(\prod_{i=1}^{i=m} \text{Enc}(d_i) \right)^{m^{-1} \bmod n} \bmod n^2. \quad (2)$$

If the plain domain mean d_{mean} is an integer, the encrypted domain mean $\text{Enc}(d_{\text{mean}})$ calculated by (2) results in the correct mean d_{mean} after decryption. However, if the plain domain mean d_{mean} is a decimal, the encrypted domain mean $\text{Enc}(d_{\text{mean}})$ calculated by (2) results in a large integer after decryption. For example, $d_{\text{mean}} = \alpha/\beta$, where α is not divisible by β . After decryption, $\text{Enc}(d_{\text{mean}})$ will result in $\alpha\beta^{-1} \bmod n^2$, which is a large integer. Reducing the large integer to the correct mean value is a two-dimensional lattice reduction problem and can be solved by the Lagrange-Gauss lattice reduction algorithm. Shah et al. proposed an efficient

Scheme	Computation complexity
EPPSA	$(m-1) \cdot T_{MM}$
[30]	$(m-1) \cdot T_{OMM}$
[33]	$(m-1) \cdot T_{OMM}$
[35]	$(m-1) \cdot T_{MM} + T_{ME}$

SCHEME 1: The Paillier cryptosystem.

method to reduce the large integer called the modified extended Euclidean algorithm (MME). The method is shown in Algorithm 1.

The modulus n of Paillier cryptosystem and large integer value w can be considered as independent points in a two-dimensional lattice space \mathcal{V} . These two basis vectors, $(0, n)$ and $(1, w)$, can be reduced for optimal values. Algorithm 1 computes the reduced value of w using adapted extended Euclidean algorithm, which is the correct mean value.

3.3. Montgomery Multiplication. Montgomery multiplication (MM) is an efficient technique for computing modular multiplications [40]. Assuming an odd modulus n is a t -bit number, let $r = 2^t$. For integers $0 < a, b < k$, the Montgomery multiplication is $MM(a, b) = ab2^{-t} \bmod n$. By taking r as a power of 2, the division becomes simple shifting. The process of MM is presented in Algorithm 2.

Utilizing the MM algorithm, the Montgomery exponentiation is present in Algorithm 3. For a number α , the corresponding number in the Montgomery domain is denoted by $\bar{\alpha}$.

4. The Proposed EPPSA Scheme

In this section, we propose the first privacy-preserving statistical aggregation scheme without revealing the total number of sensor devices to control center. In order to achieve the security goals, the edge device and control center calculates the statistics cooperatively, while control center does not know the total number of sensor devices. The Paillier cryptosystem is used as the encryption scheme and the ECDSA algorithm [41] is used as the signature scheme.

The EPPSA scheme consists of four phases including system initialization, data encryption, secure statistical aggregation, and secure statistics reading. In the system initialization phase, TA initializes the WSN system by generating and distributing the secret keys of the Paillier and ECDSA algorithms. In the data encryption phase, sensor device SD_i collects raw data and encrypts these data to generate a data report. Then sensor device sends the encrypted data report to EA via wireless networks. In the secure statistical aggregation phase, EA calculates sum and mean value in the encrypted domain and sends the statistical report to CC. In this phase, EA does not reveal the total

Input: n, w , where n is the modulus and w is the large number.
Output: $R_w = \text{MEE}(n, w)$.

- (1) $(x_1, x_2) = (0, n)$
- (2) $(y_1, y_2) = (1, w)$
- (3) $Q = \lfloor x_2/y_2 \rfloor$
- (4) $(tmp_1, tmp_2) = (x_1, x_2) - Q(y_1, y_2)$
- (5) $(x_1, x_2) = (y_1, y_2)$
- (6) $(y_1, y_2) = (tmp_1, tmp_2)$
- (7) while $w > \sqrt{n}$ do
- (8) $Q = \lfloor x_2/y_2 \rfloor$
- (9) $(tmp_1, tmp_2) = (x_1, x_2) - Q(y_1, y_2)$
- (10) $(x_1, x_2) = (y_1, y_2)$
- (11) $(y_1, y_2) = (tmp_1, tmp_2)$
- (12) end while
- (13) return $R_w = x_2/x_1$

ALGORITHM 1: The reduction based on modified extended Euclidean algorithm

(i) Input: a, b, n' , where n' is computed by the extended Euclidean algorithm.
Output: $v = \text{MM}(a, b)$.

- (1) $s = ab$
- (2) $m = sn' \bmod r$
- (3) $u = (s + mk)/r$
- (4) if $v \geq n$, then return $v - n$

(ii) else return v

ALGORITHM 2: The Montgomery multiplication

(i) Input: γ, e, n , where n' is computed by the extended Euclidean algorithm.
Output: $\theta = \gamma^e \bmod n$.

- (1) $\bar{\gamma} = \gamma \cdot r \bmod n$
- (2) $\bar{\theta} = 1 \cdot r \bmod n$
- (3) For $i = t - 1$ down to 0
- (4) $\bar{\theta} = \text{MM}(\bar{\theta}, \bar{\theta})$
- (5) if $e_i = 1$, then $\bar{\theta} = \text{MM}(\bar{\gamma}, \bar{\theta})$
- (6) $\theta = \text{MM}(\bar{\theta}, 1)$
- (7) return θ

ALGORITHM 3: The Montgomery exponentiation

number of sensor devices to CC. In the secure statistics reading phase, CC decrypts the statistical report and calculates the quadratic mean and variance of each dimension. Finally, CC gets all the arithmetic mean, quadratic mean, weighted mean, and variance without knowing the total number of sensor devices. Furthermore, to achieve the improvement in aggregation performance, we present three modified Montgomery exponentiation algorithms. Using these algorithms, EPPSA avoids frequent conversion of exponentiation results between the Montgomery domain and residue domain.

4.1. Modified Montgomery Exponentiation Algorithms. We modified Algorithm 3 to improve the aggregation performance. Three modified algorithms below map the result of modular exponentiation into the Montgomery domain.

4.1.1. Modified Montgomery exponentiation 1. The modified Montgomery exponentiation method 1 (MME1) is described in Algorithm 4.

Compared with Algorithm 3, Algorithm 4 removes the step $\theta = \text{MM}(\bar{\theta}, 1)$, which converts the result into the correct domain z_n^* . This denotes that the exponentiation result is still in the Montgomery domain. The result of exponentiation is denoted by $\bar{\theta}$ to be distinguished from the one in Algorithm 3.

4.1.2. Modified Montgomery Exponentiation 2. The modified Montgomery exponentiation method 2 (MME2) is described in Algorithm 5.

Compared with Algorithm 3, Algorithm 5 removes the step $\bar{\gamma} = \text{MM}(\gamma)$ and $\theta = \text{MM}(\bar{\theta}, 1)$. The base number and result of Algorithm 5 are both in the Montgomery domain and are denoted by $\bar{\gamma}$ and $\bar{\theta}$, respectively, to be distinguished from the ones in Algorithm 3.

4.1.3. Modified Montgomery Exponentiation 3. The modified Montgomery exponentiation method 3 (MME3) is described in Algorithm 6.

Compared with Algorithm 3, Algorithm 6 removes the step $\bar{\gamma} = \text{MM}(\gamma)$. The base number of Algorithm 6 is in the Montgomery domain and is denoted by $\bar{\gamma}$ to be distinguished from the one in Algorithm 3.

Using these algorithms, encrypted data are converted to the Montgomery domain at the beginning of the process during the process. Then encrypted data are kept in the Montgomery domain for further computation. In the end, the results are reconverted back to the residue (non-Montgomery) domain. By reducing the conversions between the Montgomery domain and the residue domain, the aggregation operation can be accelerated.

4.2. System Initialization. In the proposed system model, we assume that there are m SDs in WSN, which are denoted by D_i , ($1 \leq i \leq m$). Each device D_i generates an l -dimensional data vector $\bar{d}_i = (d_{i,1}, d_{i,2}, \dots, d_{i,j}, \dots, d_{i,l})$. Each D_i gets an identity ID_i and EA gets an identity ID_{EA} . The data in a region can be denoted by a matrix

$$D = \begin{bmatrix} d_{1,1} & \cdots & d_{1,l} \\ \vdots & \ddots & \vdots \\ d_{m,1} & \cdots & d_{m,l} \end{bmatrix}. \quad (3)$$

Given secure parameters κ and κ_1 , TA initializes the parameters of the additive homomorphic encryption algorithm and digital signature algorithm. The key generation procedure is shown as follows:

(i) Input: γ, e, n , where n' is computed by the extended Euclidean algorithm.
 Output: $\bar{\theta}$

- (1) $\bar{\gamma} = \gamma \cdot r \bmod n$
- (2) $\bar{\theta} = 1 \cdot r \bmod n$
- (3) For $i = t - 1$ down to 0
- (4) $\bar{\theta} = MM(\bar{\theta}, \bar{\theta})$
- (5) if $e_i = 1$, then $\bar{\theta} = MM(\bar{\gamma}, \bar{\theta})$
- (6) return $\bar{\theta}$

ALGORITHM 4: The modified Montgomery exponentiation 1 (MME1)

(i) Input: $\bar{\gamma}, e, n$, where n' is computed by the extended Euclidean algorithm.
 Output: $\bar{\theta}$

- (1) $\bar{\theta} = 1 \cdot r \bmod n$
- (2) For $i = t - 1$ down to 0
- (3) $\bar{\theta} = MM(\bar{\theta}, \bar{\theta})$
- (4) if $e_i = 1$, then $\bar{\theta} = MM(\bar{\gamma}, \bar{\theta})$
- (5) return $\bar{\theta}$

ALGORITHM 5: The modified Montgomery exponentiation 2 (MME2)

(i) Input: $\bar{\gamma}, e, n$, where n' is computed by the extended Euclidean algorithm.
 Output: θ

- (1) $\bar{\theta} = 1 \cdot r \bmod n$
- (2) For $i = t - 1$ down to 0
- (3) $\bar{\theta} = MM(\bar{\theta}, \bar{\theta})$
- (4) if $e_i = 1$, then $\bar{\theta} = MM(\bar{\gamma}, \bar{\theta})$
- (5) $\theta = MM(\bar{\theta}, 1)$
- (6) return θ

ALGORITHM 6: The modified Montgomery exponentiation 3 (MME3)

Step 1: TA chooses prime numbers p, q randomly, where $|p| = |q| = \kappa$. Let $n = pq$ and $\lambda = \text{lcm}(p - 1, q - 1)$. Choose g , with $g \in Z_{n^*}^*$, and the order of g is a multiple of n . Then, TA generates the encryption key (pk_{AHE}, sk_{AHE}) , where the encryption public key is $pk_{AHE} = (n, g)$ and decryption private key is $sk_{AHE} = (p, q, \lambda)$.

Step 2: TA chooses an Elliptic curve group Γ of an order q_1 with base point (generator) G , which is over the finite field Z_{p_1} of integers modulo a prime p_1 . The bit length of q_1 and p_1 should be set as the security parameter, that is, $|p_1| = |q_1| = \kappa_1$. For each SD_i ($1 \leq i \leq m$), TA chooses a secret key of digital signature $sk_{DS,i} \leftarrow Z_{q_1}$ randomly. TA sets the public key of the digital signature $pk_{DS,i} = sk_i \cdot G$. The signature key of SD_i is

$(pk_{DS,i}, sk_{DS,i})$. The signature keys of EA, CC, and TA are generated in the same way, which are denoted by $(pk_{DS,EA}, sk_{DS,EA})$, $(pk_{DS,CC}, sk_{DS,CC})$, and $(pk_{DS,TA}, sk_{DS,TA})$, respectively. The signature algorithm makes use of a hash function $H: \{0, 1\}^* \rightarrow Z_{q_1}$.

Step 3: Via a secure channel, TA sends the encryption public key pk_{AHE} and the signature private key $sk_{DS,i}$ to SD_i ($1 \leq i \leq m$). It sends the encryption public key pk_{AHE} , the signature public key $pk_{DS,i}$, and the signature private key $sk_{DS,EA}$ to EA. It sends the decryption private key sk_{AHE} and the signature public key $pk_{DS,EA}$ to CC.

After key generation, TA distributes the encryption keys and signing keys. The key distribution procedure is shown as follows:

Step 1: TA writes signature key pair $(pk_{DS,i}, sk_{DS,i})$ into the sensor device SD_i ($1 \leq i \leq m$) before deploying the sensor device. TA writes the signature public key $pk_{DS,i}$ and the signature key pair $(pk_{DS,EA}, sk_{DS,EA})$ into EA before deploying the edge device. TA sends the signature public key $pk_{DS,TA}$ and $pk_{DS,EA}$ to CC through the Internet and give the signature key pair $(pk_{DS,CC}, sk_{DS,CC})$ to CC by a USB key device.

Step 2: Using the private key $sk_{DS,TA}$, TA computes a digital signature on sk_{AHE} denoted by σ_{AHE} . Using CC's public key $pk_{DS,CC}$, TA generates a digital envelope on the Paillier private key sk_{AHE} and the signature σ_{AHE} denoted by σ_{DE} . TA sends the σ_{DE} to CC through the Internet.

Step 3: After receiving the digital envelope σ_{DE} , CC decrypts it and gets the Paillier private key sk_{AHE} and the signature σ_{AHE} . Using the public key $pk_{DS,TA}$, CC verifies the signature. If the verification is passed, the Paillier private key will be accepted.

4.3. Data Report Generation. Each sensor device SD_i , ($1 \leq i \leq m$), performs the following phases to get a data report:

(i) *Generate*: The SD_i firstly generates the raw data vector $d_i = (d_{i,1}, d_{i,2}, \dots, d_{i,j}, \dots, d_{i,l})$. Then SD_i calculates the corresponding quadratic data vector $d_i^2 = (d_{i,1}^2, d_{i,2}^2, \dots, d_{i,j}^2, \dots, d_{i,l}^2)$. Given a weight vector $w = (w_1, w_2, \dots, w_j, \dots, w_m)$, SD_i calculates the weighted data vector $d_{i,wei} = (d_{i,1,wei}, d_{i,2,wei}, \dots, d_{i,j,wei}, \dots, d_{i,l,wei})$ by $d_{i,j,wei} = d_{i,j} w_j$.

(ii) *Encrypt*: After generating the l -dimensional data vectors d_i, d_i^2 , and $d_{i,wei}$, sensor device SD_i encrypts the data using the Paillier encryption algorithm. When calculating the ciphertexts, EPPSA uses MME1 to convert the results to the Montgomery domain. These result of d_i, d_i^2 , and $d_{i,wei}$ are denoted by $\bar{c}_i = (\bar{c}_{i,1}, \dots, \bar{c}_{i,l})$, $\bar{c}_i^2 = (\bar{c}_{i,1}^2, \dots, \bar{c}_{i,l}^2)$, and $\bar{c}_{i,wei} = (\bar{c}_{i,1,wei}, \dots, \bar{c}_{i,l,wei})$, respectively.

(iii) *Sign*: Timestamp is denoted by TS , and the identity of SD_i is denoted by ID_i . SD_i chooses an instance key $k_i \leftarrow Z_{q_1}$. Calculate $(r_{x,i}, r_{y,i}) = k_i G$ and

$sig_i = (H(\overline{c_{i,1}} \parallel \dots \parallel \overline{c_{i,l}} \parallel \overline{c_{i,1}^2} \parallel \dots \parallel \overline{c_{i,l}^2} \parallel \overline{c_{i,1,wei}} \parallel \dots \parallel \overline{c_{i,l,wei}} \parallel TS \parallel ID_i) + sk_{DS,i} r_{x,i}) / k_i$. The signature is achieved by $\sigma_i = (sig_i \text{ mod } d_{q_1}, r_{x,i} \text{ mod } d_{q_1})$.

- (iv) *Send*: SD_i sends the data report $(\overline{c_i}, \overline{c_i^2}, \overline{c_{i,wei}}, \sigma_i, \text{timestamp}, ID_i)$ to EA.

4.4. Statistical Aggregation. After receiving the data $(\overline{c_i}, \overline{c_i^2}, \overline{c_{i,wei}}, \sigma_i, TS, ID_i)$ reported from m sensor devices, EA performs the following steps to generate the statistical aggregation report:

- (i) *Verify*: EA firstly calculates $(r'_{x,i}, r'_{y,i}) = G / (sig_i \cdot H(\overline{c_{i,1}} \parallel \dots \parallel \overline{c_{i,l}} \parallel \overline{c_{i,1}^2} \parallel \dots \parallel \overline{c_{i,l}^2} \parallel \overline{c_{i,1,wei}} \parallel \dots \parallel \overline{c_{i,l,wei}} \parallel \text{timestamp} \parallel ID_i) + pk_{DS,i} / sig_i \cdot r_{x,i})$. Then, EA checks the validity of $(\overline{c_i}, \sigma_i, \text{timestamp}, ID_i)$ by verifying the equation $r'_{x,i} \text{ mod } q_1 = r_{x,i} \text{ mod } q_1$.

- (ii) *Aggregate*: If the validity equation holds, EA executes the aggregation operations. EA firstly calculates the arithmetic sum, quadratic sum, and weighted sum of each dimension, which are denoted by $\overline{c_{j,\text{sum}}}$, $\overline{c_{j,q,\text{sum}}}$, and $\overline{c_{j,w,\text{sum}}}$, ($1 \leq j \leq l$), respectively. When calculating the sum, EA uses the *MM* method (Algorithm 3) for modular multiplication. Then EA calculates arithmetic mean, quadratic mean, and weighted mean of each dimension, which are denoted by $\overline{c_{j,\text{mea}}}$, $\overline{c_{j,q,\text{mea}}}$, and $\overline{c_{j,w,\text{mea}}}$, ($1 \leq j \leq l$), respectively. When calculating the mean by Equation 2, EA uses *MME2* (Algorithm 5) for modular exponentiation. The result is denoted by $\overline{c_{EA}} = (\overline{c_{1,\text{mea}}}, \dots, \overline{c_{l,\text{mea}}}, \overline{c_{1,q,\text{mea}}}, \dots, \overline{c_{l,q,\text{mea}}}, \overline{c_{1,w,\text{mea}}}, \dots, \overline{c_{l,w,\text{mea}}})$. The details of the aggregation are shown in Algorithm 7.

- (iii) *Sign*: Timestamp is denoted by TS , and the identity of EA is denoted by ID_{EA} . EA chooses an instance key $k_{EA} \leftarrow Z_{q_1}$. Calculate $(r_{x,EA}, r_{y,EA}) = k_{EA} G$ and $sig_{EA} = (H(\overline{c_{1,\text{mea}}} \parallel \dots \parallel \overline{c_{l,\text{mea}}} \parallel \overline{c_{1,q,\text{mea}}} \parallel \dots \parallel \overline{c_{l,q,\text{mea}}} \parallel \overline{c_{1,w,\text{mea}}} \parallel \dots \parallel \overline{c_{l,w,\text{mea}}} \parallel TS \parallel ID_{EA}) + sk_{EA} r_{x,EA}) / k_{EA}$. The signature is achieved by $\sigma_{EA} = (sig_{EA} \text{ mod } d_{q_1}, r_{x,EA} \text{ mod } d_{q_1})$.

- (iv) *Send*: EA sends the data report $(\overline{c_{EA}}, \sigma_{EA}, TS, ID_{EA})$ to CC.

4.5. Statistical Report Decryption. After receiving the data report $(\overline{c_{EA}}, \sigma_{EA}, TS, ID_{EA})$ reported from EA, EA performs the following steps to decrypt the statistical aggregation report:

- (i) *Verify*: EA firstly calculates $(r'_{x,EA}, r'_{y,EA}) = G / (sig_{EA} \cdot H(\overline{c_{1,\text{mea}}} \parallel \dots \parallel \overline{c_{l,\text{mea}}} \parallel \overline{c_{1,q,\text{mea}}} \parallel \dots \parallel \overline{c_{l,q,\text{mea}}} \parallel \overline{c_{1,w,\text{mea}}} \parallel \dots \parallel \overline{c_{l,w,\text{mea}}} \parallel TS \parallel ID_{EA}) + pk_{EA} / sig_{EA} \cdot r_{x,EA})$. The EA checks the validity of $(\overline{c_{EA}}, \sigma_{EA}, TS, ID_i)$ by verifying the equation $r'_{x,EA} \text{ mod } d_{q_1} = r_{x,EA} \text{ mod } d_{q_1}$.

- (ii) *Decrypt*: If the validity equation holds, CC executes the decryption operations using $d = D(c) = L(c^d \text{ mod } n^2) \text{ mod } n$. When calculating the decryption, CC uses the *MME3* (Algorithm 6) for modular exponentiation. The result is $(d_{1,\text{mea}}, \dots, d_{l,\text{mea}}, d_{1,q,\text{mea}}, \dots, d_{l,q,\text{mea}}, d_{1,w,\text{mea}}, \dots, d_{l,w,\text{mea}})$.

- (iii) *Reduce*: Considering that the decryption result of the mean may be a large integer with no sense, CC reduces each decryption result using Algorithm 2. CC takes elements in the decrypted data vector $(d_{1,\text{mea}}, \dots, d_{l,\text{mea}}, d_{1,q,\text{mea}}, \dots, d_{l,q,\text{mea}}, d_{1,w,\text{mea}}, \dots, d_{l,w,\text{mea}})$ and the modulus as inputs and gets the reduced data vector $(D_{1,\text{mea}}, \dots, D_{l,\text{mea}}, D_{1,q,\text{mea}}, \dots, D_{l,q,\text{mea}}, D_{1,w,\text{mea}}, \dots, D_{l,w,\text{mea}})$.

- (iv) *Post-Process*: The reduced data vector includes arithmetic mean, mean of square, and weighted mean of each dimension. For each dimension, CC calculates the quadratic mean $D_{j,Q\text{mea}}$ by equation (3) and variance $D_{j,\text{var}}$ by equation (4). Finally, CC gets the result of arithmetic mean, quadratic mean, weighted mean, and variance of each dimension, denoted by $(D_{1,\text{mea}}, \dots, D_{l,\text{mea}}, D_{1,Q\text{mea}}, \dots, D_{l,Q\text{mea}}, D_{1,w,\text{mea}}, \dots, D_{l,w,\text{mea}}, D_{1,\text{var}}, \dots, D_{l,\text{var}})$.

$$D_{j,Q\text{mea}} = \sqrt{D_{j,q\text{mea}}}, \quad (4)$$

$$D_{j,\text{var}} = D_{j,q\text{mea}} - (D_{j,\text{mea}})^2, \quad (5)$$

5. Security Analysis

In this section, we analyze the security properties of the proposed EPPSA scheme, following the security requirements and design goals given in Section 2.

Lemma 1. *The result of encryption in the Montgomery domain is a valid format of the ciphertext.*

Proof 1. The residue (non-Montgomery) system is a commutative ring denoted by R_n , and the Montgomery domain is a commutative ring denoted by R_n^M . The rings R_n and R_n^M are isomorphic by the isomorphism $h: R_n \rightarrow R_n^M$ defined by $h(a) = a \cdot 2^t \text{ mod } d n$ and $h^{-1}: R_n^M \rightarrow R_n$ defined by $h^{-1}(a) = a \cdot 2^{-t} \text{ mod } d n$. Due to the isomorphism, the result of encryption in the Montgomery domain is a valid format of the ciphertext. \square

5.1. Resistance to Eavesdropping Attack

Theorem 1. *WSN devices' private data and statistics cannot be obtained by an adversary α even if it is eavesdropped during transmitting.*

Proof 2. In the EPPSA scheme, the data are encrypted by the Paillier cryptosystem. According to Lemma 1, the result of encryption $c_{i,j} = g^{d_{i,j}} r^n \text{ mod } n$ in the Montgomery domain is

- (i) Input: Vectors $\overline{c}_i = (\overline{c}_{i,1}, \dots, \overline{c}_{i,l}, \overline{c}_{i,1}^2, \dots, \overline{c}_{i,l}^2, \overline{c}_{i,1,wei}, \dots, \overline{c}_{i,l,wei})$, where $1 \leq i \leq m$.
 Output: Ciphertext of arithmetic mean, mean of square, and weighted mean in the Montgomery domain of each dimension, denoted by $\overline{c}_{j,mea}$, $\overline{c}_{j,qmea}$, and $\overline{c}_{j,wmea}$, ($1 \leq j \leq l$).
- (1) $\overline{c}_{j,sum} = c_{i,1}, \overline{c}_{j,qsum} = c_{i,1}^2, \overline{c}_{j,wsum} = c_{i,1,wei}$, ($1 \leq j \leq l$)
 - (2) for $j = 1$ up to $j = l$
 - (3) for $i = 2$ up to $i = m$
 - (4) $\overline{c}_{j,sum} = MM(\overline{c}_{j,sum}, \overline{c}_{i,j})$,
 - (5) $\overline{c}_{j,mea} = MME2(\overline{c}_{j,sum}, m^{-1} \bmod n, n^2)$
 - (6) for $j = 1$ up to $j = l$
 - (ii) for $i = 2$ up to $i = m$
 - (8) $\overline{c}_{j,qsum} = MM(\overline{c}_{j,qsum}, \overline{c}_{i,j}^2)$,
 - (9) $\overline{c}_{j,qmea} = MME2(\overline{c}_{j,qsum}, m^{-1} \bmod n, n^2)$
 - (10) for $j = 1$ up to $j = l$
 - (11) for $i = 2$ up to $i = m$
 - (12) $\overline{c}_{j,wsum} = MM(\overline{c}_{j,wsum}, \overline{c}_{i,j,wei})$,
 - (13) $\overline{c}_{j,wmea} = MME2(\overline{c}_{j,wsum}, m^{-1} \bmod n, n^2)$
 - (14) return $\overline{c}_{EA} = (\overline{c}_{1,mea}, \dots, \overline{c}_{l,mea}, \overline{c}_{1,qmea}, \dots, \overline{c}_{l,qmea}, \overline{c}_{1,wmea}, \dots, \overline{c}_{l,wmea})$

ALGORITHM 7: Statistical aggregation

a valid format of the ciphertext. Meanwhile, the private key sk_{AHE} is transmitted to CC in digital envelope. The sk_{AHE} is encrypted by CC's public key $pk_{DS,CC}$ so that α cannot get it. Since Paillier cryptosystem is provably secure against the chosen plaintext attack based on the decisional Diffie–Hellman problem, α cannot guess the plaintext in a nonnegligible probability without the private key sk_{AHE} . Similarly, α cannot obtain statistics by eavesdropping on the transmission between EA and CC. In a word, the data and statistics in transmission are semantically secure. \square

5.2. Resistance to Replay Attack

Theorem 2. *If a replayed data report is transmitted to EA, or a statistical report to CC, it can be detected.*

Proof 3. If an adversary α replays the data report $(\overline{c}_{re}, \sigma_{new}, TS_{new})$ to aggregator EA, it needs to forge a new timestamp donated by $timestamp_{new}$. Since the timestamp is new, α has to forge a new signature σ_{new} of the replayed ciphertext \overline{c}_{re} . The security of the ECDSA system is based on the computational intractability of the discrete logarithm problem (DLP). The signature key pair $(pk_{DS,i}, sk_{DS,i})$ is written to SD_i directly when system initialization. Thus, α cannot guess the correct signature of the replayed report in a nonnegligible probability without the private key $sk_{DS,i}$. Similarly, the replay attack of the statistical report to CC can be detected for the same reason. In a word, the EPPSA scheme is resistant to replay attack. \square

5.3. Resistance to Manipulation Attack

Theorem 3. *If an adversary α manipulates the data report from WSN sensor device or statistics from EG, it can be detected.*

Proof 4. It is assumed that an adversary α manipulates the encrypted data $\overline{c}_i = (\overline{c}_{i,1}, \dots, \overline{c}_{i,l}, \overline{c}_{i,1}^2, \dots, \overline{c}_{i,l}^2,$

$\dots, \overline{c}_{i,l,wei}, \dots, \overline{c}_{i,l,wei})$ s during the transmission to aggregator EA. When receiving the data report, EA calculates the hash value $H(\overline{c}_{i,1} \parallel \dots \parallel \overline{c}_{i,l} \parallel \overline{c}_{i,1}^2 \parallel \dots \parallel \overline{c}_{i,l}^2 \parallel \overline{c}_{i,1,wei} \parallel \dots \parallel \overline{c}_{i,l,wei} \parallel TS \parallel ID_i)$ and checks the signature σ_i by verifying the equation $r_{x,i}' \bmod q_1 = r_{x,i} \bmod q_1$. If \overline{c}_i is manipulated, the hash value will be incorrect and the signature will not be validated. Similarly, when receiving statistical report from EA, CC calculates the hash value $H(\overline{c}_{1,mea} \parallel \dots \parallel \overline{c}_{l,mea} \parallel \overline{c}_{1,qmea} \parallel \dots \parallel \overline{c}_{l,qmea} \parallel \overline{c}_{1,wmea} \parallel \dots \parallel \overline{c}_{l,wmea} \parallel TS \parallel ID_{EA})$ and checks the signature σ_i by verifying the equation $r_{x,EA}' \bmod q_1 = r_{x,EA} \bmod q_1$. The statistical report is considered invalid if it is manipulated by α . In a word, the integrity of data and statistics can be satisfied. \square

5.4. Resistance to Internal Attack

Theorem 4. *If EA is an internal attacker which is curious about WSN devices' privacy data, it still cannot obtain the actual data of the devices.*

Proof 5. According to Lemma 1, the encrypted data from WSN sensor devices $\overline{c}_i = (\overline{c}_{i,1}, \dots, \overline{c}_{i,l}, \overline{c}_{i,1}^2, \dots, \overline{c}_{i,l}^2, \overline{c}_{i,1,wei}, \dots, \overline{c}_{i,l,wei})$ in the Montgomery domain is a valid format of the ciphertext. The aggregator EA does not have the private key to decrypt the ciphertext. \square

Theorem 5. *If CC is an internal attacker which is curious about the total number of WSN devices, it still cannot obtain the actual number of the devices.*

Proof 6. CC obtains the arithmetic mean, quadratic mean, and weighted mean by decryption and reduction. Also, CC calculates the variance by Equation (3), which uses plaintext of arithmetic mean and quadratic mean. In a word, CC does

TABLE 1: Aggregation computation complexity of MMDA and EPPSA.

Scheme	Computation complexity
EPPSA	$(m-1) \cdot T_{MM}$
[28]	$(m-1) \cdot T_{OMM}$
[31]	$(m-1) \cdot T_{OMM}$
[33]	$(m-1)T_{MM} + T_{ME}$

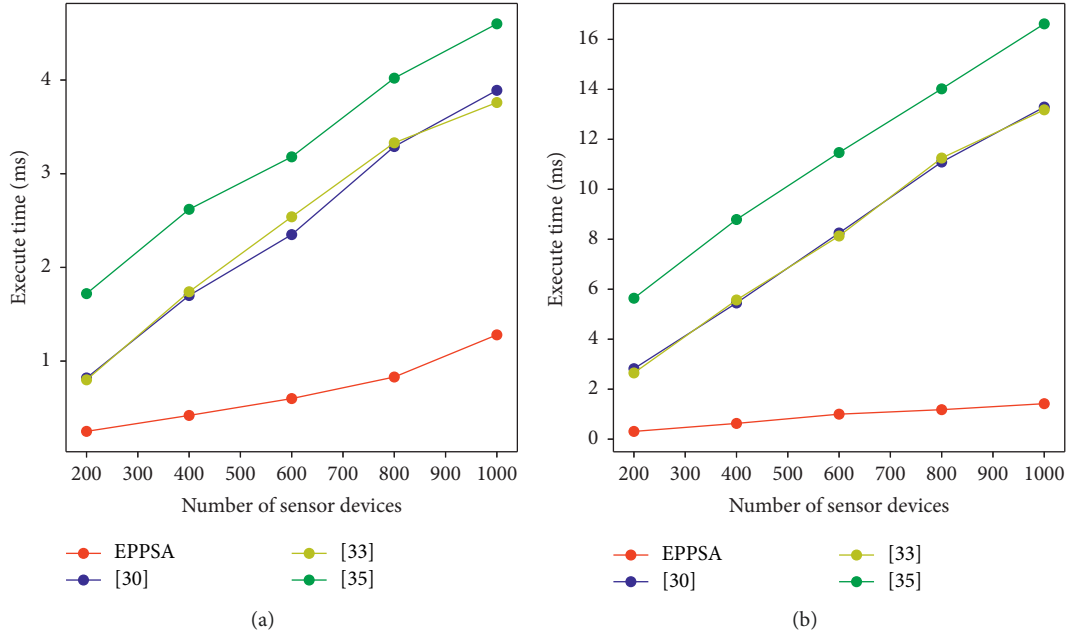


FIGURE 2: Comparison of aggregation computation costs: (a) comparison of aggregation computation cost on 1024 bits and (b) comparison of aggregation computation cost on 2048 bits.

not get any information on the total number of WSN devices when calculating statistics. \square

6. Performance Evaluation and Comparison

In this section, our scheme is evaluated in terms of computation costs and communication costs. The performance results are compared with the scheme proposed in references [28, 31, 33, 36].

6.1. Computation Cost. Assume that there are m sensor devices SD_i in the system and each of them reports an l -dimensional data vector for both our EPPSA scheme and schemes in [28, 31, 33]. For the fairness of comparison, these schemes are assumed to get moduli with the same bit length.

In our EPPSA scheme, the modified Montgomery exponentiations (Algorithms 4, 5, and 6) are used to keep the result of exponentiation in the Montgomery domain. That means the aggregation in EA only needs Montgomery multiplications. Let T_{MM} and T_{OMM} be the time cost of a Montgomery multiplication operation and an ordinary modular multiplication operation, respectively. And time

cost of a Montgomery exponentiation is denoted by T_{ME} . In our proposed EPPSA scheme, benefitting from the modified Montgomery exponentiations, $(m-1) \cdot T_{MM}$ is needed. In [28], the aggregation of each dimension is calculated by $(m-1) \cdot T_{OMM}$. In [31], the aggregation of each dimension is calculated by $(m-1) \cdot T_{OMM}$. In [33], the cost of aggregation is $(m-1) \cdot T_{MM} + T_{ME}$. A comparative summary of computation cost for m SDs aggregation is listed in Table 1.

To evaluate the performance, we execute the experiments on a Laptop with Windows 10 OS, Intel® Core™ i5-700U 2.50 GHz and 16 GB RAM. And we utilize the OpenSSL library (OpenSSL 1.1.1 h) to provide basic cryptographic primitives. For the evaluation of the EPPSA scheme, we set the n to be 512 and 1024 bits in the Paillier Cryptosystem, and the n^2 to be 1024 and 2048 bits. As the number of dimensions changes, we get the comparison of aggregation computation costs of 1024 bits in Figure 2(a), and the computation costs of 2048 bits in Figure 2(b). In summary, Figure 2 clearly shows that compared with schemes in [28, 31, 33], EPPSA has the smallest computation cost. For example, compared with [28], the EPPSA scheme gets 62.5% aggregation performance improvement on 1024 bits.

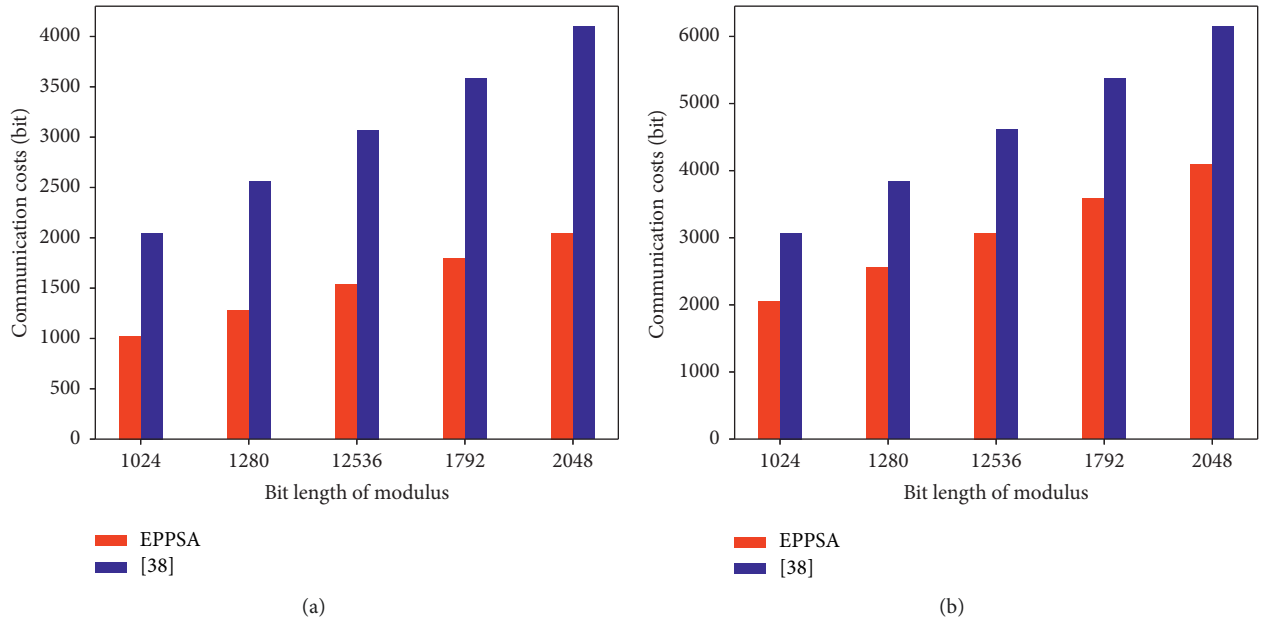


FIGURE 3: Comparison of communication cost: (a) comparison of communication cost on arithmetic mean and (b) comparison of communication cost on variance.

6.2. Communication Cost. Among the previous edge-aided aggregation schemes, the scheme in [36] is the only one that offers statistical functions. Therefore, we compare the communication costs of the EPPSA scheme with the scheme in [36]. We consider the communication costs of arithmetic mean and variance for fairness. For the sake of instruction, we denote the bit length of the modulus by L .

In [36], EA needs to transmit the aggregated ciphertext of summation and counter to CC for arithmetic mean, in which the communication cost is $2L$. In our EPPSA scheme, EA needs to send aggregated ciphertext of arithmetic mean to CC, in which the communication cost is L . In [36], EA needs to transmit the aggregated ciphertext of summation, quadratic summation, and counter to CC for variance, in which the communication cost is $3L$. In our EPPSA scheme, EA needs to send aggregated ciphertext of arithmetic mean and quadratic mean to CC, in which the communication cost is $2L$. Figure 3 shows the communication cost comparison of EPPSA and [36] in different bit lengths. It can be demonstrated that the communication cost of the EPPSA scheme decreases by 50% on arithmetic mean and 33% on variance.

7. Conclusion

In this article, we present an efficient privacy-preserving statistical aggregation scheme for edge computing-enhanced WSNs. The EPPSA scheme adopts the Paillier encryption scheme and ECDSA signature algorithm to guarantee data confidentiality, authentication, and data integrity. Compared with the existing multidimensional and multifunctional data aggregation schemes, the EPPSA scheme improves the efficiency of aggregation and decreases the communication load. Furthermore, the EPPSA scheme

improves privacy protection by hiding the total number of devices in the data report. The EPPSA scheme can be applied in various WSN scenarios, such as smart factory, health care, and environmental monitoring.

Data Availability

The data used in the experiments will be available upon request.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this article.

Acknowledgments

This work was supported by the Key Research and Development Program of Shandong Province (the Major Scientific and Technological Innovation Project of Shandong Province) under Grant no. 2020CXGC010114.

References

- [1] M. Assim and A. Al-Omary, "Design and Implementation of Smart home Using WSN and IoT Technologies," in *Proceedings of the 2020 International Conference On Innovation And Intelligence For Informatics, Computing And Technologies (3ICT)*, pp. 1–6, Sakheer, Bahrain, December 2020.
- [2] H. Gao, C. Liu, and Y. Yin, "A hybrid approach to trust node assessment and management for VANETs cooperative data communication: historical interaction perspective," *IEEE Transactions on Intelligent Transportation Systems*, 2021.
- [3] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy, "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular

- ad hoc networks,” *Cluster Computing*, vol. 20, no. 3, pp. 2439–2450, 2017.
- [4] P. Vijayakumar, V. Chang, L. J. Deborah, B. Balusamy, and P. G. Shynu, “Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks,” *Future Generation Computer Systems*, vol. 78, pp. 943–955, 2018.
- [5] X. Ge, J. Yu, H. Zhang, J. Bai, J. Fan, and N. N. Xiong, “SPPS: a search pattern privacy system for approximate shortest distance query of encrypted graphs in IIoT,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, 2021.
- [6] B. Wang, X. Gu, and S. Yan, “STCS: A practical solar radiation based temperature correction scheme in meteorological WSN,” *International Journal of Sensor Networks*, vol. 28, no. 1, pp. 22–33, 2018.
- [7] A. Zainuri, R. Yuwono, S. R. Arief, and M. Ghadafi, “Performance of temperature and humidity sensors with WSN mesh topology,” *Advanced Science Letters*, vol. 25, no. 1, pp. 70–74, 2019.
- [8] N. Sivakumar, “Minimizing transmission loss using inspired ant colony optimization and Markov chain Monte Carlo in underwater WSN environment,” *Journal of Ocean Engineering and Science*, vol. 4, no. 4, pp. 317–327, 2019.
- [9] Y. Yin, Z. Cao, Y. Xu, H. Gao, R. Li, and Z. Mai, “QoS prediction for service recommendation with features learning in mobile edge computing environment,” *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 4, pp. 1136–1145, 2020.
- [10] Y. Huang, H. Xu, H. Gao, R. Li, and Z. Mai, “SSUR: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center,” *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 670–681, 2021.
- [11] Y. Zhu, W. Zhang, Y. Chen, and H. Gao, “A novel approach to workload prediction using attention-based LSTM encoder-decoder network in cloud environment,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, p. 274, 2019.
- [12] X. Ma, H. Xu, H. Gao, and M. Bian, “Real-time Multiple-Workflow Scheduling in Cloud Environments,” *IEEE Transactions on Network and Service Management(TNSM)*, vol. 18, 2021.
- [13] X. Gao, J. Yu, Y. Chang, H. Wang, and J. Fan, “Checking only when it is necessary: enabling integrity auditing based on the keyword with sensitive information privacy for encrypted cloud data,” *IEEE Transactions on Dependable and Secure Computing*, 2021.
- [14] D. Mishra, D. Dharminder, P. Yadav, Y. S. Rao, P. Vijayakumar, and N. Kumar, “A provably secure dynamic ID-based authenticated key agreement framework for mobile edge computing without a trusted party,” *Journal of Information Security and Applications*, vol. 55, Article ID 102648, 2020.
- [15] X. Liu, J. Yu, F. Li, W. Lv, Y. Wang, and X. Cheng, “Data aggregation in wireless sensor networks: from the perspective of security,” *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6495–6513, 2020.
- [16] R. Li, C. Sturtivant, J. Yu, and X. Cheng, “A novel secure and efficient data aggregation scheme for IoT,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1551–1560, 2018.
- [17] H. Gao, Y. Zhang, H. Miao, R. J. D. Barroso, and X. Yang, “SDTIOA: Modeling the Timed Privacy Requirements of IoT Service Composition: A User Interaction Perspective for Automatic Transformation from BPEL to Timed Automata,” *Mobile Networks and Applications*, vol. 26, 2021.
- [18] H. Gao, X. Qin, R. J. D. Barroso, W. Hussain, Y. Xu, and Y. Yin, “Collaborative learning-based industrial IoT API recommendation for software-defined devices: the implicit knowledge discovery perspective,” *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2020.
- [19] C. Li, R. Lu, H. Li, L. Chen, and J. Chen, “Pda: a privacy-preserving dual-functional aggregation scheme for smart grid communications,” *Security and Communication Networks*, vol. 8, no. 15, pp. 2494–2506, 2015.
- [20] H. Bao and L. Chen, “A lightweight privacy-preserving scheme with data integrity for smart grid communications,” *Concurrency and Computation: Practice and Experience*, vol. 28, no. 4, pp. 1094–1110, 2016.
- [21] K. Alharbi and X. Lin, “Lpda: a lightweight privacy-preserving data aggregation scheme for smart grid,” in *Proceedings of the International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–6, Huangshan, China, October 2012.
- [22] Z. Sui, M. Niedermeier, and H. de Meer, “RESA: A robust and efficient secure aggregation scheme in smart grids,” in *Proceedings of the Proceedings of the 10th International Conference on Critical Information Infrastructures Security*, pp. 171–182, Cham, May 2015.
- [23] J. Ni, K. Zhang, X. Lin, and X. S. Shen, “EDAT: efficient data aggregation without TTP for privacy-assured smart metering,” in *Proceedings of the 2016 IEEE International Conference on Communications (ICC)*, pp. 1–6, Kuala Lumpur, Malaysia, May 2016.
- [24] Y. Liu, W. Guo, C. I. Fan, L. Chang, and C. Cheng, “A practical privacy-preserving data aggregation (3PDA) scheme for smart grid,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1767–1774, 2018.
- [25] H. Wang, Z. Wang, and J. Domingo-Ferrer, “Anonymous and secure aggregation scheme in fog-based public cloud computing,” *Future Generation Computer Systems*, vol. 78, pp. 712–719, 2018.
- [26] 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.
- [27] H. Shen, M. Zhang, and J. Shen, “Efficient privacy-preserving cube-data aggregation scheme for smart grids,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1369–1381, 2017.
- [28] P. Zeng, B. Pan, K. K. R. Choo, and H. Liu, “MMDA: multidimensional and multidirectional data aggregation for edge computing-enhanced IoT,” *Journal of Systems Architecture*, vol. 106, Article ID 101713, 2020.
- [29] X. Liu, Y. Zhang, B. Wang, and H. Wang, “An anonymous data aggregation scheme for smart grid systems,” *Security and Communication Networks*, vol. 7, no. 3, pp. 602–610, 2014.
- [30] Z. Guan, Y. Zhang, L. Wu et al., “APPA: an anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT,” *Journal of Network and Computer Applications*, vol. 125, pp. 82–92, 2019.
- [31] X. Wang, Y. Liu, and K. K. R. Choo, “fault-tolerant multi-subset aggregation scheme for smart grid,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4065–4072, 2020.
- [32] A. Mohammadali and M. S. Haghghi, “A privacy-preserving homomorphic scheme with multiple dimensions and fault tolerance for metering data aggregation in smart grid,” *IEEE*

- Transactions on Smart Grid*, vol. 12, no. 6, pp. 5212–5220, 2021.
- [33] Y. Zhang, J. Chen, H. Zhou, and L. Dang, “A privacy-preserving data aggregation scheme with efficient batch verification in smart grid,” *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 15, no. 2, pp. 617–636, 2021.
- [34] Y. Guo, N. Wang, Z. Y. Xu, and K. Wu, “The internet of things-based decision support system for information processing in intelligent manufacturing using data mining technology,” *Mechanical Systems and Signal Processing*, vol. 142, Article ID 106630, 2020.
- [35] P. Zhang, J. Wang, K. Guo, F. Wu, and G. Min, “Multi-functional secure data aggregation schemes for WSNs,” *Ad Hoc Networks*, vol. 69, pp. 86–99, 2018.
- [36] C. Peng, M. Luo, P. Vijayakumar, D. He, O. Said, and A. Tolba, “Multi-functional and multi-dimensional secure data aggregation schemes in WSNs,” *IEEE Internet of Things Journal*, vol. 9, 2021.
- [37] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in *Proceedings of the 17th International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 223–238, Berlin, Heidelberg, April 1999.
- [38] *ISO/IEC 18033-6:2019, IT Security Techniques, Encryption Algorithms Homomorphic Encryption* (British Standard), 2019, <https://www.iso.org/standard/67740.html>.
- [39] M. Shah, W. Zhang, H. Hu, and N. Yu, “Paillier cryptosystem based mean value computation for encrypted domain image processing operations,” *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 15, no. 3, pp. 1–21, 2019.
- [40] S. Gueron, “Efficient software implementations of modular exponentiation,” *Journal of Cryptographic Engineering*, vol. 2, no. 1, pp. 31–43, 2012.
- [41] R. K. Kodali, “Implementation of ECDSA in WSN,” in *Proceedings of the 2013 International Conference On Control Communication And Computing (ICCC)*, pp. 310–314, IEEE, Thiruvananthapuram, India, December 2013.

Research Article

Multiagent Reinforcement Learning for Task Offloading of Space/Aerial-Assisted Edge Computing

Yanlong Li,^{1,2,3,4} Lei Liang,^{1,2} Jielin Fu ,^{1,2} and Junyi Wang^{1,2}

¹College of Information and Communication, Guilin University of Electronic Technology, Guilin, Guangxi 541004, China

²Key Laboratory of Cognitive Radio Information Processing of the Ministry of Education, Guilin University of Electronic Technology, Guilin, Guangxi 541004, China

³Optical Communications Laboratory, Ocean College, Zhejiang University, Zhoushan, Zhejiang 316021, China

⁴Ocean Research Center of Zhoushan, Zhejiang University, Zhoushan, Zhejiang 316021, China

Correspondence should be addressed to Jielin Fu; fujielin@gmail.com

Received 17 December 2021; Revised 14 January 2022; Accepted 21 March 2022; Published 2 May 2022

Academic Editor: Yuyu Yin

Copyright © 2022 Yanlong Li 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 task offloading in space-aerial-ground integrated network (SAGIN) has been envisioned as a challenging issue. In this paper, we investigate a space/aerial-assisted edge computing network architecture considering whether to take advantage of edge server mounted on the unmanned aerial vehicle and satellite for task offloading or not. By optimizing the energy consumption and completion delay, we formulate a NP-hard and non-convex optimization problem to minimize the computation cost, limited by the computation capacity and energy availability constraints. By formulating the problem as a Markov decision process (MDP), we propose a multiagent deep reinforcement learning (MADRL)-based scheme to obtain the optimal task offloading policies considering dynamic computation request and stochastic time-varying channel conditions, while ensuring the quality-of-service requirements. Finally, simulation results demonstrate the task offloading scheme learned from our proposed algorithm that can substantially reduce the average cost as compared to the other three single agent deep reinforcement learning schemes.

1. Introduction

The current in-depth development of fifth generation (5G) and beyond 5G technology is envisioned to build an interconnected world opening up to everyone. The increasing number of various ultradense heterogeneous Internet of things (IoT) devices and the continuous improvement of application requirements have put forward higher requirements for data transmission rate and network coverage [1, 2]. Compared with a fixed terrestrial network, the advantages of versatility, manoeuvrability deployment, as well as seamless coverage make space-air-ground integrated network (SAGIN) an emerging hot research topic [3, 4]. Meanwhile, mobile edge computing (MEC) is a promising approach to improve the quality of service (QoS) and network performance [5].

Therefore, the MEC technology of the terrestrial network is introduced in SAGIN to provide efficient and flexible

computing services by utilizing multilevel and heterogeneous computing resources at the edge of network. Especially, in the case of cellular base station damaging by natural disaster or the case of special senses (e.g., mountainous areas, polar regions, and oceans), UAVs and low earth orbit (LEO) satellite constellation can act as aerial relays or stations, and ground users (GUs) can offload computation tasks for fast processing [6]. In general, cooperative communication by multiple UAVs can be a possible solution to reduce the offloading delay and extend UAVs' service lifetime [7]. However, there introduces more challenging issues to minimizing offloading delay while employing the multiple UAV architecture.

Recently, task offloading has been studied extensively, and task offloading processes are generally modeled as mixed integer programming problems [8], solutions such as heuristic algorithms [9, 10], and convex relaxation [11, 12]. However, these optimization methods require a large

number of iterations to reach a satisfactory local optimum, which makes them unsuitable for real-time offloading decisions when environmental conditions change rapidly and significantly [13, 14]. Meanwhile, deep reinforcement learning (DRL) has been widely used as an effective approach to optimize different problems including offloading policy, which can help overcome the prohibitive computational requirements [15].

The research on task offloading of space/aerial-assisted edge computing has been at its initial stage. In the SAGIN, various single-agent DRL-based task offloading schemes are proposed to maximize the network utility or minimize the computation cost [16]. Considering the limited capacity of MEC server and channel conditions of UAVs, reference [17] proposed a computation offloading scheme based on deep Q-learning network (DQN) to solve the dynamic scheduling problem, and reference [18] adopted a risk-aware reinforcement learning algorithm using actor-critic architecture to minimize the weighted sum of delay and energy consumption. Furthermore, reference [19] proposed a joint resource allocation and task-scheduling methods based on a distributed reinforcement learning algorithm to achieve the optimal partial offloading policy. Reference [20] adopted a deep deterministic policy gradient (DDPG)-based computation offloading scheme to solve high-dimensional state space and continuous action space. Multiagent reinforcement learning (MARL) has been applied in different problems such as path planning [21], dynamic resource allocation [22], and channel access [23]. Compared with single-agent reinforcement learning methods, distributed multiagent systems undoubtedly have better performance. However, the study on task offloading considering the cooperation of space, aerial, and ground multilayer network under multi-UAV multiuser environment is still missing in above research studies. None of above references take full advantage of a possible collaborative framework, but only used multiple parallel deep neural network and decisions are taken independently by each agent of the system. In this paper, a MARL-based method is proposed to solve the cooperative task offloading issue in the space/aerial-assisted edge network. The multiple agents can achieve the offloading optimization collaboratively, in order to reduce the cost of computation tasks. In particular, our main contributions of this work are as follows:

- (1) Different from traditional UAV-enabled MEC task offloading scheme, we design a space/aerial assisted edge network for dynamic task offloading in a cooperative environment with multi-UAV.
- (2) This paper considers the problem of computation offloading under the SAGIN architecture with the joint communication and computing (C2) service. We formulate the above-mentioned problem as a Markov decision process to minimize the computational cost. We assume each agent shares information with other agents and makes a decision according to current strategies and local real-time observations to select which component of the system to execute.

- (3) We propose a multiagent deep deterministic policy gradient (MADDPG)-based task offloading approach. Unlike other DRL algorithms such as Q-learning and DQN which restrict the agent actions to a low-dimensional finite discrete space, the agents in MADDPG can search the best action in an independent consecutive action space and maximize the long-term reward to reduce the computation cost by finding optimal strategy. Furthermore, MADDPG can be decentralized executed once the network has been centralized trained.

The remainder of this paper is organized as follows. In Section 2, the space/serial-assisted edge network architecture and task offloading models are introduced. Section 3 describes the problem formulation and the MADDPG-based solution. The simulation results and analysis are presented in Section 4. Finally, this work is concluded in Section 5.

2. System Model and Problem Formulation

2.1. Network Architecture. As shown in Figure 1, a remote region without cellular coverage is considered; therefore, we provide network access, edge computing, and caching through the aerial segment. We consider a space/aerial-assisted edge computing framework, which consists of N ground users (GUs), I UAVs and, a low earth orbit (LEO) satellite constellation. Figure 1 depicts a multi-UAV, multicomputational node (satellite with remote cloud server, UAV as an aerial MEC server) to provide services to GUs, and let $\mathbf{N} = \{1, 2, \dots, N\}$ be the set of GUs. The SAGIN components that tasks can be offloaded to are denoted by $\mathbf{I} = \{0, 1, 2, \dots, I\}$, where indexes $1, 2, \dots, I$ and 0 denote UAVs and the LEO satellite constellation, respectively. Considering a discrete time-slotted system with equal slot duration τ . Furthermore, we assume that the overall system has M tasks, denoted by the set $\mathbf{M} = \{1, 2, \dots, M\}$. The main parameters of this paper are shown in Table 1.

The GU can either execute the computation task locally or offload it to edge server in two ways. Each GU n can determine whether or not to offload its computing task to the edge server k , and let $x_{nmi}(t)$ denote the task offloading decision of task m of GU n . Specifically, $x_{nmi}(t) = 1$ means that the GU n offloads the task m to the edge server k , and $x_{nmi}(t) = 0$ means that the GU n disposes its task locally. There exists constraint (1) indicating the binary constraint of offloading decision:

$$x_{nmi}(t) \in \{0, 1\}. \quad (1)$$

2.2. Computation Model. Without the loss of generality, a tuple (ϕ, γ) is adopted to model the computing tasks from GU devices, where ϕ (in bits) represents the size of computation task, and γ (in CPU cycles per bit) indicates the computing workload means that how many CPU cycles are required to process one bit input data [17]. The delay and energy consumption of downloading can be ignored when the computing results are transmitted back to the GUs by the edge server because the key point of policy is task uploading

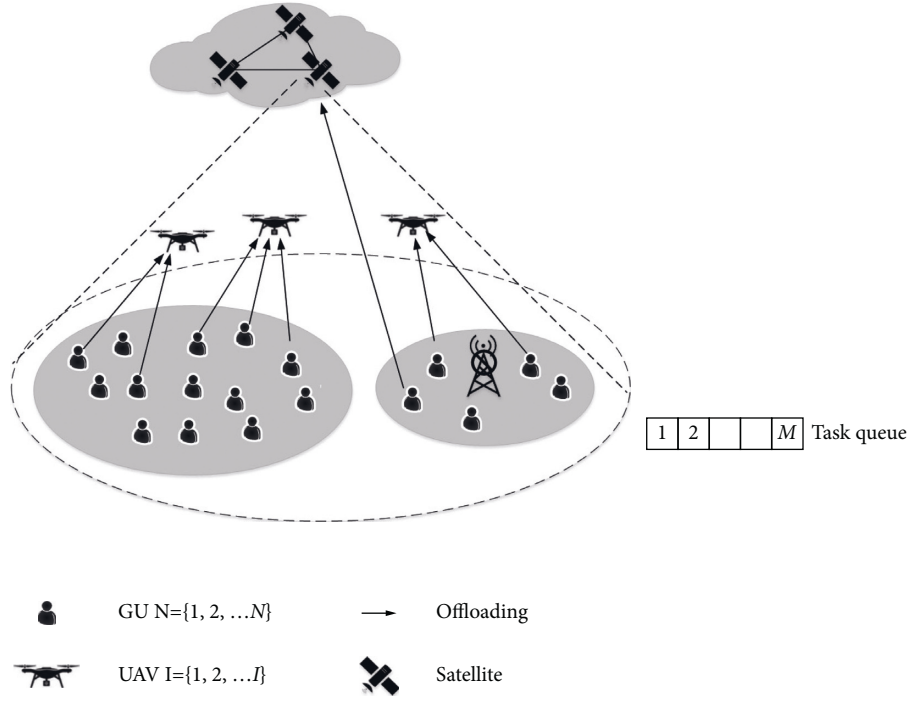


FIGURE 1: The network model.

TABLE 1: Notation.

N	Number of GUs
I	Number of UAVs
M	Number of initial offloaded tasks
T	Number of time slot needed to finish offloading
$\mathbf{X}[t] = [x_{nmi}(t)]$	Offloading indication matrix of GUs at time slot t
$f^i, i \neq 0$	Computation Capacity of UAVs
f^0	Computation Capacity of Satellite
f_n	Computation Capacity of GUs
ϕ	Data size (in bits)
γ	Computing workload (in CPU cycles per bit)
$d_n^{e,exec}, d_n^{l,exec}$	Computational cost of all SAGIN components
$d_n^{l,wait}$	Queuing time
$\rho_n(t)$	Remained computation tasks at time t
e_n^l	Local execution energy consumption
$P_{n,i}$	Transmission power
B_i	Bandwidth
N_0	Noise power
H	Channel gain of GU to satellite
PL	Path loss of GU n to UAV i
r_n^i	Transmission rate of GU n to UAV i or satellite
$d_{n,i}^{tran}$	Transmission delay
e_n^c	Communication-related energy consumption
ψ	Discount factor
δ	Soft update factor
$\mu(s \theta^u)$	Actor online with parameter θ^u and input s
$\mu^t(s \theta^{u'})$	Actor target with parameter $\theta^{u'}$ and input s
$Q(\mathbf{S}^{all}, \mathbf{A}^{all} \theta^Q)$	Critic online with parameter θ^Q and $(\mathbf{S}^{all}, \mathbf{A}^{all})$
$Q^t(\mathbf{S}^{all}, \mathbf{A}^{all} \theta^{Q'})$	Critic target with $\theta^{Q'}$ and $(\mathbf{S}^{all}, \mathbf{A}^{all})$
Z	Minibatch size
\mathbb{B}	Replay buffer
$\Delta\mu$	Action random noise

in the considered scenario [9, 24]. In the following, we consider the computation overhead in terms of completion delay and energy consumption for edge computing and local execution.

2.2.1. Edge Computing Model. The computing capability (in CPU cycles per second, the clock frequency of the CPU chip) of edge servers mounted on UAVs and satellite is denoted by f^i ($i \in \{1, 2, \dots, I\}$) and f^0 , respectively. Consequently, the computational cost of all SAGIN components can be calculated as the following equation:

$$d_n^{e,exec}(t) = \sum_{m=1}^{M_t} \sum_{i=0}^I \frac{x_{nmi}(t)\phi\gamma}{f^i}. \quad (2)$$

2.2.2. Local Computing Model. Since the limited computing capability of GUs, we assume that the remaining tasks wait to be processed in the queue. The delay of local processing is the sum of the computation execution time and the queuing time. The local execution time of GU n is given by

$$d_n^{l,exec}(t) = \frac{\sum_{m,i} (1 - x_{nmi}(t))\phi\gamma}{f_n}, \quad (3)$$

while the queuing time is calculated as

$$d_n^{l,wait}(t) = \max \left\{ \rho_n(t) - \left\lfloor \frac{f_n \tau}{\phi\gamma} \right\rfloor - \sum_{m=1}^M \sum_{i=0}^I x_{nmi}(t), 0 \right\} \tau, \quad (4)$$

where $\rho_n(t) \in [0, M_{\max}]$ denotes the unaccomplished computation task at the beginning of time slot, M_{\max} is the maximum length of the computing queue, $\lfloor \cdot \rfloor$ denotes the

floor function, and f_n is the computing capability of GU n . The local execution energy consumption is given by

$$e_n^l(t) = \xi_n \cdot \sum_{m,i} (1 - x_{nmi}(t)) \phi \gamma f_n^2, \quad (5)$$

where ξ_n denotes the effective switched capacitance for the chip architecture [25]. Clearly, the f_n can be adjusted to achieve the optimum computation time and energy consumption by using the DVFS [8].

2.3. Communication Model. Since UAVs and satellites use different frequency bands to communicate, we suppose that there is no interference between UAVs and satellite in this work [26]. Meanwhile, we neglect the propagation delay from GU devices to the UAVs because we assume that the UAV is sufficiently close to GU devices [27]. The aerial to ground communication channel depends on the altitude, angle of elevation, and type of propagation environment [28]. Based on reference [16], the average path loss of the aerial to ground channel can be defined as

$$PL(r, h) = 20 \log \left(\frac{4\pi f_c (h^2 + r^2)^{1/2}}{c} \right) + P_{LoS} \eta_{LoS} + (1 - P_{LoS}) \eta_{NLoS}, \quad (6)$$

where P_{LoS} represents the line of sight (LoS) connection probability between GU n and UAV i , and h , r , η_{LoS} , η_{NLoS} denote the UAV flying altitude, horizontal distance between the UAV and the GU, and the additive loss incurred on top of the free space path loss for line-of-sight and not-line-of-sight links [29], respectively. We set the altitude of the UAV to 10m. f_c denotes the carrier frequency, and c denotes the velocity of light. According to [19], the values of $(\eta_{LoS}, \eta_{NLoS})$ are (0.1, 2.1) in remote area. Adopting the Weibull-based channel model [30], we generate the channel gain when $x_{nm0}(t) \neq 0$, which can be given by=

$$H = \frac{G_{tx} G_{rx} \lambda^2}{(4\pi l_{sat})^2} 10^{-F_{rain}/10}, \quad (7)$$

where G_{tx} and G_{rx} are antenna gains, F_{rain} denotes the rain attenuation, and l_{sat} denotes the distance between GU and the satellite. Consequently, the data rate denoted by $r_i(t)$ is calculated by

$$r_n^i(t) = \begin{cases} B_i \log_2 \left(1 + \frac{P_{ni}(t) \cdot |H|^2}{\sigma_S^2} \right), & i = 0, \\ B_i \log_2 \left(1 + \frac{P_{ni}(t) \cdot 10^{-(PL/10)}}{\sigma_U^2} \right), & i \neq 0, \end{cases} \quad (8)$$

where P_{ni} indicates the transmission power, B_i denotes the channel bandwidth of the aerial-ground link and the ground-satellite link, indexes $1, 2, \dots, I$, and 0 denotes the UAV swarm and the LEO satellite constellation, respectively. σ_S and σ_U represent the noise power. In line with mentioned

earlier, we can define the transmission delay for task off-loading over aerial-assisted computing as

$$d_{n,i}^{tran}(t) = \begin{cases} \sum_{m=1}^M \left(\lceil x_{nm0}(t) \rceil d_{sat} + \left(\frac{x_{nmi}(t) \phi}{r_n^i(t)} \right) \right), & i = 0, \\ \sum_{m=1}^M \frac{x_{nmi}(t) \phi}{r_n^i(t)}, & i \neq 0, \end{cases} \quad (9)$$

where d_{sat} denotes the propagation delay between the LEO satellite and GUs, which cannot be ignored. While the communication-related energy consumption can be defined as

$$e_n^i(t) = P_{ni} d_{n,i}^{tran}(t). \quad (10)$$

2.4. Problem Formulation. In line with the computation model and communication model, the computation cost can be defined as the weighted sum of completion delay and energy consumption for completing all tasks of GU n . Generally, the completion delay is the sum of the local execution time, the queuing time, the computational delay of all SAGIN components, and the transmission delay, which is defined as

$$D_n(t) = d_n^{l,exec}(t) + d_n^{l,wait}(t) + d_n^{e,exec}(t) + \sum_{i=0}^I d_{n,i}^{tran}(t), \quad (11)$$

while the energy consumption is given by

$$E_n(t) = e_n^l(t) + \sum_{i=0}^I e_n^i(t), \quad (12)$$

Consequently, the computational cost of GU n in space/aerial-assisted network can be calculated as

$$C_n(t) = \omega_n^1 D_n(t) + \omega_n^2 E_n(t), \quad (13)$$

where ω_n^1 and ω_n^2 denote the weights for the energy consumption and the completion delay, respectively, which can be regarded as the trade-off between delay and energy consumption. We can adjust the weights to meet different user demands by using this form of computational cost. Notably, the weights can be further divided into local execution model and edge computing model to increase diversity among these cases. We formulate the optimization problem in our scenario to minimize the computational cost. Therefore, the optimization problem is given by

$$\begin{aligned} & \min_X \lim_{T \rightarrow \infty} \frac{1}{T} \sum_{t=1}^T \omega_n^1 D_n(t) + \omega_n^2 E_n(t) \\ & \text{s.t. } x_{nmi}(t) \in \{0, 1\}, \forall n \in \mathbf{N}, \forall m \in \mathbf{M}, \forall i \in \mathbf{I}, \\ & \sum_{i=0}^I x_{nmi}(t) \in [0, 1], \forall n \in \mathbf{N}, \forall m \in \mathbf{M}, \\ & \sum_{m=0}^{M_i} \sum_{i=0}^I x_{nmi}(t) \leq M_{\max}, \forall n \in \mathbf{N}. \end{aligned} \quad (14)$$

3. MARL for Task Offloading

3.1. MARL Framework. Since above optimization problem in (14) is non-convex and NP hard, we adopt a multiagent reinforcement learning approach to achieve the feasible solution. In this section, we model the formulated optimization problem as a Markov decision process (MDP) [31], and the purpose of action selection is to maximize the reward function. In the space/aerial-assisted network environment, each GU acts as an agent, chooses an action, and then receives the reward at time slot t . The state space, action space, and reward function are described as follows.

3.1.1. State Space. The state $s_n(t) \in \mathbf{S}$ consists of the channel vectors, the task size randomly generated in the time slot t , the unaccomplished task queue, and the remaining energy. These quantities change over time because of the impact of single and combined actions of this system, so we define the state in our scenario as

$$s_n(t) = \{h_t^n, \phi_n^{CPR}, \rho_t^n, E_t^n\}. \quad (15)$$

3.1.2. Action Space. Based on current state $s_n(t)$ and other agents' experience, each agent is supposed to select its action to schedule the computation tasks. Formally, we define the vector $a_n(t) = \{x_{nmi}(t), \forall n \in \mathbf{N}, \forall m \in \mathbf{M}, \forall i \in \mathbf{I}\}$ as the binary offloading decision, where $x_{nmi}(t) \in \{0, 1\}$ indicates that GU n whether to offload its task m to the MEC server i or not. The constraints of the problem (14) are considered as the binary offloading decision strategy, and computation is offloaded to at most one node at time slot t .

3.1.3. Reward Function. In line with reinforcement learning, each agent can select its own action in a decentralized execution to maximize the global reward. The agent's choice is based on the reward function, which specifies the goal of the algorithm. With the objective of long-term weighted sum of delay and energy consumption of all tasks, we define a function to minimize the computation cost as follows:

$$R_n(t) = - \left[\lim_{T \rightarrow \infty} \frac{1}{T} \sum_{t=1}^T C_n(t) |s_n(t) \right]. \quad (16)$$

Let π denotes the stationary policy, and a value function is defined to determine the value of reward, which is given by

$$V_n(s, \pi) = \mathbb{E} \left[\sum_{t=0}^{\infty} \psi R_n(s_t^n, a_t^n) | s_t^n = s, \pi \right], \quad (17)$$

where $\psi \in [0, 1]$ denotes the discounting factor, which refers to the cumulative utility. The overall reward of all agents at time slot t can be calculated as

$$R(t) = \sum_{n=1}^N R_n(t), \forall n \in \mathbf{N}. \quad (18)$$

The main objective is to minimize the computation cost in the space/aerial-assisted network. We denote the group of

GUs' optimal strategies as $\pi^* = \{\pi_1^*, \pi_2^*, \dots, \pi_n^*\}$. We maximize the long-term reward as

$$\pi^* = \arg \max_a \mathbb{E}_{\pi} \left[\sum_{t=1}^{\infty} \lambda^{t-1} R(t) \right], \quad (19)$$

where the π_n^* can be expressed as

$$V_n(s, \pi_n^*, \pi_{-n}^*) \leq V_n(s, \pi_n, \pi_{-n}^*), \quad (20)$$

where π_n and $\pi_{-n}^* = \{\pi_1^*, \dots, \pi_{n-1}^*, \pi_{n+1}^*, \dots, \pi_N^*\}$ denote the set of all possible strategies taken by GU n and other agents' strategies, respectively. Therefore, the MADRL algorithm can obtain the optimal policy through convergence.

3.2. MADDPG-Based Task Offloading Scheme. In this section, the MADDPG [32]-based task offloading scheme is proposed to derive the near-optimum decision by optimizing the continuous variable \mathbf{X} . MADDPG not only retains the greatest advantages of DDPG that can consider continuous action space but also solves the shortcomings of Q-learning or policy gradient algorithms that are not suitable for the multiagent environment by extending the DDPG algorithm into a multiagent domain.

As shown in Figure 2, the MADDPG framework is carried out by centralized training and distributed execution. Each GU has a critic and an actor as agent n , critic n can choose the appropriate action a_n according to the observation s_n , and actor n would evaluate the action a_n based on the global observation \mathbf{S}^{all} . During the training procedure, each actor n collects the policies of other agents and denotes them as \mathbf{A}^{all} . In our MADDPG architecture, the actor is trained to generate a deterministic policy, the critic is trained to evaluate the actor, and the experience replay buffer \mathbb{B} is denoted to effectively avoid the correlated action, which can store the minibatches of samples $(s, a, R, s') \sim U(\mathbb{B})$. The random minibatch size of samples can be denoted by Z .

In the MADDPG algorithm, each agent selects an optimal action $a_n^k = \mu(s_n^k | \theta^\mu)$ as the output of actor network μ . The actor network can be updated in the form of gradient, which is given by

$$\nabla_{\theta^\mu} J \approx \mathbb{E}_{(s, a, R, s') \sim U(\mathbb{B})} \left[\left(\nabla_a Q(s, a | \theta^Q) \nabla_{\theta^\mu} \mu(s | \theta^\mu) \right) \right], \quad (21)$$

and the critic network Q is updated as the following expression:

$$L(\theta^Q) = \mathbb{E}_{\mathbf{S}^{all}, \mathbf{A}^{all}} \left[\left(Q(\mathbf{S}^{all}, \mathbf{A}^{all} | \theta^Q) - y \right)^2 \right], \quad (22)$$

where $y_n = R_t^n + \psi Q_\pi(\mathbf{S}^{all}, \mathbf{A}^{all} | \theta) |_{a_n^{k+1} = \mu'(s_n^{k+1})}$, a_n^{k+1} is the predication of the next action in target actor network. To minimize the policy gradient of agent n , the parameters are soft updated for both the target actor and networks as follows:

$$\begin{cases} \theta_n^{\mu'} \leftarrow \delta \theta_n^\mu + (1 - \delta) \theta_n^{\mu'} \\ \theta_n^{Q'} \leftarrow \delta \theta_n^Q + (1 - \delta) \theta_n^{Q'} \end{cases}, \quad (23)$$

where δ is the forgetting factor.

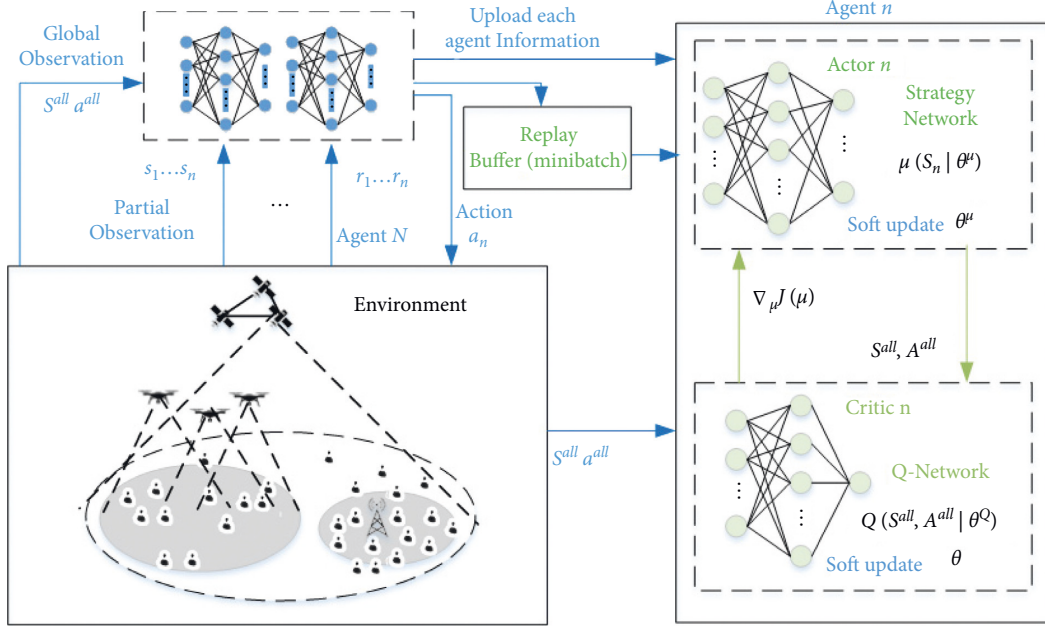


FIGURE 2: The MADDPG-based task offloading scheme.

The details of MADDPG-based task offloading scheme are shown in Algorithm 1. At first, we initialize four DNNs for each GU, i.e., critic network, actor network, and the two target networks (line 2-3). At the beginning of each episode, each GU obtains its observation state (line 7). Without the loss of generality, we divide each episode into T time slots. For each time slot, agents firstly select an action according to the current policy, and the noise is added into exploration (line 8-9). Afterward, all agents execute their actions, and each agent can receive the corresponding reward and the next state (line 10-11). Then, the experience tuple generated from the above iteration is stored into the replay buffer for parameter update (line 12). Finally, given the sampled minibatch of transitions from the replay buffer, each agent updates the parameter of the critic network by minimizing the loss value, updates the parameter of the actor network by gradient ascent, and updates the parameters of the target networks using (23) (line 15-17).

3.2.1. Analysis of Complexity. The deep neural network of the actor-critic framework can be represented as matrix multiplication. Let N and H define the dimension of output and the number of hidden layers, respectively. We can get the computational complexity between agents $O(N)$, and the complexity of each actor can be expressed as $O(HN^2)$. In our proposed algorithm, the training algorithms can be affected by the agent cost C_n , the number of training episodes K , and batch size Z . Therefore, the computational cost of critic networks and training procedure can be estimated as $O(C_n KN)$ and $O(C_n KZH N^2)$, respectively.

3.2.2. Analysis of Convergence. In the proposed algorithm, the gradient method is adopted to approximate the optimal by updating the weight of target networks. Obviously, the

parameters θ_n^μ and θ_n^Q will converge to a particular value after a finite number of iterations. Therefore, the convergence of our proposed algorithm can be guaranteed. Furthermore, the convergence can be observed through simulations.

4. Simulation Results

4.1. Simulation Settings. In this section, simulation is carried out to verify the proposed model and algorithm. Specifically, we begin by elaborating on the simulation settings. Afterwards, we present an evaluation on the experiment results. Simulation environment is implemented via Python 3.6 with TensorFlow 2.0 on a personal computer with a AMD R7-4800H CPU. ReLU function is used as the activation function after the fully connected layer, and L2 regularization is used to reduce DNN overfitting. The number of neurons in the two hidden layers are 256 and 128, and we set 2000 and 0.001 to the number of episode and learning rate. Other important constant parameters are listed in Table 2.

4.2. Convergence Analysis. To evaluate the performance of our proposed scheme, we further compare the convergence of three algorithms and the mean computation cost in the system. We adopt the other two benchmark schemes: DDPG [31] and DQN [18]. We first conducted a series of experiments to determine the optimal values of the hyperparameters used in the algorithm. The selection is based on the performance of the algorithm under different learning rates and discount factors. The convergence performance of the algorithm under different learning rates is shown in Figure 3. We can observe that the convergence speed will be reduced when the learning rate is too small, and generally, if the learning rate is too large, the algorithm will not converge normally.

```

(1) Initialization:
(2) Randomly initialize critic network  $Q(s, a | \theta_n^Q)$  and actor  $\mu(s, a | \theta_n^\mu)$  with weights  $\theta_n^Q$  and  $\theta_n^\mu$ 
(3) Initialize target network  $Q'$  and  $\mu'$  with weights  $\theta_n^{Q'} \leftarrow \theta_n^Q$  and  $\theta_n^{\mu'} \leftarrow \theta_n^\mu$ 
(4) Empty replay buffer  $\mathbb{B}$ 
(5) for episode  $k = 1, 2, \dots, K$  do
(6)   Initialize a Gaussian noise  $\Delta\mu$  with mean = 0;
(7)   Receive initial observation state  $\mathbf{S} = \{s_1, s_2, \dots, s_N\}$ ;
(8)   for time slot  $t = 1, 2, \dots, T$  do
(9)     Select action  $a_n(t) = \mu(s_t^\mu | \theta_n^\mu) + \Delta\mu$  according to the current policy and exploration noise  $\Delta\mu$ 
(10)    Execute action  $a_n(t)$  and observe the reward  $R_n$ , and the next state  $s_n(t+1)$ 
(11)    Collect the global state  $\mathbf{S}^{all}$ ,  $\mathbf{S}'^{all}$  and the action  $\mathbf{A}^{all}$ ;
(12)    Store transition  $(\mathbf{S}^{all}, \mathbf{A}^{all}, R_n(t), \mathbf{S}'^{all})$  in  $\mathbb{B}$ ;
(13)    Sample a random mini-batch of transitions  $\{(\mathbf{S}^{all}, \mathbf{A}^{all}, R_n(t), \mathbf{S}'^{all})\}_{z=1}^Z$  from  $\mathbb{B}$ ;
(14)    Set  $y_n = R_n + \psi Q_\pi(\mathbf{S}^{all}, \mathbf{A}^{all} | \theta) |_{a_n^{k+1} = \mu'(s_n^{k+1})}$ ;
(15)    Update the critic network  $Q(s, a | \theta_n^Q)$  by minimize the loss
       $L(\theta^Q) = 1/Z \sum_{z=1}^Z ((y_z - Q_\pi(s_z, \mathbf{A}^{all} | \theta_n^Q))^2)$ 
(16)    Update the actor policy by using the sampled policy gradient
       $\nabla_{\theta_n^\mu} J \approx 1/Z \sum_{z=1}^Z ((\nabla_a Q(\mathbf{S}^{all}, \mathbf{A}^{all} | \theta_n^Q) |_{a_z = \mu(s_z)}) \nabla_{\theta_n^\mu} \mu(\mathbf{S}^{all} | \theta_n^\mu))$ ;
(17)    Update the target networks for each agent  $n$ :
       $\theta_n^{\mu'} \leftarrow \delta \theta_n^{\mu'} + (1 - \delta) \theta_n^\mu$  and  $\theta_n^{Q'} \leftarrow \delta \theta_n^{Q'} + (1 - \delta) \theta_n^Q$ ;
(18)  end
(19) end

```

ALGORITHM 1: MADDPG algorithm for task offloading in SAGIN.

TABLE 2: Simulation parameters.

Parameter	Value
Number of GUs N	5
Number of UAVs I	4
Computation Capacity of UAVs $f^i, i \neq 0$	5 GC/s
Computation Capacity of Satellite f^0	10 GC/s
Computation Capacity of GUs f_n	200 MC/s
Data size ϕ	2 MB
Computing workload γ	25 cycles/bit
Transmission power $P_{n,i}$	[1.5, 5]W
Bandwidth B_i	[2, 3]MHz
Noise power N_0	-100 dBm
Discount factor ψ	0.99
Soft update factor δ	0.001

As shown in Figure 4, we show the convergence of our proposed algorithm on average reward with episodes, where the weight index of time delay $\omega^1 = 0.6$, and energy consumption weight index $\omega^2 = 1 - \omega^1$, and the results are averaged from ten numerical simulations, proving the effectiveness of neural networks. The average award values of MADDPG, DDPG, and DQN increase continuously until convergence. Obviously, the MADDPG algorithm become stable earlier than DDPG and DQN algorithms, and the other two schemes become stable after more than 400 training episodes. Moreover, the average reward of final convergence of the MADDPG algorithm is higher than the other two algorithms. Based on the simulation result, we conclude that the MADDPG algorithm outperforms the benchmark schemes in minimizing the long-term cost, which can reduce the wastage of resource by learn the policy of cooperation and maximize the global reward.

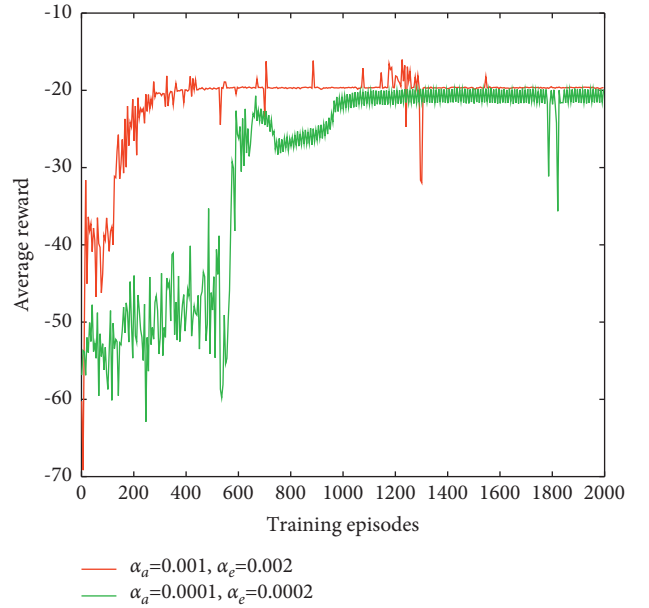


FIGURE 3: The convergence of the proposed algorithm under different learning states.

4.3. Average Cost. In this section, we discuss the average cost in terms of several number of GUs' devices and the size of offloading tasks. Figure 5 demonstrates the performance of proposed scheme and the three baselines in space/aerial-assisted network to minimize the average computation cost. We provide one other baseline: greedy algorithm [33], and each GU firstly makes its best effort to offload computation tasks, and then the remaining tasks will be processed locally.

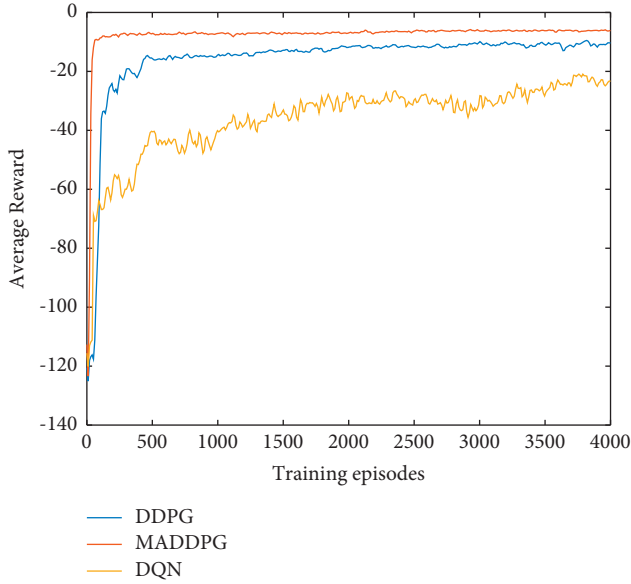


FIGURE 4: Comparison of the convergence under different algorithms.

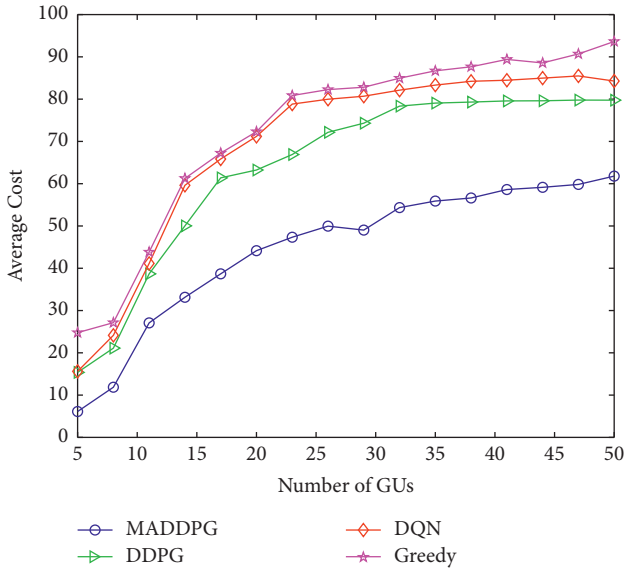


FIGURE 5: Average cost with number of GUs.

From Figure 5, we can observe that the average computation cost increases as the number of GUs' devices increasing. DQN algorithm, DDPG algorithm, and MADDPG algorithm all use deep reinforcement learning to automatically generate offloading strategies. According to the simulation results, the computation cost is reduced by the MADDPG algorithm, 29.066% compared to the DDPG algorithm, 36.392% compared to the DQN scheme, and 51.602% compared to the greedy scheme. Therefore, the proposed MADDPG scheme can still keep the computation cost lower than benchmark schemes, proving the validity of cooperative policy.

Figure 6 demonstrates the average cost under different sizes of offloading tasks. Obviously, the average cost increases as the size of offloading data size increases. This is

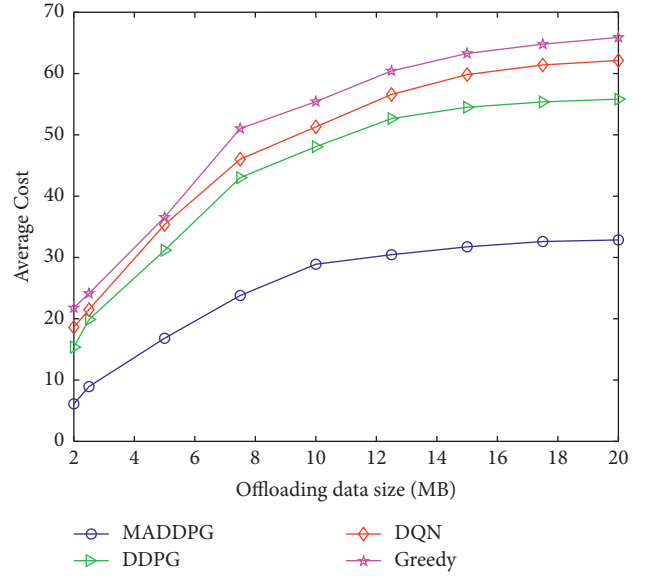


FIGURE 6: Average cost vs. different size of offloading tasks.

because each agent needs to unload a large amount of data, which increases the computational cost of the system. The proposed MADDPG scheme can obtain the best reward to minimize the computation cost than these benchmark schemes. The performance of strategies generated from the DQN algorithm and the DDPG algorithm is general in various scenarios, which is mainly because the training results of the two algorithms are unsuitable in multiagent environment. In contrast, MADDPG can effectively learn stable strategies by decentralized execution and centralized training. Therefore, we conclude that the MADDPG algorithm outperforms the three comparison algorithms in terms of different scenarios.

5. Conclusion

In this paper, an efficient task offloading scheme is proposed for the space/aerial-assisted edge computing system in SAGIN. Firstly, we elaborated the SAGIN architecture. Then, we express task offloading as a nonlinear optimization problem with the goal of minimizing the weighted sum of energy consumption and delay. On this basis, we propose an algorithm based on MADDPG to solve this problem. Finally, the simulation results show that the computation cost can be significantly saved by offloading the task to the edge server on the UAV or satellite, and the convergence performance and effectiveness of the proposed scheme in the simplified scenario are also proved by compared with three benchmark schemes.

In the future, we will further consider the mobility management of satellites and UAVs. In addition, the task offloading scheme of SAGIN in areas with rich computing resources is also worth for further study.

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 by the National Natural Science Foundation of China under grant (61761014), Guilin University of Electronic Technology Ministry of Education Key Laboratory of Cognitive Radio and Information Processing (CRKL190109).


References

- [1] Y. Xu, Y. Wu, H. Gao, S. Song, Y. Yin, and X. Xiao, "Collaborative apis recommendation for artificial intelligence of things with information fusion," *Future Generation Computer Systems*, vol. 125, pp. 471–479, 2021.
- [2] H. Gao, Xi Qin, R. J. D. Barroso, W. Hussain, Y. Xu, and Y. Yin, "Collaborative learning-based industrial iot api recommendation for software-defined devices: the implicit knowledge discovery perspective," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 6, no. 1, 2020.
- [3] Z. Zhang, Y. Xiao, Z. Ma et al., "6g wireless networks: vision, requirements, architecture, and key technologies," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 28–41, 2019.
- [4] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, "Space-air-ground integrated network: a survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2714–2741, 2018.
- [5] S. S. D. Ali, H. P. Zhao, and H. Kim, "Mobile edge computing: a promising paradigm for future communication systems," in *Proceedings of the TENCON 2018-2018 IEEE Region 10 Conference*, pp. 1183–1187, IEEE, Jeju, Korea (South), October 2018.
- [6] N. Cheng, W. Xu, W. Shi et al., "Air-ground integrated mobile edge networks: architecture, challenges, and opportunities," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 26–32, 2018.
- [7] A. Gao, Q. Qi, W. Liang, and Z. Ding, "Game Combined Multi-Agent Reinforcement Learning Approach for Uav Assisted Offloading," *IEEE Transactions on Vehicular Technology*, vol. 70, pp. 12888–12901, 2021.
- [8] A. Sacco, F. Esposito, M. Guido, and P. Montuschi, "Sustainable Task Offloading in Uav Networks via Multi-Agent Reinforcement Learning," *IEEE Transactions on Vehicular Technology*, vol. 70, 2021.
- [9] S. Bi and Y. J. Zhang, "Computation rate maximization for wireless powered mobile-edge computing with binary computation offloading," *IEEE Transactions on Wireless Communications*, vol. 17, no. 6, pp. 4177–4190, 2018.
- [10] T. X. Tran and D. Pompili, "Joint task offloading and resource allocation for multi-server mobile-edge computing networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 856–868, 2018.
- [11] X. Lyu, W. Ni, H. Tian et al., "Optimal schedule of mobile edge computing for internet of things using partial information," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2606–2615, 2017.
- [12] T. Q. Dinh, J. Tang, D. La Quang, and T. Q. S. Quek, "Offloading in mobile edge computing: task allocation and computational frequency scaling," *IEEE Transactions on Communications*, vol. 65, no. 8, pp. 3571–3584, 2017.
- [13] X. Ma, H. Xu, H. Gao, and M. Bian, "Real-time Multiple-Workflow," *Scheduling in Cloud Environment*, vol. 18, no. 4, 2021.
- [14] H. Gao, C. Liu, Y. Yin, Y. Xu, and Li Yu, "A hybrid approach to trust node assessment and management for vanets cooperative data communication: historical interaction perspective," *IEEE Transactions on Intelligent Transportation Systems*, 2021.
- [15] M. Min, L. Xiao, Y. Chen, P. Cheng, D. Wu, and W. Zhuang, "Learning-based computation offloading for iot devices with energy harvesting," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1930–1941, 2019.
- [16] A. M. Seid, G. O. Boateng, B. Mareri, G. Sun, and W. Jiang, "Multi-agent Drl for Task Offloading and Resource Allocation in Multi-Uav Enabled Iot Edge Network," *IEEE Transactions on Network and Service Management*, vol. 18, 2021.
- [17] C. Zhou, W. Wu, H. He et al., "Delay-aware iot task scheduling in space-air-ground integrated network," in *Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, IEEE, Waikoloa, HI, USA, December 2019.
- [18] C. Zhou, W. Wu, H. He et al., "Deep Reinforcement Learning for Delay-Oriented Iot Task Scheduling in Space-Air-Ground Integrated Network," 2020, <http://arxiv.org/abs/2010.01471>.
- [19] X. Cheng, F. Lyu, W. Quan et al., "Space/aerial-assisted computing offloading for iot applications: a learning-based approach," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 5, pp. 1117–1129, 2019.
- [20] Y. Wang, W. Fang, Y. Ding, and N. Xiong, "Computation offloading optimization for uav-assisted mobile edge computing: a deep deterministic policy gradient approach," *Wireless Networks*, vol. 27, no. 4, pp. 2991–3006, 2021.
- [21] Q. Han, D. Shi, T. Shen, X. Xu, Li Yuan, and L. Wang, "Joint optimization of multi-uav target assignment and path planning based on multi-agent reinforcement learning," *IEEE Access*, vol. 7, pp. 146264–146272, 2019.
- [22] J. Cui, Y. Liu, and A. Nallanathan, "The application of multi-agent reinforcement learning in uav networks," in *Proceedings of the 2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, IEEE, Shanghai, China, May 2019.
- [23] Z. Cao, P. Zhou, R. Li, S. Huang, and D. Wu, "Multiagent deep reinforcement learning for joint multichannel access and task offloading of mobile-edge computing in industry 4.0," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6201–6213, 2020.
- [24] H. Gao, Y. Zhang, H. Miao, R. J. D. Barroso, and X. Yang, "Sdtioa: modeling the timed privacy requirements of iot service composition: a user interaction perspective for automatic transformation from bpel to timed automata," *Mobile Networks and Applications*, vol. 26, pp. 1–26, 2021.
- [25] Q. Tang, Z. Fei, B. Li, and Z. Han, "Computation offloading in leo satellite networks with hybrid cloud and edge computing," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 9164–9176, 2021.
- [26] N. Zhang, H. Liang, N. Cheng, Y. Tang, J. W. Mark, and X. S. Shen, "Dynamic spectrum access in multi-channel cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 11, pp. 2053–2064, 2014.
- [27] W. Shi, J. Li, W. Xu et al., "Multiple drone-cell deployment analyses and optimization in drone assisted radio access networks," *IEEE Access*, vol. 6, pp. 12518–12529, 2018.
- [28] S. Chandrasekharan, K. Gomez, A. Al-Hourani et al., "Designing and implementing future aerial communication

- networks," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 26–34, 2016.
- [29] A. Al-Hourani, S. Kandeepan, and S. Lardner, "Optimal lap altitude for maximum coverage," *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 569–572, 2014.
- [30] S. A. Kanellopoulos, C. I. Kourogiorgas, A. D. Panagopoulos, S. N. Livieratos, and G. E. Chatzarakis, "Channel model for satellite communication links above 10ghz based on weibull distribution," *IEEE Communications Letters*, vol. 18, no. 4, pp. 568–571, 2014.
- [31] T. P. Lillicrap, J. J. Hunt, P. Alexander et al., "Continuous control with deep reinforcement learning," 2015, <http://arxiv.org/abs/1509.02971>.
- [32] R. Lowe, Yi Wu, Aviv Tamar, J. Harb, P. Abbeel, and I. Mordatch, "Multi-agent actor-critic for mixed cooperative-competitive environments," 2017, <http://arxiv.org/abs/1706.02275>.
- [33] F. Wei, S. Chen, and W. Zou, "A greedy algorithm for task offloading in mobile edge computing system," *China Communications*, vol. 15, no. 11, pp. 149–157, 2018.

Research Article

Comparison of Blackhole and Wormhole Attacks in Cloud MANET Enabled IoT for Agricultural Field Monitoring

**Tauqeer Safdar Malik,¹ Muhammad Nasir Siddiqui,¹ Muhammad Mateen,¹
Kaleem Razzaq Malik,¹ Song Sun,² and Junhao Wen ²**

¹Department of Computer Science, Air University Multan Campus, Multan 60000, Pakistan

²School of Big Data and Software Engineering, Chongqing University, Chongqing 401331, China

Correspondence should be addressed to Junhao Wen; jhwen@cqu.edu.cn

Received 10 November 2021; Revised 30 December 2021; Accepted 14 March 2022; Published 29 April 2022

Academic Editor: Yuyu Yin

Copyright © 2022 Tauqeer Safdar Malik 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 Mobile Ad hoc Network (MANET) enabled Internet of Things (IoT) agricultural field monitoring, sensor devices are automatically connected and form an independent network that serves as a cloud for many services such as monitoring, securing, and properly maintaining. Cloud-based services in MANET models can prove to be an extremely effective way of smart agricultural functionalities for device-to-device information exchange. Security is a serious issue with Cloud-MANET-based IoT since nodes are scattered, mobile, and lacking centralized administrator, which makes it possible for data tampering and illegal actions on cloud servers. Therefore, these types of networks are more vulnerable to Denial of Service (DoS) attacks such as Blackhole and Wormhole. The MANET Enabled IoT-Agricultural Field Monitoring environment is deployed through a case study. The effect of Blackhole and Wormhole attacks is analyzed using the Ad hoc On-demand Distance Vector (AODV) routing protocol with the help of Network Simulator 3 (NS-3) in order to determine which has the most impact on network performance. We computed performance constraints such as throughput, packet delivery ratio (PDR), end-to-end delay (EED), and Jitter-Sum of preprocessed data gathered with the flow-monitor module of NS-3. The effect of attacks on MANET Enabled IoT-Agricultural Field Monitoring is compared on the varying number of nodes participating in the Cloud-MANET-based IoT network. The throughput and goodput capability of every node is computed through the trace metric package. This method is also highly useful for future Cloud-MANET-Based IoT smart agricultural field security research.

1. Introduction

Cloud MANET-Based IoT is a smart devices platform that combines MANET, Cloud Computing, and IoT. This platform may connect to the cloud and provide cloud-based services to MANET customers by existing smart devices of the IoT system, which handles all the computing, data processing, and resource allocation. Inside the MANET coverage, IoT devices can circulate between one position to another to communicate and share information through cloud servers. Multiple MANETs may link with the same cloud and employ real-time cloud services. Connection of the IoT devices with mobile applications is required to link cloud-based MANET's smart devices to the cloud [1].

The connectivity between the smart devices does not rely on a centralized infrastructure for locating neighboring devices in IoT-MANET platform. The use of cloud-based resources in MANET model for device-to-device connectivity can be a very effective way to improve smart device abilities [2]. Users of smart devices can also use cloud services to reduce the amount of useable data within big data and process videos, text, audio, and images [2]. Farmers working in the agriculture sector can use the data obtained from the farming to analyze, monitor, and make a decision. Farmers may use mobile devices, sensors, and scanners to access a variety of cloud-based services for IoT devices working in MANET environment [3].

Mobile Ad hoc Network sets up a network with their neighbors' smart devices and transfers data to another device just like a router. MANET and Cloud computing make up the cloud-MANET platform for smart devices. This system will connect to and provide cloud resources to MANET users by the smart devices, which manages all calculations, management of resources, and data handling. Smart devices have the potential to switch between one place to another, and Multiple MANETs can link to a certain cloud and use run-time cloud services. To connect MANET's smart devices to the cloud, interconnection with mobile applications is required. The MANET framework of smart devices with local connectivity can perform best when connected to the cloud, but it fails when connected to an existing wired networking infrastructure. An entry point, equivalent to gateways, would be needed for operating in wireless and wired networks [4].

In order to join a smart device to some other device throughout the cloud-MANET network, each IoT smart device must have been uniformly equipped with resources such as memory, connectivity, and energy [5]. For routing purpose, cloud-based IoT devices linked to MANET nodes and IoT nodes in MANETs use MANET Routing Protocols. The IoT devices linked to MANET in cloud-based network for agricultural field monitoring must ensure the availability and connectivity at all times. The availability in terms of security is most important in monitoring application for an agricultural field, so that a farmer can get the real-time data collection and decision making. The cloud-based data servers can work very efficiently to ensure the availability of up-to-date information for real-time decision making [6]. Therefore, it is extremely important to implement a cloud MANET enabled IoT network for monitoring of agricultural field. The IoT nodes participating in cloud-based MANET for monitoring agricultural fields are much susceptible to availability attacks such as Denial of Service (DoS) attacks due to their very limited capability of memory, computing, and energy. The blackhole and wormhole attacks are very known and dangerous in DoS attacks on availability in MANET. The availability of real-time data is critical in case of monitoring of agricultural field on cloud MANET enabled IoT network. The data centers provide the best computing facility for any case of emergency, and IoT nodes in MANETs have been equipped with the Internet and low power and lossy network (LLN) topology, for routing protocol standard (RPL) [7]. The existing security and limited hardware resources in RPL are having deficiency in defense against numerous security attacks. Gateway routers linked with IoT devices in MANETs must be consistent and valid to protect MANET routing protocols and Internet routing protocols [8].

The communications in cloud-based MANET are carried through the different kind of reactive and proactive routing protocols such as Ad hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR) to find nearest path from source to destination node [9]. The cloud-based MANET is used in different fields such as in IoT, Industrial Internet of Things (IIoT), Medical Services, Security, Commercial, and Agriculture Sectors [10]. We used AODV

routing protocol that establishes a path from source node to destination node upon request in cloud MANET enabled IoT for monitoring of agricultural field. The physical manipulation like stealing or attacks by insects and animals, as well as modification in physical address or connection, makes smart devices defenseless in agricultural field monitoring solution based on cloud MANET enabled IoT. The different types of Denial of Service (DOS), congestion, and forwarding attacks can affect the common gateway, providing the services of cloud-based MANET to the end user [11]. The cloud-based MANET routing protocols are not secure, and therefore, the malicious node can find the drawbacks and attack on network, because sensor devices are widely dispersed, and they are vulnerable to malicious cyberattacks [12].

In this paper, we have simulated blackhole and wormhole attack to test the functionality of Cloud MANET enabled IoT for monitoring agricultural field with and without DoS attacks for monitoring the agricultural field as shown in Figure 1. On the base of performance metrics, the main contribution of this paper is to:

- (i) Compare the effect of blackhole and wormhole attacks on the performance of the Cloud MANET enabled IoT network for monitoring of agricultural field.
- (ii) Determine either blackhole attack or wormhole attack is more harmful and affecting the network performance of cloud MANET enabled IoT network.

To simulate results, we have utilized the Network Simulator-3 (NS-3), which is very famous as an open-source tool. Following the outcomes of the tests, we evaluated network performance by using metrics like average throughput, average end-to-end delay, average packet delivery ratio, and average jitter sum delay with reference to the total number of nodes within the network. We also have evaluated goodput and throughput of every node that are present in the network under with and without blackhole and wormhole attacks in cloud MANET enabled IoT network for agricultural field monitoring.

The rest of the paper is arranged as follows: the related work is discussed in the upcoming section for the literature review and effectiveness of the research. The material and methodology are followed by literature review in the next section with detailed graphical view and methodological model of Cloud MANET enabled IoT network for monitoring of an agricultural field. The next section discusses the simulation setup for varying number of IoT nodes participating in MANET enabled IoT network, followed by a complete section of results and analysis of the implemented setup. Finally, conclusion and recommendations for future work are given in last section.

2. Related Work

With the rapid deployment of Internet of Things (IoT) in the smart agriculture, it is modern and essential to cope it with future technology Cloud-based MANET. The innovation-driven architecture of cloud-based MANET is related to the

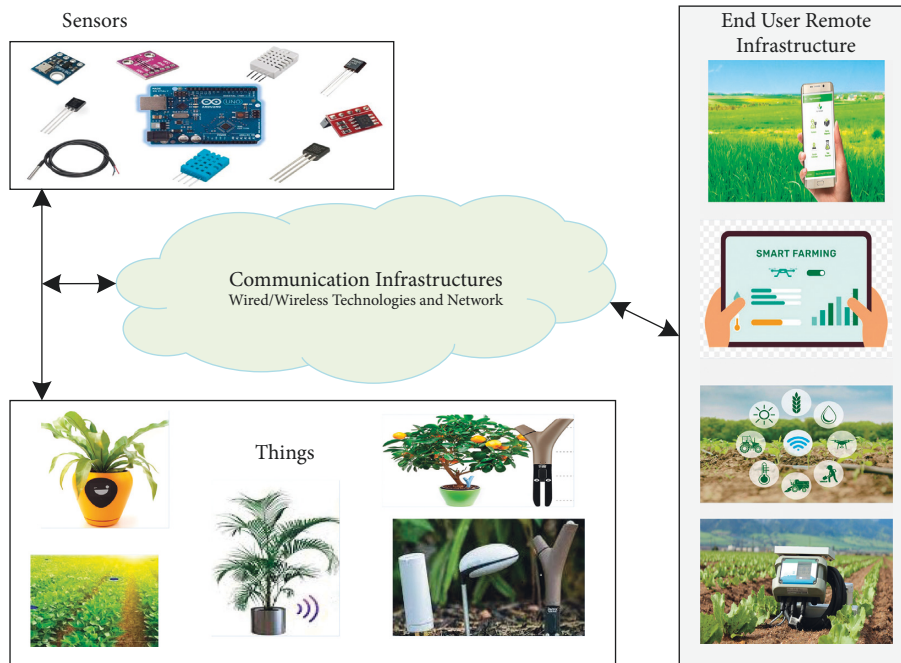


FIGURE 1: Graphical representation of agricultural field monitoring using MANET enabled IoT network.

monitoring solutions and is subject to security risks and privacy issues for an excessive number of IoT devices [13]. There are many solutions of Cloud-based MANET, which enable the agricultural monitoring solutions and highlights the dire need of IoT based devices to be equipped with these technologies. The cloud computing-based models such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) are heterogeneous in adopting the virtualization of different technologies [14]. Due to the heterogeneity and diversity of applications, especially the development and emergence of IoT, they offer more challenges and security threats in cloud environments [15]. Therefore, Cloud enabled MANET in Agricultural monitoring has massive data transmission on the network links, which not only affects the energy consumption in the cloud environment, but also increases the security risks. A cloud-based data center for MANET should facilitate the users with privacy and availability at all times while working in agricultural monitoring application. The cloud-based MANET should enable the user the better network configuration and availability of service at all times when monitoring any special task to ensure the services of the users especially in cyber-physical systems [16]. In the literature, there are various types of attacks discussed on availability in MANET, but there is still infancy to detect and prevent such attacks especially in cloud-based networks. The Denial of Service (DoS) attacks are very popular on availability and many solutions presented for its detection in MANET, and it is very important to analyze the effect of these attacks in cloud-based MANET especially in IoT devices. In [17], the authors presented a scenario of cooperative blackhole attack, one of the most dangerous DoS attacks, in Wireless Sensor Network (WSN) and MANET as a defenseless attack. A cooperative blackhole attack contains a

large number of malicious nodes working with trusted users, which affect the performance of IoT enabled MANET [18]. The security and privacy of IoT challenges should be verified by using formal methods, such as DoS, theorem-proving, and formal testing [19]. An algorithm for determining the safer path in case of blackhole attack between the sender and receiver is presented in [20] for secure and efficient communication by evaluating each route and channel, but this reliable path is for fixed locations.

Similarly, the detection of the wormhole attack not only reveals the Internet of Things (IoT) network, but also identifies the victim nodes undergoing remotely controlled [20]. There are other attacks too, such as Sybil attack, HELLO flood attack, sinkhole attack, and spoofing attack, which are caused by the wormhole attack. Therefore, the wormhole attack should be explored and simulated in the cloud-based MANET especially for IoT network, in which heterogeneous technologies were used, which could be causes of software and hardware exploitation. Later, in [21], the authors developed a system that focused on the variety of cyberattacks in IoT and Industrial IoT networks caused by blackhole attacks established on Routing Protocol for Low-power and Lossy Networks (RPL). The malevolent network nodes modify the path of packets and immediately send it through a different route than the one specified for the wormhole and blackhole nodes [22]. It may result in illegal data packet observation or even small amount of packet loss in IoT networks based on cloud [23]. This is known as a black hole attack when the Packet Delivery Ratio (PDR) exceeds a certain threshold, but the overall throughput of the network is not observed in cloud-based MANET.

In [24], the authors worked on MANET enabled IoT network and simulated the effects of Sybil attack in on network performance using routing protocol RPL. It can

first and foremost allow a dynamic scope of movement between nodes in the network, which is becoming increasingly important for real-time applications. But on the other hand, due to its resource constraints, RPL is extremely prone to numerous security attacks such as blackhole and wormhole attacks [25].

The IoT devices especially sensors are viewed as a significant security risk because of its modification that can be used as source nodes for DoS attacks [22]. Furthermore, there are many other resource limitations in cloud-MANET enabled IoT network such as less memory, conversation capacity, and minimum energy utilization to execute large and refined algorithms in IoT devices [26]. The safety and location for the position of information, as well as IoT empower location-based services used mostly for smart agriculture, are vulnerable to threats like device capturing [27]. An attacker can easily spoof an IoT device and retrieve the cryptographic design as well as having its uncontrolled usages to get all the information contained in the cache of device [28]. Extra demands for edge device functionalities may also be imposed in automation of IoT nodes for smart agricultural functionalities [29]. However, the significant risk that may be in agricultural as well as other industrial environment due to these weaknesses needs to be investigated more in the upcoming works [30].

The literature stated various levels of the IoT environment and highlighted many security concerns that must be researched and resolved. Inadequate protection may result in loss of data and violation of privacy and obtain raw data regarding on-field criteria and other important intellectual properties [31]. The DoS attacks, those that can come in the form of signal cancelling or jamming, are highly vulnerable to wireless links and put accessibility of a IoT device at risk in cloud-based MANET. Although spread spectrum techniques could be employed to prevent wireless jamming, there is still no feasible solution for preventing DoS attacks for IoT devices with limited resources [32].

Due to restricted memory, connectivity capacity, and low power consumption, complicated and refined algorithms are difficult to be incorporated in IoT devices [33]. The gateway can also be targeted by congestion, DoS, and routing attacks. Furthermore, cloud servers are vulnerable to data modification and unauthorized operations, which can disrupt operations in the agricultural farms. Session hijacking, server access control and database problems, and login misuse are some of the other security issues that can threaten cloud platform in the presence of DoS attacks [34]. Therefore, to secure the cloud MANET enabled IoT network from the DoS attacks such as blackhole and wormhole attacks in a limited resources of hardware and software, first of all, there must be a proper comparison of these attacks on network performance in monitoring of agricultural fields to prevent them. Hence, there is a need to check which DoS attack is more vulnerable for the overall performance of cloud MANET enabled IoT network for a limited capacity of IoT devices used in monitoring of agricultural fields.

3. Materials and Methods

The smart agricultural field monitoring is based on not only agricultural knowledge to support the deployment of a variety of intelligent applications, but also the expertise of the IoT devices, wireless technology, cloud computing, and intelligent systems. Figure 2 depicts the materials required to implement the cloud MANET enabled IoT network for monitoring of an agricultural field. IoT nodes are used as sensors to calculate weather, levels of soil moisture, temperature, soil fertility, and soil Ph level to assess whether each field has the best growing season and cultivation areas. The IoT devices are part of the network, performing different tasks in the agricultural field monitoring as shown in Figure 2. The attacker nodes are circled red in the network, which are causing the blackhole and wormhole attacks to make network unavailable for its services. Due to these attacks, the cloud-based MANET may not take the real-time decisions in case of unavailability. The data collection on cloud is delayed and partially received due to the blackhole and wormhole attack on IoT devices participating in monitoring of agricultural field. The cloud computing environment facilitates the traditional computing platforms to avoid the maintaining cost and investments in hardware by users, usually in terms of virtual machines. This new computing mode can enhance the efficiency, productivity, and scalability of increasingly more applications such as earthquake prediction, weather forecasting, and monitoring of smart agriculture. The diversity of IoT devices and its applications in smart agriculture brings more concerns and opportunities for real-time decision making in the cloud [16]. This is essential for gaining the most output of the production while minimizing loss of environmental resources [29]. As a result, different kinds of sensors are used in conjunction with other controller equipment to gather information in order to protect agricultural areas [30]. The Global Positioning System (GPS) is a space-based navigation system that offers a real-time features and positioning information across all weather conditions for monitoring. As a result, GPS helps farmers in increasing development and controlling land resources [31]. One of the really significant considerations in ensuring the efficiency of an agricultural commodity is the protection of such areas. Farmers can quickly implement video monitoring systems in their agricultural regions and provide consumers with really fresh and high-quality products at the end of the day, while securing livestock, vehicles, and services from damage and misuse. As a result, a web camera is an excellent tool for accomplishing this mission because it can catch photographs of any dangerous rodent within seconds when Infrared sensors sense motion [28]. The IoT nodes can communicate with the cloud servers directly or by a gateway, whereas digital images can be recorded by camera nodes through field cameras, drones, and sometimes satellite pictures. The connectivity of IoT nodes with the cloud servers is maintained for the purpose of remote visualization and smart application creation. Remote users may be using either workstations or/and smart devices to acquire the data and smart applications, which can be used to acquire the cloud

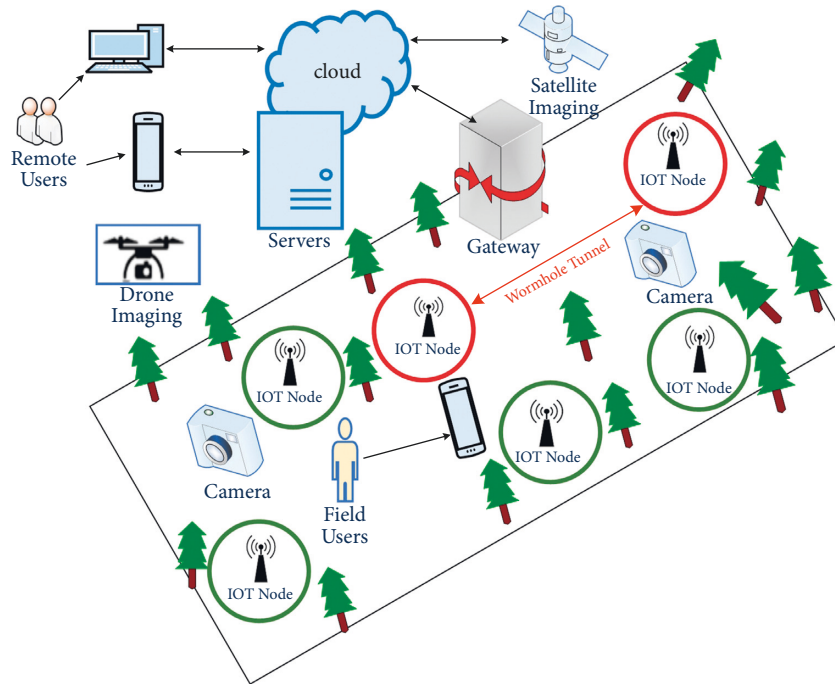


FIGURE 2: Cloud MANET enabled IoT Deployment for the Agricultural Field Monitoring.

for field users. Because of this, there is a possibility of different kind of attacks that not only destroy the overall network performance, but also make it unavailable for its services. The service of remote field monitoring of agricultural field requires the availability at all time and detects any malicious activity from the cloud-based MANET.

The state-of-the-art methodology is presented to implement and analyze the effect of blackhole and wormhole attacks in cloud MANET enabled IoT network for monitoring of an agricultural field. The enactment of blackhole and wormhole attacks in the MANET enabled IoT network requires modifying the working of existing Ad hoc On-demand Distance Vector (AODV) routing protocol. IoT Nodes are mobile in MANET, and AODV provides facility to these nodes to find route instantaneously that is necessary for communication. The effect of blackhole and wormhole attacks is simulated separately, and its detailed method is presented in the next subsections, respectively.

3.1. Blackhole Attack Execution in Cloud MANET Enabled IoT Network. The blackhole attack is the type of a Denial-of-Service (DoS) attack, and it affects the availability of a user by disrupting the network layer, which serves as routing purposes in cloud MANET enabled IoT network. An attacker node changes the normal behavior of routing protocol, and the victim node assumes that it has a valid route to transmit packets to destination. During the route-finding process, a source node broadcasts RREQ to all its neighboring nodes. When attacker node receives this request, it sends RREP message to source node with large sequence number and hop count 1 [35]. Upon reception of these packets by attacker node, it drops all the packets and does not forward them to

the destination IoT node as shown in Figure 3, which makes the data unavailable for cloud MANET.

IoT node S is the source node, and IoT node D is the destination node. The source node sends RREQ message to all its neighbors A, B, and C. The IoT Node B is an attacker node that sends RREP message to source node S by increasing sequence number and minimizing hop count earlier than IoT Node A and C. The source (victim) node S decides that node B (attacker node) provides valid/fast route to destination and sends data packets to it. Upon receiving packets, node B drops all the packets and does not forward them to the destination node D. Hence, the blackhole attacker makes the user unavailable to its services.

The blackhole attacks can be categorized as single and collaborative blackhole attacks. When one single node in the network acts as an attacker node to make unavailable the victim node as shown in Figure 3, it is categorized as single blackhole attack, whereas when more than one attacker node collaboratively attacks as shown in Figure 4, it is called collaborative blackhole attack [36].

Here, two attacker nodes B and C make unavailable node S and drop data packets as received from source node. Both blackhole scenarios can be implemented and executed in the cloud MANET enabled IoT network as presented in Figure 5. The AODV routing protocol is modified to execute the blackhole attacks in single or collaborative mode using Algorithm 1 in cloud MANET enabled IoT network. The mathematical model is presented in Figure 6 to compare the results.

3.2. Wormhole Attack Execution in Cloud MANET Enabled IoT Network. Usually, a wormhole attack is initiated by two or more malevolent IoT nodes using a special path called

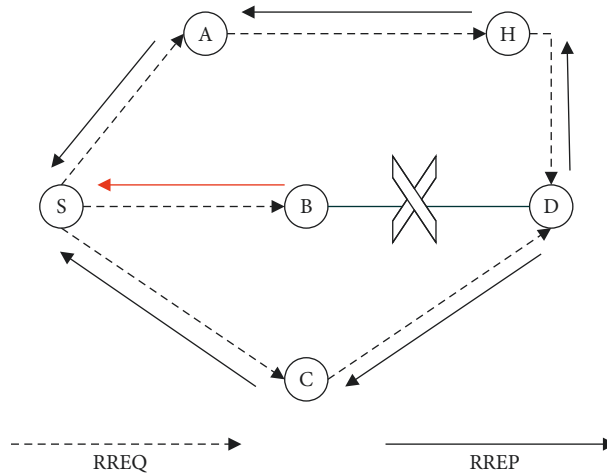


FIGURE 3: Blackhole attack in AODV routing of MANET enabled IoT.

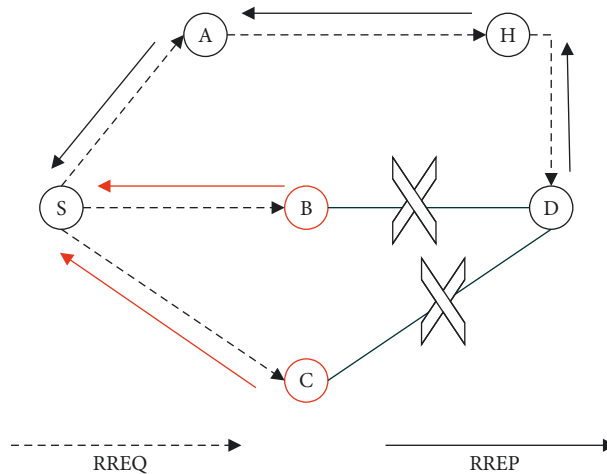


FIGURE 4: Collaborative blackhole attack in AODV routing of MANET enabled IoT.

tunnel among them in cloud MANET enabled IoT network. Data packets received by any one of the malevolent nodes are sent to the other malevolent node by using this tunnel. The malevolent IoT nodes may send data packets to each other in many numbers of times using this tunnel and due to this, the battery of other nodes becomes overextended, and the IoT device services of monitoring the agricultural field were affected [36].

The wormhole attack is depicted in Figure 7, in which the two IoT attacker nodes are represented as X and Y in MANET enabled IoT network. In path finding process, source IoT node S transmits RREQ to its neighbors A and X where X is the first end of worm tunnel, which is connected with second end of worm tunnel Y. Y sends RREQ to its neighbor C-G to reach destination node IoT D. Destination (final) node transmits RREP message to source (initial) IoT node using the path of worm tunnel, and source IoT node is still waiting for the RREP message, which makes IoT node unavailable for the services of cloud MANET enabled IoT network. This wormhole tunnel implementation and

execution is used in cloud MANET enabled IoT network as shown in Figure 8.

On another end, if RREQ request reaches node Y, then it forms a fast link between Y and X and the destination IoT node sends RREP to source node using different path as shown in Figure 9. Because of this, the energy of other nodes is exhausted, and the attacker nodes drop the packets destined for cloud MANET enabled IoT devices. The complete changes of AODV routing protocol to implement wormhole attack in cloud MANET enabled IoT network are presented in Algorithm 2, and the mathematical model of performance metrics used is shown in Figure 6.

3.3. *Simulations.* The accessibility of a tool for Internet of Things (IoT) or wireless network simulation is one of the primary facilitators for fast development in academia. Chernyshe et al. provide a complete set of simulators utilized in recent research for MANET-based IoT networks [36]. One of them, a very common utilized simulator for cloud MANET

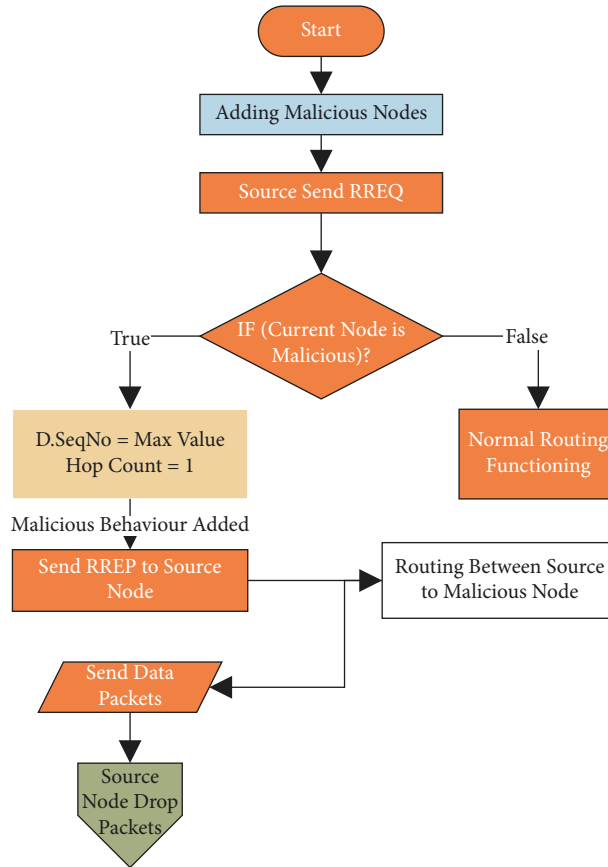


FIGURE 5: Implementation of a blackhole Attack by modification of AODV Routing Protocol.

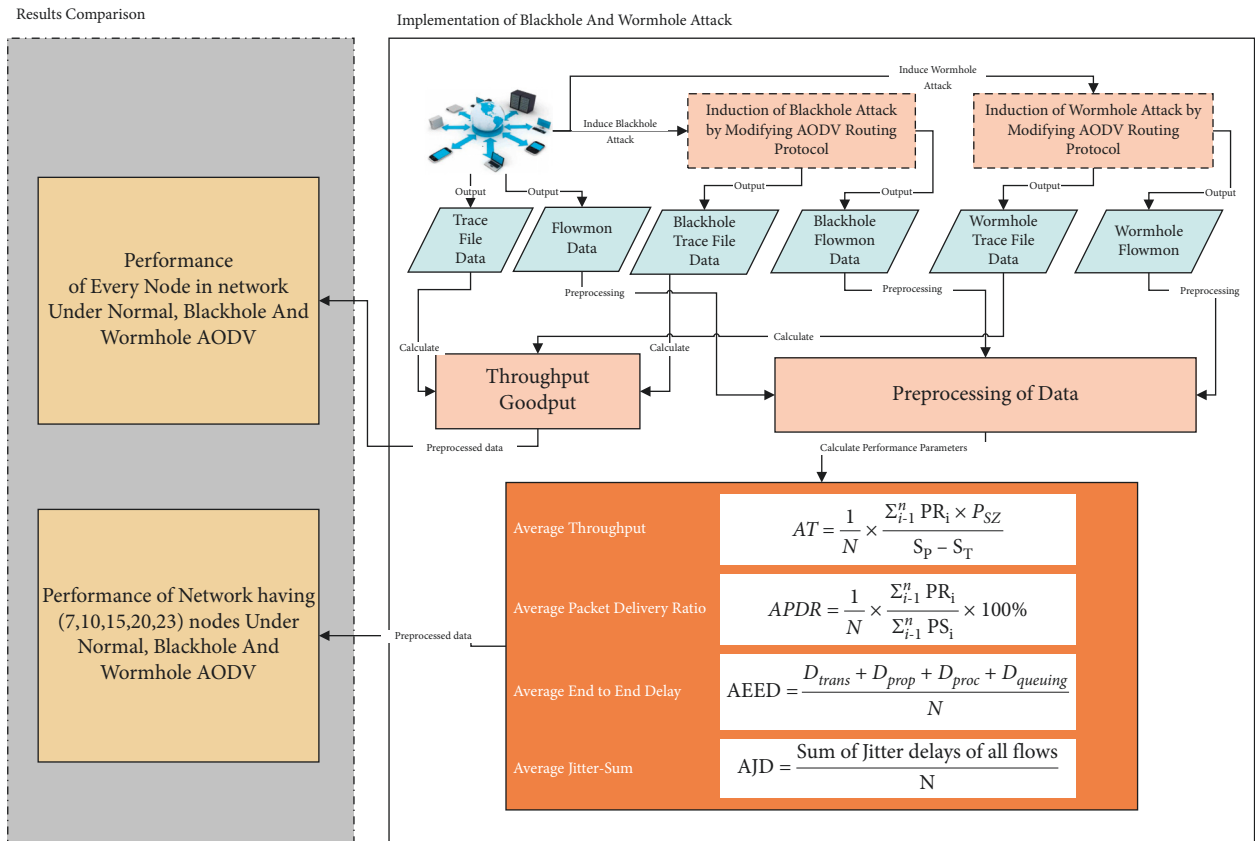


FIGURE 6: The overall methodology for comparative analysis of blackhole and wormhole attacks.

```

Step 1: Start: cloud MANET enabled IoT Network without attacker nodes
Step 2: Add one or more IoT attacker node/s in the cloud MANET enabled IoT network.
Step 3: Source node transmits Rout Request (RREQ) message to every neighbor (cloud MANET Enabled IoT) node.
Step 4: if (existing node attacker?)
    Enlarge sequence number with big value and set hop count 1.
    Attacker node transmits Route Reply (RREP) to source node.
    Build route among the Originating node and the attacker node.
    Forward data packets from originating node to attacker node.
    Attacker node will drop all the packets.
    Else
    AODV Routing Protocol will execute its tasks as usual.
    End if
Step 5: Stop

```

ALGORITHM 1: Implementation of blockhole attack in cloud MANET Enabled IoT Network.

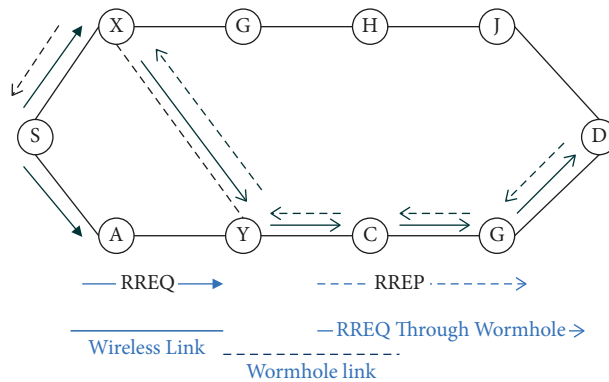


FIGURE 7: Wormhole Attack in AODV Routing of MANET enabled IoT.

enabled IoT research, is NS-3, an open-source simulator [36]. A network of varying number of IoT nodes participating in cloud MANET enabled IoT network is simulated in Network Simulator-3 (NS-3) and the cloud-based data collected during the monitoring of agricultural field using Flowmon module of NS-3. The trace file data is obtained for throughput and goodput of each node by using trace metric package of NS-3 [37]. Three numbers of blockhole IoT attacker nodes with one wormhole tunnel are used for varying number of IoT nodes participating in cloud MANET enabled IoT network for agricultural field monitoring. The mathematical model for calculating of throughput (TP), end-to-end delay (EED), packet delivery ratio (PDR), and jitter sum (JT) as performance metrics is shown in Figure 6. The results of throughput and goodput are compared to determine the effect of individual attack on cloud MANET enabled IoT network by analyzing the trace file data obtained from the cloud in trace metric module of NS-3. The overall simulation parameters are presented in Table 1.

The simulation setups of cloud MANET enabled IoT network of having different number of IoT-nodes participating in monitoring of an agricultural field are depicted in Figures 10–14. The network area (field) without any attack is represented in (a) part of every Figure and in (b) part of each figure; there are 3 malicious nodes with black color that caused the blackhole attacks shown. Finally, the field with wormhole attack is shown in (c) part of each figure, in which there are 2

malicious nodes with black color. This varying number of IoT nodes is implemented as monitoring devices in agricultural fields to collect the data and make it available on the cloud to make real-time decisions for different purposes [38]. The real-time data is unavailable due to the blackhole and wormhole attacks, and it affects the performance of network performance in terms of throughput, EED, PDR, and JT.

4. Results and Analysis

The results are analyzed and compared on the performance metrics such as Throughput (TH), Packet Delivery Ratio (PDR), End-to-End Delay (EED), Jitter-Sum (JS), and Goodput (GP). The effect of blackhole and wormhole attacks in cloud MANET enabled IoT network is analyzed under three scenarios such as without any attack and with blackhole attack and wormhole attack. The attacks are compared and determined upon the throughput and goodput for varying number of IoT nodes participating in cloud MANET enabled IoT network.

4.1. Effect of Blackhole and Wormhole Attacks on Performance Metrics. The effect of blackhole and wormhole attacks on throughput is shown in Figure 15 for normal operation of network and with attacks of wormhole and blackhole on different IoT nodes participating in cloud MANET enabled

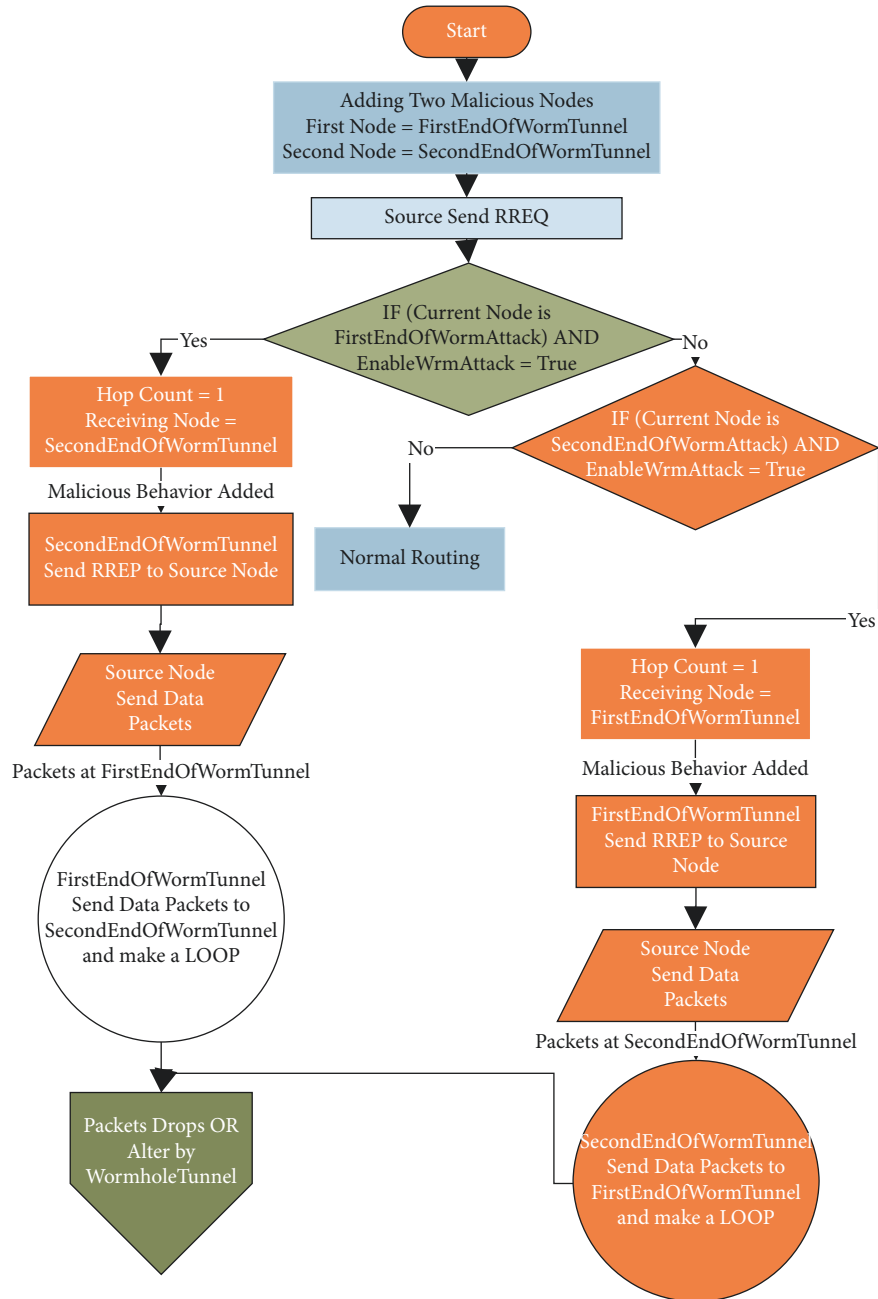


FIGURE 8: Flowchart implementation of a wormhole attack by modification of AODV routing protocol.

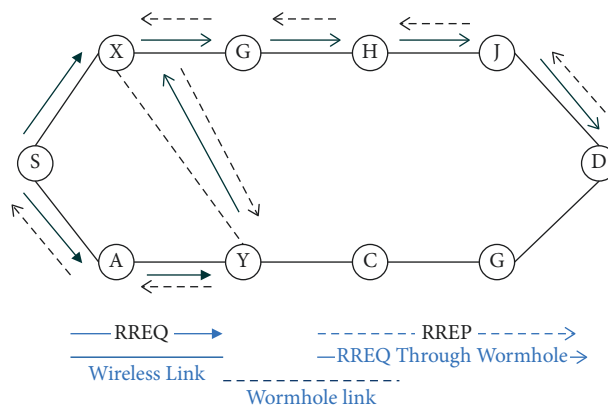


FIGURE 9: Wormhole Attack using fast link in AODV Routing of MANET enabled IoT.

```

Step 1: Start: cloud MANET enabled IoT Network without attacker nodes
Step 2: Add two attacker nodes in the cloud MANET enabled IoT network.
Step 3: Set First attacker node as FirstEndOfWormTunnel and second attacker node SecondEndOfWormTunnel
Step 4: Source Node transmits Rout Request (RREQ) message to every neighbor (cloud MANET Enabled IoT) node.
Step 5: if (EnableWrmAttack is TRUE andand Node is FirstEndOfWormTunnel?)
    Set hop count to 1.
    Set ScondEndOfWormTunnel as receiving node and form a fast tunnel
    ScondEndOfWormTunnel transmits Rout Request (RREQ) message to its neighbor nodes.
    Destination node transmits Route Reply (RREP) message to source node using prearranged Path.
    Source node send packets to destination node using prearranged path.
    When packets reach at FirstEndOfWormTunnel, it forwards it to SecondEndOfWormTunnel
    Else if (EnableWrmAttack is TRUE andand Node is SecondEndOfWormTunnel?)
        Set hop count to 1.
        Set FirstEndOfWormTunnel as receiving node and form a Fast tunnel.
        FirstEndOfWormTunnel transmits Route Request (RREQ) message to its neighbors' nodes.
        Destination node transmit Route Reply (RREP) message to source node using predefined Path.
        Source node Forward data packets to destination node using prearranged path.
        When packets reach at SecondEndOfWormTunnel, it forwards it to FirstEndOfWormTunnel, and start reiterating this
process
    All Packets drops or change by wormhole nodes.
    Else
        AODV Routing Protocol execute its tasks as usual.
    End if
End if
Step 6: Stop

```

ALGORITHM 2: Implementation of wormhole attack in cloud MANET Enabled IoT Network.

TABLE 1: Simulation parameters.

Network parameters	Values
Simulator	NS-3
Platform	Ubuntu 16.04
Simulation time	100 sec
Number of nodes	7, 10, 15, 20, 23
Number of blackhole nodes	3
Traffic	CBR (constant bit rate)
Transmission speed	250 kbps
Transmission rang	250 m * 250 m
Packet size	512 bytes
Routing protocol	AODV
Transport protocol	UDP
Physical layer	DLT_IEEE802_11
MAC layer	802.11 b

IoT network. The graph shows that the average throughput declines steadily as the number of cloud MANET enabled IoT nodes increases due to the network activities of every IoT node. The average throughput for normal working (without attack) on cloud MANET enabled IoT network is 89 kilobits per second in the start and rapidly declines and reaches 29 kilobits per second. The average throughput drops much in case of blackhole attacker node and starts with 19 kilobits per second and declines and decreases faster with increment in the number of IoT nodes and reaches 8.5 kilobits per second. Finally, it is much worse in the presence of wormhole attack and reduces to 1.5 kilobits per second with the increment of number of IoT nodes as shown in Figure 15.

Similarly, the average packet delivery ratio (PDR) of MANET enabled IoT network remains the same in case of

normal operation (without attack) with the increment in number of IoT nodes as shown in Figure 16. On the other hand, the average PDR is much worse and extremely less in case of a lesser number of IoT nodes participating in cloud MANET enabled IoT network in the presence of blackhole attack due to less choices of routing decisions, whereas this is not the case of wormhole attack as it starts with a lesser number of IoT nodes, and the average PDR is much better than blackhole attack and decreases with the increasing number of IoT nodes. Hence, the cloud MANET enabled IoT network is not giving a good average PDR in case of blackhole attack when the number of participating nodes in MANET enabled IoT is lesser as shown in Figure 16.

The MANET enabled IoT network surprisingly behaves the same for average End-to-end delay (EED) and average Jitter-Sum (JS) results as shown in Figures 17 and 18. It is shown that the average EED and average JS increase with the increment in the number of IoT nodes in the presence of blackhole attack, and this is even worse in the presence of wormhole attack.

4.2. The Harmfulness of Blackhole and Wormhole Attacks.

In this section, the performance of cloud MANET enabled IoT network is compared in terms of throughput (TP) and goodput (GP) for varying number of attacker and victim IoT nodes to determine the harmfulness of blackhole and wormhole attacks and discussed for varying number of nodes participating in monitoring of agricultural filed. The TP refers to the total amount of data that flows across a link, regardless of whether it is beneficial or not, whereas GP is only concerned with useful data.

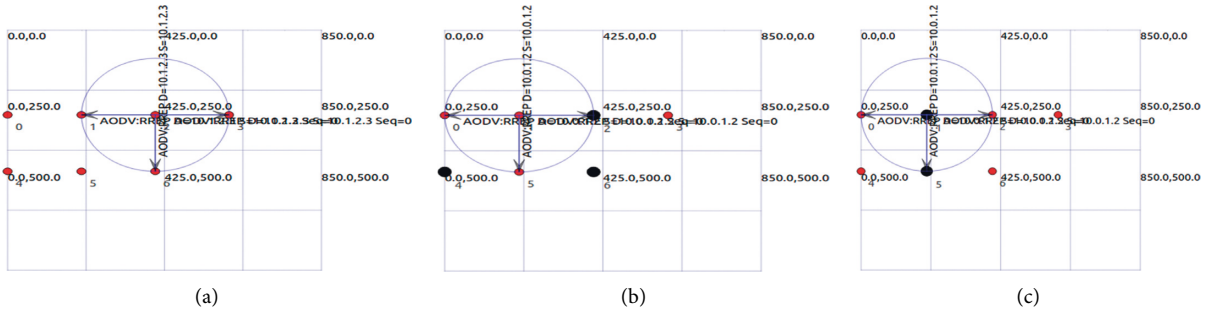


FIGURE 10: Smart Agri-Field with 7 number of MANET enabled IoT nodes.

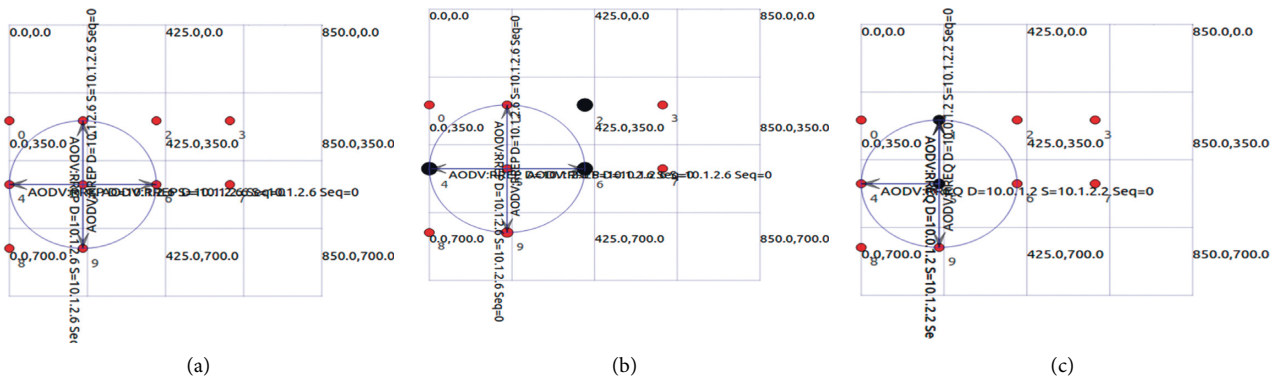


FIGURE 11: Smart Agri-Field with 10 number of MANET enabled IoT nodes.

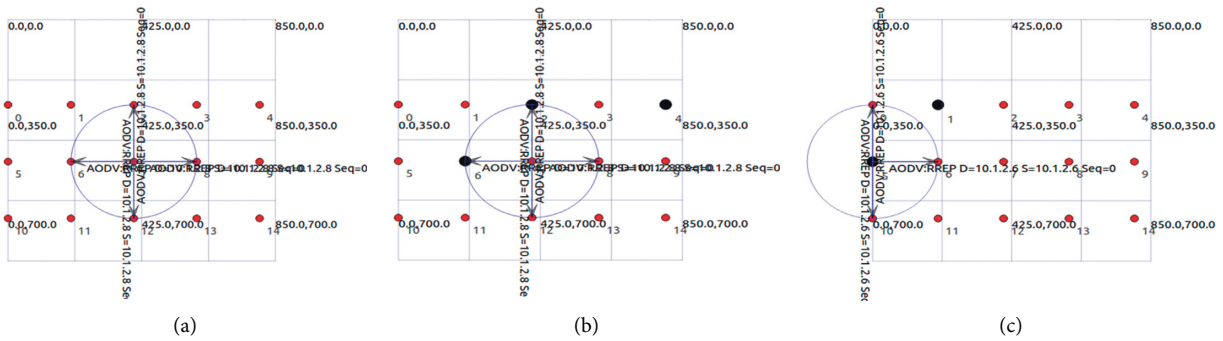


FIGURE 12: Smart Agri-Field with 15 number of MANET enabled IoT nodes.

4.2.1. 7 Cloud MANET Enabled IoT Nodes. The graph in Figure 19 shows that the TP of IoT nodes in normal operations and blackhole attack situation stays the same, whereas, in case of wormhole attack, it is very high in the start and drops thereafter rapidly and reaches the same level as in normal operation of cloud MANET enabled IoT network. The graph of GP demonstrates that the IoT nodes performing normal operations (without attack) and with blackhole as well as for wormhole attack are having very good GP in the start, but they reach zero as the number of nodes increases in case of blackhole and wormhole attacks.

The TP contains unwanted data such as data retransmissions and overhead and protocol headers, which are excluded in case of GP. That is why its value is large on every IoT node as compared to the GP. On the other hand, due to

tunneling of packet between two attacker nodes, TP of every IoT node is more in case of wormhole attack as compared to blackhole attack.

4.2.2. 10 Cloud MANET Enabled IoT Nodes. Figure 20 illustrates that the overall TP of every IoT node is high in case of wormhole attack as compared to the normal operation (without attack) and in case of blackhole attack. This is because of the presence of wormhole tunnel on both sides, and it provides much better communication for cloud MANET enabled IoT network. The graph of GP shows that the GP of some IoT nodes is higher than that of all other IoT nodes for normal operation, blackhole, and wormhole attacks due to data retransmission and protocol overhead. The

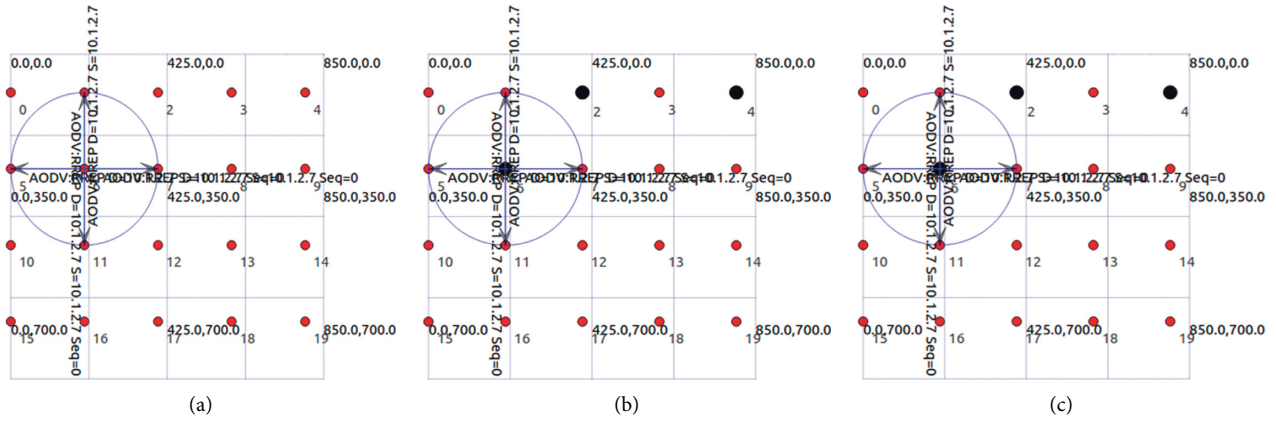


FIGURE 13: Smart Agri-Field with 20 number of MANET enabled IoT nodes.

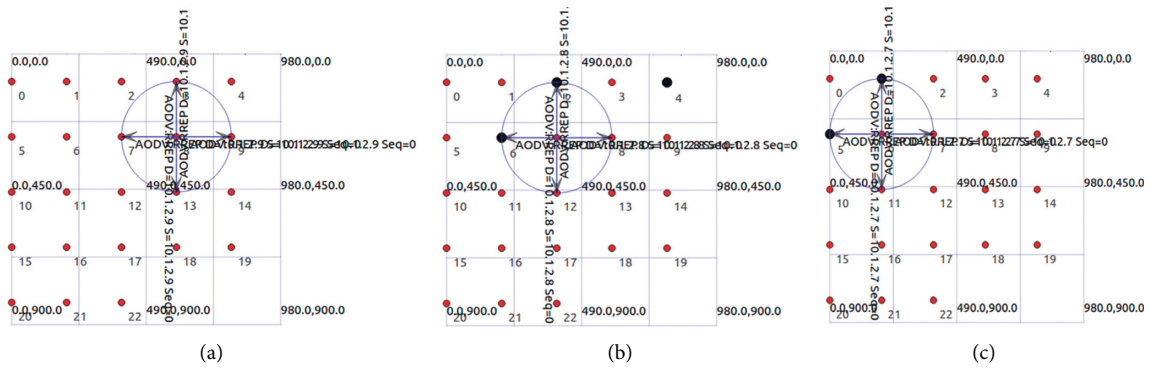


FIGURE 14: Smart Agri-Field with 23 number of MANET enabled IoT nodes.

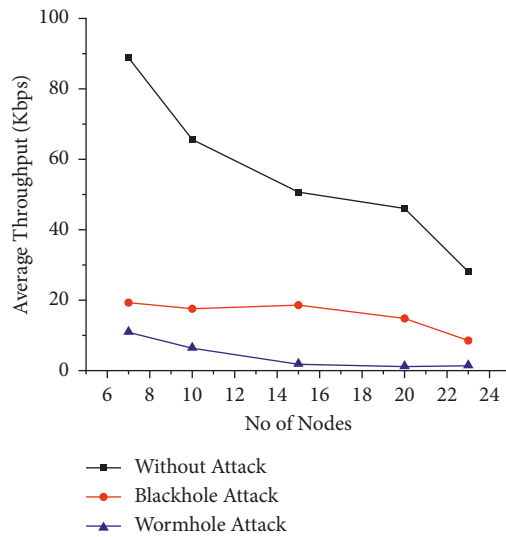


FIGURE 15: Number of MANET enabled IoT nodes V/S average throughput.

TP value for every IoT node is more as compared to the GP because most of time is consumed in tunneling of data packets.

4.2.3. 15 Cloud MANET Enabled IoT Nodes. The TP graph in Figure 21 shows that the TP remains high for nearly all IoT nodes in case of wormhole attack as compared to other

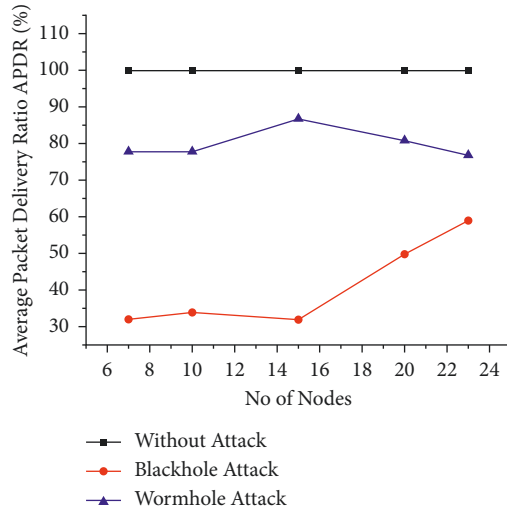


FIGURE 16: Number of MANET enabled IoT nodes V/S average packet delivery ratio.

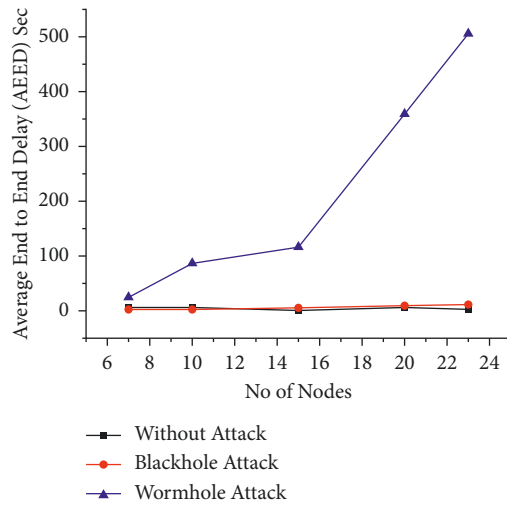


FIGURE 17: Number of MANET enabled IoT nodes vs average end to end delay.

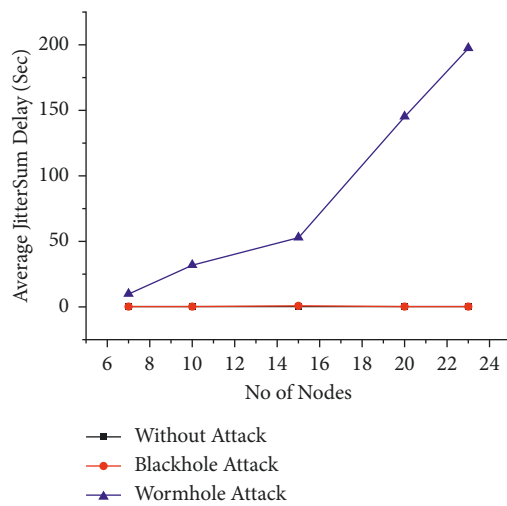


FIGURE 18: Number of MANET enabled IoT nodes vs average jitter-sum delay.

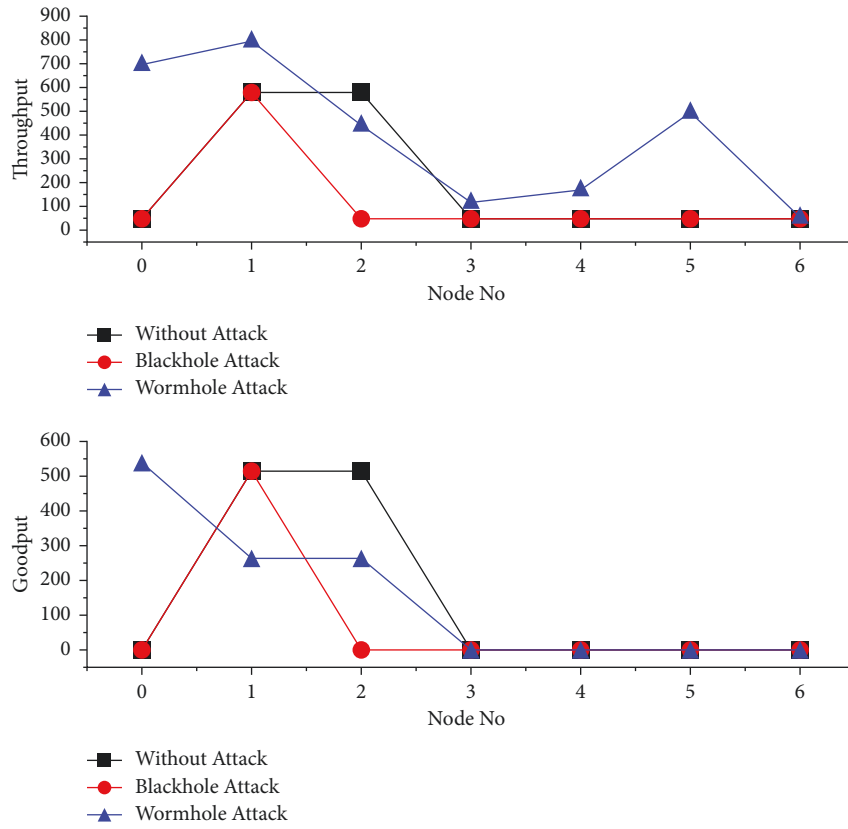


FIGURE 19: 7 MANET enabled IoT nodes.

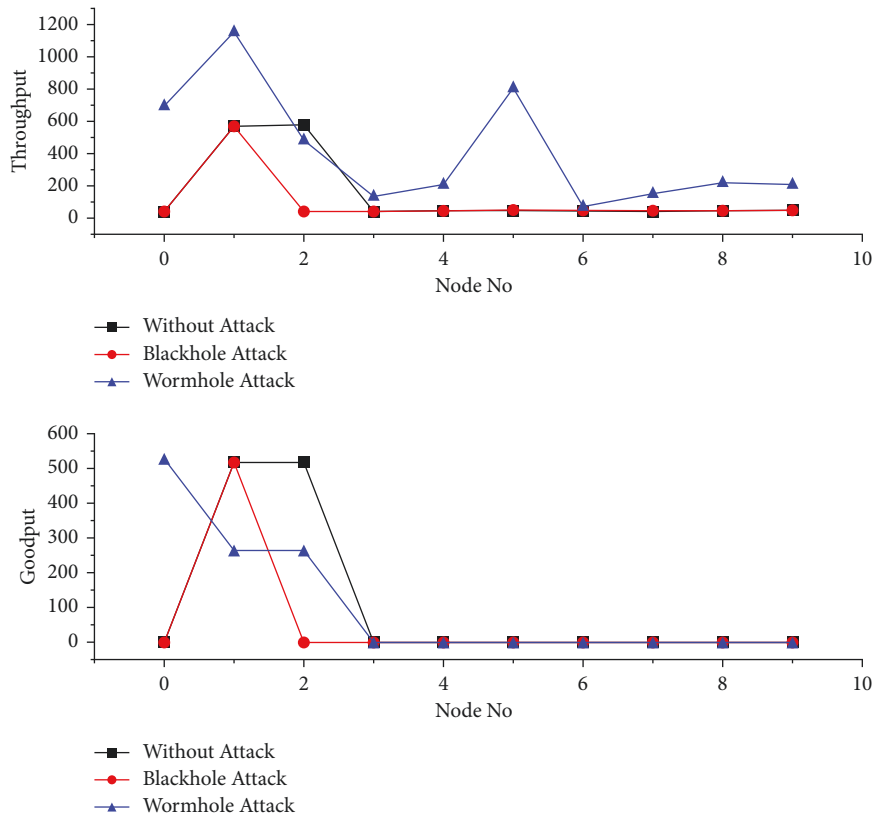


FIGURE 20: 10 MANET enabled IoT nodes.

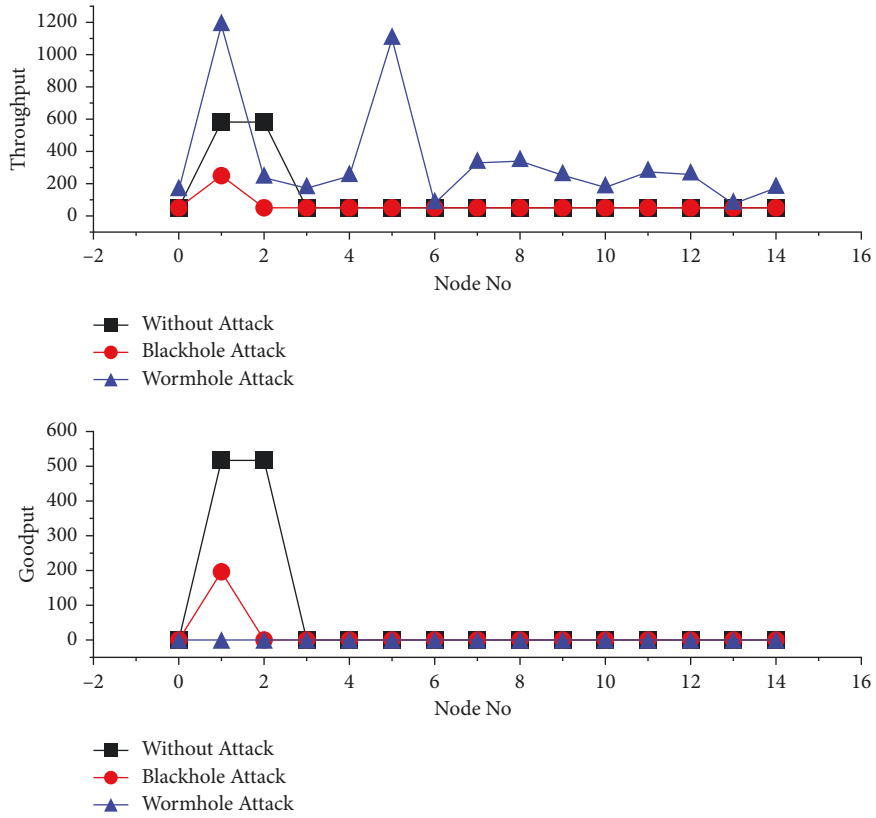


FIGURE 21: 15 MANET enabled IoT nodes.

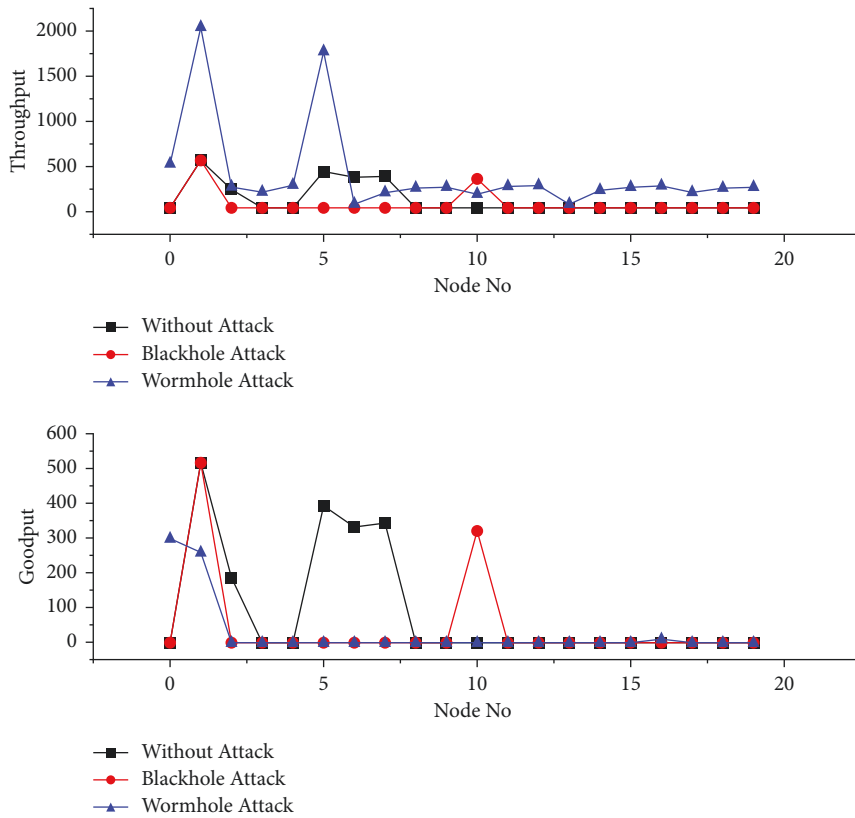


FIGURE 22: 20 MANET enabled IoT nodes.

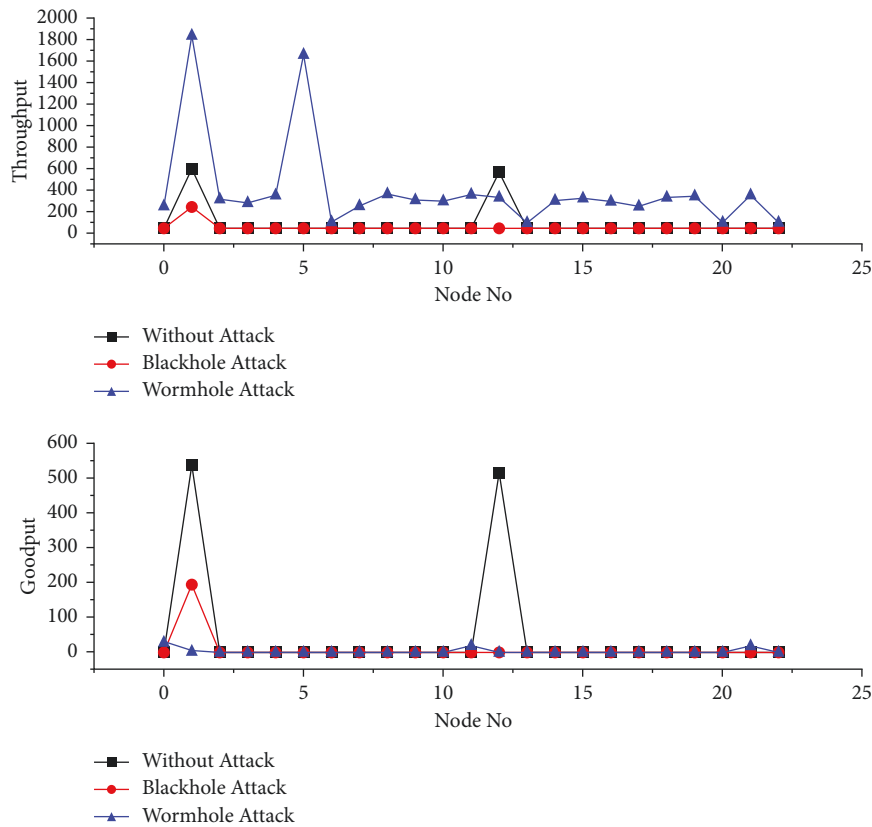


FIGURE 23: 23 MANET enabled IoT nodes.

cases, whereas the GP of wormhole attack is 0 across all IoT nodes within the cloud MANET enabled IoT network. Hence, it is clear that as the number of participating IoT nodes in cloud MANET enabled IOT network increases, the TP is higher with respect to the GP.

4.2.4. 20 Cloud MANET Enabled IoT Nodes. The TP and GP in Figure 22 illustrate that the same condition of IoT nodes performing normal operation (without attack) is higher than that of blackhole and wormhole attack. TP of IoT nodes under wormhole attack is better than that under the blackhole attack due to tunneling and data retransmission as well as protocol overhead.

4.2.5. 23 Cloud MANET Enabled IoT Nodes. The TP of wormhole attack is high on all IoT nodes as shown in Figure 23. However, the TP of IoT nodes is the same in the start in case of blackhole attack and decreases as soon as the number of nodes increases. The GP graph shows that the GP is very low of the overall cloud MANET enabled IoT network excluding on some IoT nodes. The throughput on every node is higher with respect to the GP because it includes data retransmission and protocol overhead. It is also observed that the TP of the overall cloud MANET enabled IoT network is higher in the presence of wormhole attack as compared to the blackhole attack when increasing the number of IoT nodes for monitoring. This is because of the tunneling availability of routing decisions in case of wormhole attacks.

5. Conclusions

The cyber security is a much concern when preserving the confidentiality, availability, and integrity of future networks. This concern even increases in Mobile Ad hoc Network (MANET) enabled Internet of Things (IoT) for varying and much personal IoT devices participating in communications. The application of MANET enabled IoT network in agricultural field towards making smart fields can talk and share its much important data and requires an independent network that serves as a cloud for many services such as monitoring in a secure and privately. Therefore, this paper compares the cloud-based services for MANET enabled IoT network under blackhole and wormhole attacks for IoT device-to-device information exchange. The agricultural field is simulated in a contextual view and simulated to observe the vulnerabilities towards Denial of Service (DoS) attacks such as blackhole and wormhole. The simulations are performed using an open-source simulator, Network Simulator 3 (NS-3), in order to determine the impact of blackhole and wormhole attacks on network performance of cloud MANET enabled IoT network deployed for monitoring of an agricultural field. The results are evaluated on the evaluations metrics such as throughput, packet delivery ratio (PDR), end-to-end delay (EED), and Jitter-Sum of preprocessed data gathered with the flow-monitor module of NS-3. This paper is highly useful for future cloud MANET enabled IoT smart agricultural field security research purpose.

Data Availability

Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

Acknowledgments

This work was partly supported by the National Natural Science Foundation of China (Grant no. 62072060).

References

- [1] W. S. Affi, A. A. El-Moursy, M. Saad, S. M. Nassar, and H. M. El-Hennawy, "Importance of cloud computing in 5G radio access networks," *Research Anthology on Developing and Optimizing 5G Networks and the Impact on Society*, pp. 226–239, 2021.
- [2] J. Huang, B. Lv, Y. Wu, Y. Chen, and X. Shen, "Dynamic admission control and resource allocation for mobile edge computing enabled small cell network," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 2, pp. 1964–1973, 2022.
- [3] T. Alam, "Internet of things: a secure cloud-based MANET mobility model," *International Journal on Network Security*, vol. 22, no. 3, pp. 516–522, 2020.
- [4] K. Yogeswaranathan and R. Collier, "A systematic survey on the role of cloud, fog, and edge computing combination in smart agriculture," *Sensors*, vol. 21, no. 17, Article ID 5922, 2021.
- [5] Y. Chen, N. Zhang, Y. Zhang, X. Chen, W. Wu, and X. S. Shen, "TOFFEE: task offloading and frequency scaling for energy efficiency of mobile devices in mobile edge computing," *IEEE Transactions on Cloud Computing*, vol. 9, no. 4, pp. 1634–1644, 2021.
- [6] Y. Chen, Y. Zhang, Y. Wu, L. Qi, X. Chen, and X. Shen, "Joint task scheduling and energy management for heterogeneous mobile edge computing with hybrid energy supply," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8419–8429, 2020.
- [7] J. Huang, C. Zhang, and J. Zhang, "A multi-queue approach of energy efficient task scheduling for sensor hubs," *Chinese Journal of Electronics*, vol. 29, no. 2, pp. 242–247, 2020.
- [8] A. Aiiad, "An image hashing-based authentication and secure group communication scheme for IoT-enabled MANETs," *Future Internet*, vol. 13, no. 7, Article ID 166, 2021.
- [9] K. Demestichas, N. Peppes, and T. Alexakis, "Survey on security threats in agricultural IoT and smart farming," *Sensors*, vol. 20, no. 22, Article ID 6458, 2020.
- [10] C. Z. Sirmollo and M. A. Bitew, "Mobility-Aware routing algorithm for mobile ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6672297, 12 pages, 2021.
- [11] S. Jaiganesh, K. Gunaseelan, and V. Ellappan, "IOT agriculture to improve food and farming technology," in *Proceedings of the Conference on Emerging Devices and Smart Systems (ICEDSS)*, pp. 260–266, Mallasamudram, India, March 2017.
- [12] R. Trivedi and P. Khanpara, "Robust and secure routing protocols for MANET-based internet of things systems—a survey," emergence of cyber physical system and IoT in smart automation and robotics," *Advances in Science, Technology & Innovation (IEREK Interdisciplinary Series for Sustainable Development)*, Springer, Berlin, Germany, 2021.
- [13] H. Gao, Y. Zhang, H. Miao, R. J. D. Barroso, and X. Yang, "SDTIOA: modeling the timed privacy requirements of IoT service composition: a user interaction perspective for automatic transformation from bpel to timed automata," *Mobile Networks and Applications*, vol. 26, 2021.
- [14] X. Ma, H. Xu, H. Gao, and M. Bian, "Real-time multiple-workflow scheduling in cloud environments," *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4002–4018, 2021.
- [15] Y. Huang, H. Xu, H. Gao, X. Ma, and W. Hussain, "SSUR: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 670–681, 2021.
- [16] Y. Yin, Z. Cao, Y. Xu, H. Gao, R. Li, and Z. Mai, "QoS prediction for service recommendation with features learning in mobile edge computing environment," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 4, pp. 1136–1145, 2020.
- [17] N. Papadakis, N. Koukoulas, I. Christakis, I. Stavrakas, and D. Kandris, "An IoT-based participatory antitheft system for public safety enhancement in smart cities," *Smart Cities*, vol. 4, no. 2, pp. 919–937, 2021.
- [18] R. R. Chandan and P. K. Mishra, "Performance analysis of AODV under black hole attack," in *Proceedings of the 2nd International Conference on Advanced Computing and Software Engineering (ICACSE)*, March, 2019.
- [19] H. Gao, X. Qin, R. J. D. Barroso, W. Hussain, Y. Xu, and Y. Yin, "Collaborative learning-based industrial IoT API recommendation for software-defined devices: the implicit knowledge discovery perspective," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 6, no. 1, pp. 66–76, 2022.
- [20] G. Nagasubramanian, R. K. Sakthivel, and R. Patan, "Detection and isolation of black hole attack in mobile ad hoc networks: a review," *Disruptive Technologies in Information Sciences*, vol. 11419, Article ID 114190N, 2020.
- [21] R. Rana and R. Kumar, "Performance analysis of AODV in presence of malicious node," *Acta Electronica Malaysia*, vol. 3, no. 1, pp. 1–5, 2019.
- [22] P. Varga, S. Plosz, G. Soos, and C. Hegedus, "Security threats and issues in automation IoT," in *Proceedings of the IEEE 13th Int. Workshop FactoryCommun. Syst. (WFCS)*, pp. 1–6, Trondheim, Norway, May 2017.
- [23] S. Palacharla, M. Chandan, K. Teja, and G. Varshitha, "Wormhole attack: a major security concern in internet of things (IoT)," *International Journal of Engineering and Technology*, vol. 7, no. 3, pp. 147–150, 2018.
- [24] A. David, J. Gutiérrez, and S. Kumar Ray, "A trust-aware RPL routing protocol to detect blackhole and selective forwarding attacks," *Australian Journal of Telecommunications and the Digital Economy*, vol. 5, pp. 50–69, 2017.
- [25] S. Murali and A. Jamalipour, "A lightweight intrusion detection for sybil attack under mobile RPL in the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 379–388, 2020.
- [26] J. Karlsson, L. S. Dooley, and G. Pulkkis, "Secure routing for MANET connected Internet of Things systems," in *Proceedings of the IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 114–119, Barcelona, Spain, August 2018.

- [27] M. G. Samarasinghe and K. A. Kulawansa, "Use of IOT for smart security management in agriculture," in *Proceedings of the 9th Intl. Conf. on Advances in Computing, Control and Networking*, London, UK, July 2019.
- [28] S. Laxmi, B. Hemavati, and B. Biradar, "Design and implementation of IoT based smart security and monitoring for connected smart farming," *International Journal of Computer Application*, vol. 179, no. 11, 2018.
- [29] R. Haribabu, T. Santhosh, R. Sethupathi, S. Veerakumar, and A. Abinash, "Multiple tasks of IOT based smart security a monitoring devices for agriculture," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 5, no. 3, 2017.
- [30] P. Gupta, P. Goel, P. Varshney, and N. Tyagi, "Reliability factor based AODV protocol: prevention of black hole attack in MANET," *Smart Innovations in Communication and Computational Sciences*, Springer, Singapore, 2019.
- [31] I. Kaushik, N. Sharma, and N. Singh, "Intrusion detection and security system for blackhole attack," in *Proceedings of the 2nd International Conference on Signal Processing and Communication (ICSPC)*, pp. 320–324, Coimbatore, India, March 2019.
- [32] V. Kumar, "A review on detection of black hole attack techniques in MANET," *International Journal of Advanced Research*, vol. 4, no. 3, 2018.
- [33] M. Imran, F. A. Khan, T. Jamal, and M. H. Durad, "Analysis of detection features for wormhole attacks in MANETs," *Procedia Computer Science*, vol. 56, pp. 384–390, 2015.
- [34] M. Chernyshev, Z. Baig, O. Bello, and S. Zeadally, "Internet of things (IoT): research, simulators, and testbeds," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1637–1647, 2018.
- [35] L. Campanile, M. Gribaudo, M. Iacono, F. Marulli, and M. Mastroianni, "Computer network simulation with ns-3: a systematic literature review," *Electronics*, vol. 9, no. 2, 2020.
- [36] A. Hinds, M. Ngulube, S. Zhu, and H. Al-Aqrabi, "A review of routing protocols for mobile ad-hoc networks (manet)," *International journal of information and education technology*, vol. 3, no. 1, 2013.
- [37] S. Gurung and S. Chauhan, "A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET," *Wireless Networks*, vol. 25, no. 4, pp. 1685–1695, 2019.
- [38] C. Aydogdu and E. Karasan, "Goodput and throughput comparison of single-hop and multi-hop routing for IEEE 802.11 DCF-based wireless networks under hidden terminal existence," *Wireless Communications and Mobile Computing*, vol. 16, no. 9, pp. 1078–1094, 2016.

Research Article

Multinode Data Offloading for Urban Wireless Sensor Networks Based on Fog Computing: A Multiarmed Bandit Approach

Yuchen Shan, Hui Wang , and Chenxiang Zhang

School of Mathematics and Computer Science, Zhejiang Normal University, Yingbin Avenue, Jinhua 321004, China

Correspondence should be addressed to Hui Wang; hwang@zjnu.cn

Received 7 December 2021; Revised 24 January 2022; Accepted 27 January 2022; Published 29 April 2022

Academic Editor: Yuyu Yin

Copyright © 2022 Yuchen Shan 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.

Urban wireless sensor networks (UWSNs) are an important application scenario for the Internet of Things (IoT). With the emergence of many computationally intensive applications based on urban environments, sensors in wireless sensor networks are unable to meet demands such as latency due to their limited resources. Fog computing architectures have the potential to liberate data transmission from resource-constrained sensor nodes through data offloading. Therefore, data collection and scalable collaboration based on fog architectures are seen as a challenge. For the multinode data offloading problem, a multinode data offloading strategy based on stable matching and MAB (multi-armed bandit) model is proposed to maximize the offloading success rate while guaranteeing the latency requirements of the source task nodes. Firstly, the multinode data offloading problem is modelled. Secondly, the case of multinode selection conflict is considered, and selection conflict and information exchange are reduced by the MAB model and the fallback timer. Then, an adjustment strategy is proposed based on the idea of delayed reception in the stable matching of game theory. Finally, the multinode data offloading problem is solved by successive iterations. The proposed algorithm not only accomplishes coordinated cooperation between nodes to achieve high-quality data offloading and avoid collisions between nodes but also reduces the amount of information exchanged between nodes. The effectiveness of the algorithm is demonstrated by theoretical analysis and simulation experiments.

1. Introduction

Our lives are increasingly dependent on smart IoT devices that sample data and collect data from the environment and operate in the physical world [1]. Many IoT devices, such as sensor nodes, are deployed in cities and large metropolitan areas for applications such as security monitoring, traffic, pollution monitoring, infotainment, and energy management [2, 3], as well as in vehicle-based self-organizing networks to support data communication between nodes via wireless multihop transmission [4]. In the future, many new applications will emerge in everyday life, such as smart homes, smart cities, and smart grids. The proliferation of urban IoT applications has created an unprecedented amount of data, including physical quantities sampled from the environment [5]. Specifically, data are collected from the real world by IoT devices and then transmitted to processing centres for calculation and processing using the internet as a

communication network [6]. In addition, the proliferation of a large number of heterogeneous IoT devices and the dynamic changes in the environment adds to the difficulty of real-time computation and decision-making for IoT devices.

To realize the above vision of the future, the devices in the network need to perform a lot of real-time calculations and need to make decisions constantly, which places high demands on the computing power and battery consumption of the devices. In order to reduce the cost of various devices, a viable option today is to use cloud computing and cloud infrastructure to increase sufficient computing and storage resources for the network. Cloud computing can offload data and computing tasks from the device to a remote cloud for supplementary computing [7]. Using this approach can reduce the burden and energy consumption of the device itself, save local storage resources, and reduce the cost of network equipment. For example, in [8], real-time workflow scheduling in a cloud-based environment effectively reduces

network costs. However, with the rapid spread of emerging applications such as virtual reality (VR), face recognition, image recognition, and video processing, centralized cloud-based solutions have raised concerns about the latency issues arising from the long distances between end devices and the cloud, as well as link loading issues. As a result, the concept of fog computing was introduced, with fog computing networks distributing computing, storage, control, and communication services across a cloud-to-thing continuum, rather than offloading them to the cloud [9]. Some network edge devices that are closer to end devices such as small base stations, wireless access points, laptops, moving vehicles, and smartphones with some computing and storage capabilities are used as an intermediate layer between the cloud and end devices, i.e., the fog layer. Fog computing networks are considered to be a promising network architecture that uses more edge network resources to improve services such as offloading, triage, and caching for devices. Compared to cloud computing, fog computing is not only effective in reducing latency but also in reducing the number of communications between the base station and the core network, thereby reducing link load. In summary, fog computing can effectively support compute-intensive and latency-sensitive applications and can better meet the needs of the future Internet of Everything.

There are many application scenarios for IoT, such as industrial IoT [10] and IoT in urban environments. Urban wireless sensor networks are one of the key application scenarios for the IoT. Data from the surrounding environment are sampled by sensor nodes deployed in urban wireless sensor networks to support intelligent detection of urban applications such as temperature, humidity, water levels, vehicle activity on roads, alley crime monitoring, and other scenarios [11]. With the increase in urban population, the massive increase in data volume, and the proliferation of a large number of heterogeneous devices, urban habitats are more likely to interfere with wireless sensor network communications, resulting in degraded network performance. Therefore, research on urban wireless sensor networks based on fog computing is necessary. Sensor nodes can only effectively support urban applications if they first successfully offload sampled data to fog layer devices (fog nodes). Sensor nodes have limited resources, which prevent them from storing the sampled data indefinitely. It is therefore crucial that data are offloaded to resource-rich nodes before storage space is exhausted, a problem known as the “data loss problem.”

The sensor nodes in the network that need to offload data are referred to as task nodes, while resource-rich nodes, i.e., nodes that can help resource-limited nodes with data offloading, are referred to as helper nodes. Designing an offloading solution to prevent the “data loss problem” is very challenging: an effective strategy requires careful collaboration between nodes, but the limited resources of sensor nodes preclude a significant overhead of coordination mechanisms. In real urban wireless sensor networks, there are often multiple task nodes that need to be offloaded simultaneously. Therefore, it is a natural trend to consider multinode data offloading schemes. In the multinode data

offloading problem, there are selection conflicts between nodes and fairness issues, i.e., multiple task nodes compete for a “best” helper node for data offloading. Therefore, in this paper, the problem of collision between nodes and pairing fairness is a pressing challenge based on a scenario where multiple nodes coexist.

Most existing solution strategies customize offloading or content caching as a constrained convex optimization problem and choose different metrics and constraints such as latency, network throughput, and energy efficiency. In [12], Lan et al. proposed two schemes, both of which aim to maximize the average utility of the system. The first scheme formulates a task caching optimization problem based on stochastic theory and designs task caching algorithms to solve it. The second scheme describes the task offloading and resource optimization problem as a mixed-integer nonlinear dynamic programming problem. Jiang [13] studied the edge cache optimization problem in foggy radio access networks. Intending to minimize delay, they considered the use of joint and parallel transmission strategies to transform the objective into a nondeterministic polynomial. In [14, 15], the authors of [14] wanted to maximize the weighted computation rate of all wireless devices in the network by jointly optimizing the selection of individual computation modes and the allocation of system transmission delays. They first assumed that the mode selection is given and considered decoupled optimization to solve the problem. However, this approach is highly complex in large networks. The authors of [15] investigated the problem of joint task offloading and resource allocation to maximize offloading gains for users, and the problem they considered is formulated as a mixed-integer nonlinear program involving joint optimal offloading decisions, the uplink transmission power for mobile users, and computational resource allocation for mobile edge cloud servers. The authors of [16] considered the total gain of the network by computing offloading decisions, resource allocation, and content caching policies as an optimization problem. The authors transformed the problem into a convex problem and proposed alternating directions based on a multiplier algorithm to solve the optimization problem. In addition, many researchers are currently using game theory or its variants to solve the above problems, such as a smart gateway based on game theory for offloading and migration functions for the Internet of Things in fog computing [17], where the authors proposed an approach based on noncooperative game theory to reduce the latency and energy consumption during application execution. There is also a multiuser partial computation offloading strategy based on a game theory proposed by the authors of [18], who modelled the computational overhead based on game theory with the objective of a multiuser partial offloading problem in a mobile edge computing environment under wireless channels. There are also literature studies [19, 20] that are based on game theory. Almost all of the approaches mentioned above are premised on the assumption that a complete model of the system and the state transfer probabilities of the individual states can be obtained. However, in actual dynamic reality scenarios, such assumptions are too idealistic.

In addition to formulating the problem as a convex optimization problem, many scholars have studied the problems regarding data collection and offloading in IoT scenarios based on fog computing through many different theories. The authors of [21] used cloud and fog computing paradigms to design a multilayer data offloading protocol for a variety of data-centric applications in urban scenarios. Specifically, to reduce the probability of data loss, the protocol exploits the heterogeneity in the network and the characteristics of fog computing by logically dividing sensor nodes into “in-need” and “helper” nodes based on Markov chains, enabling sensor nodes to collaboratively offload data to each other or the fog nodes. However, their solution assumes that the nodes have enough storage space to store all the data and that the mobility of the nodes is fixed and known in advance. The authors of [22] focused on security and privacy-preserving issues during data collection and offloading. To achieve efficient and secure large sensory data collection in fog computing-based IoT, firstly, the authors proposed a sampling perturbation encryption method without sacrificing data relevance. Secondly, the authors developed an optimization model of the measurement matrix to ensure the accuracy of data reconstruction. Finally, the authors developed an efficient offloading decision algorithm by determining the offloading ratio for the joint optimal allocation of resources with the minimum offloading time as the goal. This paper focuses on improving the success rate of data offloading as high as possible while satisfying the requirement of maximum tolerable time delay for data offloading, and therefore, data security and privacy issues during offloading are not the focus of this paper. In addition to this, there are still many scholars studying the problems regarding offloading decisions in fog computing-based IoT scenarios; for example, the authors of [23] focused on fog computing-based offloading solutions in industrial IoT scenarios. Their aim was that computational tasks can be completed within the desired energy consumption and latency and with minimal energy consumption. The authors not only found the optimal value by means of an acceleration gradient algorithm with joint optimization of the offloading rate and transmission time but also developed an alternating minimization algorithm taking into account dynamic electrocompression party techniques. Also, the authors of [24] developed latency-minimized offloading decisions and resource allocation for fog computing-based IoT scheme based on queueing theory to propose a joint optimization problem for offloading decisions, local resources, etc., for fog nodes. They took this mixed-integer nonlinear programming problem and dynamically decomposed it into two subproblems, which are in turn optimized by a simulated annealing algorithm.

To solve the problem of the too idealized hypothetical model in actual dynamic scenes, some scholars use the reinforcement learning (RL) based method. Guo et al. [25] believed that the existing cache strategy is “blind” to users; that is, users do not know whether the file to be requested is in the local cache of nodes around them. Therefore, the authors made local cache efficient by actively informing users what the base station has cached. Since the probability

of request is unknown, the authors used Q-learning to perceive the probability of request and random arrival and departure of mobile users and then optimized the cache replacement strategy. In [26], the authors proposed a new joint offloading and resource allocation method in a WiFi-based multiuser mobile edge architecture. Their goal was to minimize the energy consumption of mobile terminals under application delay constraints, and the optimal offloading strategy was implemented jointly with radio resource allocation. Therefore, the authors presented this problem as a new online reinforcement learning problem and proposed a new strategy based on a Q-learning algorithm to solve this problem, considering both delay and device computing constraints. Q-learning is a model-free algorithm in RL, which can learn the best strategy by constantly interacting with the environment without knowing the complete system model and system state. However, as the number of individual states and actions increases, the computational complexity and storage cost based on Q-learning will increase exponentially, so it is not suitable for complex dynamic Internet of Things scenarios.

With the increasing application of reinforcement learning as the core technology, research and attention on reinforcement learning have been gradually increased in various fields. MAB model is a classic application model in reinforcement learning. In the randomized MAB problem, given a set of arms (actions), one arm is selected in each trial, and a reward is obtained from the reward distribution following that arm. Each arm has an unknown random reward, and by pulling an arm, the player can immediately receive a reward. The player decides which arm to pull in a series of experiments to maximize the rewards accumulated over time. Naturally, the multinode data offloading problem in urban wireless sensor networks based on fog computing can be modelled as the MAB problem. During data offloading, mission nodes can be modelled as players in the MAB scene, and help nodes can be modelled as arms in the MAB scene. Similarly, each help node has an unknown random reward for data offloading. Task nodes offload data through the decision helper node and obtain the feedback structure (reward) for offloading data after completion. The task node decides on the helper node for offloading in each round to maximize the long-term accumulated feedback results about offloading. Currently, MAB algorithms are widely used in various fields, such as website optimization [27], optimal control strategies for robots [28], distributed dynamic recommender systems [29], competitive cooperative learning [30], and learning in changing environments [31].

The MAB model has a classic EE (exploitation and exploration) problem, in which the player must update the algorithmic strategy through trial and error to achieve the optimal strategy with the highest expected reward. This learning feature leads to the decision maker’s need to constantly balance the relationship between exploration and utilization: the strategy to improve the probability of winning the reward by using the accumulated known data and, at the same time, to explore other unselected arms, to obtain more data and more accurately evaluate the strategy of the

currently selected arm operation. This requires a lot of interactions with the environment, some of which are effective and some of which are meaningless, such as repeated exploration of an area where rewards are known and low.

By far, the most practical and effective exploration strategy in practice is the reward bonus, a mechanism that adds exploration rewards to the unexplored or less frequently decided arms, driving the decision maker to explore these arms based on a high exploration reward. The mechanism is mainly based on the unknown optimistic exploration method [32], the main idea of which is to use historical data to build an estimate of the maximum possible reward for an unknown environment, i.e., an upper bound on the confidence interval, and then to select arms based on this upper bound. A simple idea is to calculate the upper bound of the confidence interval for the dereward function and add it to the reward, which means that a larger value of the reward function represents a greater unknown for this arm, which would drive the decision maker to collect more data about this arm. For example, the authors of [33] proposed an online learning-based offloading strategy for dynamic fog computing networks using the UCB1 algorithm to optimize the average offloading delay and offloading success rate, which can make optimal offloading decisions in real time. However, in this paper, this author only considers the context when a single node performs offloading. In practical IoT scenarios, it is necessary and challenging to consider scenarios where multiple nodes perform data offloading with the massive increase of a large number of IoT heterogeneous devices.

In summary, this paper considers the multinode data offloading problem in an urban dynamic sensor network based on fog computing with the maximum tolerable delay of data offloading as a constraint, thus improving the success rate of data offloading. The UCB1 algorithm, based on the optimistic idea, models the multinode data offloading problem as a MAB model in reinforcement learning, allowing decision makers in the network to exploit and explore without prior knowledge of the complete system model and the transfer probabilities of individual states by continuously learning through interaction with the environment and using the upper bound of the rewarded confidence interval. In addition, considering the selection conflict and fairness issues in multinode data offloading scenarios, the MAB framework is improved using stable matching theory [34] and fallback timers to make the system robust and effective in terms of time delay and offloading success. With this one-to-one selection mechanism, multi-task node selection conflicts are avoided. Moreover, the introduction of the fallback timer can reduce a large amount of information exchange. For maximizing the data offloading success rate to minimize the latency, the MTDOsa-MAB strategy is proposed based on the consideration of the selection conflict problem and the fairness problem. Our main contributions are summarized as follows:

- (i) A novel learning framework is proposed to learn the multinode data offloading problem as a MAB

problem without requiring any prior knowledge about the characteristics of the helper nodes.

- (ii) To reduce the computational overhead and to resolve conflicts in a distributed manner, an offloading strategy has been proposed, namely, MTDOsa-MAB (a multinode data offloading strategy based on stable matching and MAB model). This strategy implements the selection of helper nodes by using the stable matching theory and a fallback timer. In this case, collisions are eliminated to ensure efficient data collection and to avoid extensive information exchange.
- (iii) An upper bound on the regret value of the MTDOsa-MAB strategy is proposed, and the effectiveness of the strategy is verified by simulation experiments.

2. Model and Problem Formulation

2.1. Network Model and Offload Model. Figure 1 illustrates the dynamic fog computing model for a certain time slot. With the support of helper nodes, task nodes offload data to fog nodes before resources are exhausted to support urban applications. The helper node acts as a forwarder of data and does not process the data, which is all processed by the fog node. In this paper, we consider a many-to-many (multiple task nodes, multiple helper nodes) data offloading scenario with indivisible data.

This paper focuses on optimizing data offloading for fog networks in the context of resource-limited sensor nodes. It uses the fog network paradigm to design a data offloading protocol, shown in Figure 2, for various data-centric applications in urban wireless sensor network scenarios. Specifically, it exploits the heterogeneity in fog computing networks, so sensor nodes can collaboratively offload data to each other or to mobile fog nodes. To reduce the coordination overhead between sensor nodes and fog nodes, sensor nodes are logically divided into task node and helper node categories based on their buffer availability and relative locations. Firstly, when a task node sends a request to offload data, the helper node updates its own status and feeds the status information back to the task node. Secondly, the historical offload reward information of a helper node and the request conditions of the task node to offload data are fed back to the fog node for decision analysis and to complete the data offload. Finally, after the data offloading is completed, the fog node feeds the offloading result under this decision to the task node. Table 1 shows the symbols used in this paper and their meanings.

At the beginning of each time slot, the task node makes a request to offload data R_i , which is represented by the triplet $\{\text{data}_i, \text{cycles}_i, \text{delay}_i\}$. Time is divided into several time slots, where data_i denotes the size of the offloaded data, cycles_i indicates the number of CPU cycles required to complete the data processing, and delay_i is the maximum tolerable delay to complete the offload request R_i . The system model is assumed to consist of N task nodes, $H \geq N$ helper nodes, and fog nodes.

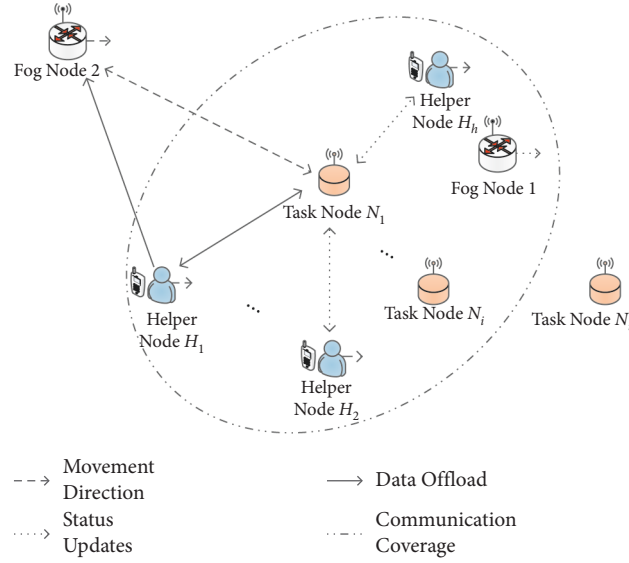


FIGURE 1: Illustration of a dynamic fog computing network at a time slot.

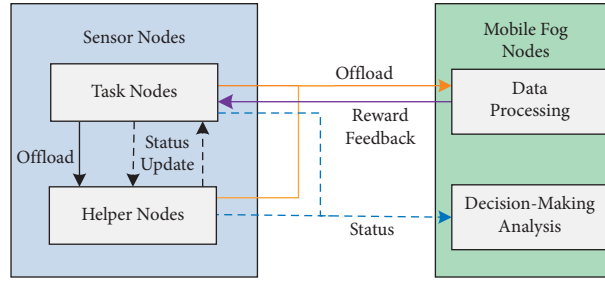


FIGURE 2: Collaborative data offload model.

TABLE 1: Symbols and their meanings.

Symbols	Meanings
k	Total number of time slots
t	An arbitrary time slot
i, h	The pairing of task node i and the helper node
hh	A match with N pairs of task and helper nodes
hh^*	An optimal match with N pairs of task and helper nodes
$X_{i,h}(t)$	The instantaneous reward for offloading data
$\theta_{i,h}$	Mean value of instantaneous rewards after k time slots
$k_{i,h}$	Number of times helper node h has been decided by task node i
$\theta_{i,h}(t)$	The mean value of rewards observed to the current time slot t
$U_{i,h}$	Task node i observes the UCB index of helper node h
$f(U_{i,h})$	A predetermined common decreasing function
$\tau_{i,h}$	Fallback time obtained according to $U_{i,h}$ after a conflict
$\Delta_{i,h} \{X^* - X_{i,h}\}$	X^* is any maximal element in the set $\{X_{i,1}, \dots, X_{i,h}\}$
$\Delta_{i,h}^{hh}(t)$	$\theta_{i,h}^{hh^*}(t) - \theta_{i,h}^{hh}(t)$
Δ_{\min}	$\min_{hh} \Delta_{i,h}^{hh}$
Δ_{\max}	$\max_{hh} \Delta_{i,h}^{hh}$
$T_{i,h}(k)$	The number of choices for nonoptimal task node and helper node pairings

Minimizing the average data offloading delay and increasing the success rate of data offloading are considered as the objectives of this paper in designing the data offloading strategy. The delay in completing the offload request R_i is

accomplished by two components: transmission delay and calculation delay. In general, since the returned results are small (a few to a few tens of bits), the delay in returning the results is negligible [35].

There are two parts of transmission delay in the model, namely, the transmission delay $D_{i,h}^{\text{trans}}$ from the task node i offloading data to the helper node h and the transmission delay $D_{h,f}^{\text{trans}}$ from the helper node offloading data to the fog node f . That is,

$$\begin{aligned} D_{i,h}^{\text{trans}} &= \frac{\text{data}_i}{r_h(t)}, \\ D_{h,f}^{\text{trans}} &= \frac{\text{data}_i}{r_f(t)}, \end{aligned} \quad (1)$$

where $r_h(t)$ is the transmission power of data offloading to the helper node h and $r_f(t)$ is the transmission power of data offloading to the fog node f . According to Shannon's formula,

$$r(t) = B \log_2 \left(1 + \frac{p(t)g(t)}{y_o(t)} \right), \quad (2)$$

where $p(t)$ is the transmit power, $g(t)$ is the channel gain, and $y_o(t)$ is the noise power. The data are processed by the fog node. The computational capacity of the fog node is assumed to be FC , from which the computational latency of the offloaded data at the fog node can be obtained.

$$D_f^{\text{comp}} = \frac{\text{cycles}_i}{FC}. \quad (3)$$

Ultimately, the delay in offloading data to the fog node for processing via helper node h can be expressed as

$$D_{i,h} = D_h^{\text{trans}} + D_f^{\text{trans}} + D_f^{\text{comp}}. \quad (4)$$

2.2. Problem Formulation. The problem of data offloading can be naturally modelled as a MAB problem. The task nodes are considered as players, and the helper nodes are considered as arms. In each round, the player expects to choose the arm with the highest reward. Similarly, during the data offloading process in each time slot, the task node offloads data to the helper node and expects a high reward, e.g., a high level of data offloading success.

The objective function of this paper is to satisfy the task node data offload latency with the highest data offload success rate and maximize system performance. The DoS (degree of satisfaction) of a single task node is defined as

$$\text{DoS}_i = \begin{cases} 1, & D_i \leq \text{delay}_i, \\ 0, & D_i > \text{delay}_i, \end{cases} \quad (5)$$

where DoS_i is the task node satisfaction, and DoS_i is one if the data offload delay is less than or equal to the maximum tolerated delay; otherwise, it is zero.

At moment t , the task node $i \in \{1, \dots, N\}$ selects a helper node $h \in \{1, \dots, H\}$ for offloading. Assuming that no other task node selects the same helper node h at that moment and that the value DoS_i is one, the task node receives an instantaneous reward message $X_{i,h}(t)$. Otherwise, if multiple task nodes select the same helper node, there is a selection conflict, and none of the conflicting task nodes receives a

reward (i.e., the reward is zero). The instantaneous reward information $X_{i,h}(t)$ is composed of random variables that are independent of each other and obey a uniform distribution. Without loss of generality, the normalized reward is $X_{i,h}(t) \in [0, 1]$. The random variable $X_{i,h}(t)$ has a mean value of $\theta_{i,h} = E_k[X_{i,h}(t)]$, and k is the total number of time slots. The value is not known in advance by the task nodes, and different task nodes have different mean values. The set of mean information of all task nodes to all helper nodes is denoted as $\vartheta = \{\theta_{i,h}, 1 \leq i \leq N, 1 \leq h \leq H\}$. In the data offloading process proposed in this paper, task nodes are constantly exploring and learning to estimate and predict the availability of helper nodes.

Considering the simultaneous existence of multiple task nodes, selection conflicts between multiple nodes are bound to exist, and therefore, an effective data offloading strategy needs to be developed to solve the problem. In the MAB framework, the regret value is used to measure the performance of a bandit algorithm [36]. Its definition can be described as the difference between the total system gain obtained by adopting the optimal strategy in the ideal case and the total gain obtained by adopting the learning strategy φ . The mathematical expression for the regret value can be expressed as follows:

$$R(\vartheta; k) = k \sum_{(i,h) \in hh^*} \theta_{i,h} - E^\varphi \left[\sum_{t=1}^k S_{\varphi(t)}(t) \right], \quad (6)$$

where hh^* is used to specify the pairing of task nodes and helper nodes that contain the N maximum rewards. $S_{\varphi(t)}(t)$ denotes the total reward of N task nodes after k time slots, as indicated in the following:

$$S_{\varphi(t)}(t) = \sum_{h=1}^H \sum_{i=1}^N X_{i,h}(t) \times I_{i,h}(t). \quad (7)$$

In the above equation, $I_{i,h}(t)$ denotes the conflict coefficient between task nodes. At moment t , when only one task node selects a certain helper node, it is considered that no conflict occurs, i.e., $I_{i,h}(t)$ is one; otherwise, it is zero.

In summary, the objective function for maximizing the satisfaction of all task nodes is expressed as

$$\begin{cases} \max \frac{1}{N} \sum_{i=1}^N \text{DoS}_i, \\ \min R(\vartheta; k). \end{cases} \quad (8)$$

3. MTDOsa-MAB

3.1. Design of Algorithms. In this paper, the bilateral matching method in game theory and the fallback timer are used to improve the MAB framework, and a data offloading strategy is proposed to solve the above problems. A bilateral match is a one-to-one, many-to-one, or many-to-many match of elements in one set with elements in another set. All task nodes are considered as one set, and all helper nodes are considered as another set. The data offloading process

can be seen as a bilateral matching of one or more task nodes to one helper node. A stable matching is a state of bilateral matching in which Nash equilibrium is reached as well as game theory [37]. Several definitions of stable matching exist here.

3.1.1. Partial Order Relations. Let A be a set and the preference relation on A be a two-way relation, i.e.,

- (1) For each $a \neq b$, there exists $a > b$ or $b > a$, and the relation is complete
- (2) $a > a$ is not valid, and the relation is non-self-referential
- (3) If $a > b$ and $b > c$, then $a > c$ is transitive

3.1.2. Matching Problem. A matching problem is described as the existence of two sets, a set N of task nodes and a set H of helper nodes. Each helper node has a preference relation on the set of task nodes. A task node i considers a helper node h_1 to be superior to h_2 , and this relationship is expressed as $i: h_1 > h_2$.

3.1.3. Bilateral Matching. The matching in this paper is a bijection from the set of task nodes to the set of helper nodes for a pairing (N_i, H_h) is included in a match, i.e., a request to offload data on behalf of the task node N_i is matched to the helper node H_h .

3.1.4. Matching Opposition. A helper node and a task node oppose a match if they believe that there exists an individual on the other side that is better than the individual they are matched to under the current match. A match is stable on the premise that there is no such opposition.

3.1.5. Stable Match. \mathbb{C} stands for a match. A match \mathbb{C} is stable if a helper node believes that another task node's request is better than its partner under match \mathbb{C} , and this task node believes that the helper node it matches is better than the other helper nodes under match \mathbb{C} . A stable matching is always present.

The advantages of the stable matching theory in helper node allocation are as follows. (i) Because the stable matching theory always specifies a stable one-to-one match based on any preference function, it avoids the multinode competition under this interference model. (ii) When the values of the preference functions of the bilateral elements are different, the stable matching theory has only unique stable matching solutions. (iii) Stable matching theory allows each participant (i.e., task node and helper node) to define its respective utility based on its local information. Being that our proposed algorithm has no significant overhead, the computational complexity of the algorithm is greatly reduced.

In [32], the authors proposed the UCB1 strategy, which is a decision learning algorithm. In a UCB1 policy, the task node selects the policy to be executed at the next moment by

analysing a series of historical policies and their resulting rewards. To provide an optimistic evaluation of the helper nodes, subject to the latency requirement, the UCB1 algorithm associates an index called the UCB index to each task node and helper node pair. The UCB index of each task node and helper node pair is calculated to estimate the reward expectation of the response, and the pair with the highest index is selected.

When performing bilateral matching, each element of the bilateral set will have a preference ranking of all elements of the other set, and this ranking rule needs to be developed first. The order of preference of task nodes to helper nodes is to first identify the helper nodes that satisfy the time delay requirement and then to rank them according to their UCB values [32], with higher UCB values having higher priority. Conversely, helper nodes are preference ordered based on the maximum tolerable offload latency of the data posted by the task node, with requests with low latency being given high priority.

At each time slot t , when a task node and a helper node are paired, all values of $(i, h) \in hh(t)$ ($hh(t)$ is a set that contains information about the pairing of N task and helper nodes) can be observed. $\theta_{i,h}(t)$ is the average reward prediction generated by pairing a task node with a helper node up to the current time slot. $k_{i,h}(t)$ is the number of times that helper node h is selected by task node i at the current time slot. $\theta_{i,h}(t)$ and $k_{i,h}(t)$ are updated in the following way:

$$\hat{\theta}_{i,h}(t) = \frac{\hat{\theta}_{i,h}(t-1)k_{i,h} + X_{i,h}(t)}{k_{i,h}(t-1) + 1}, \quad (9)$$

$$k_{i,h} = k_{i,h}(t-1) + 1.$$

Based on the above description, the pseudo-code of the algorithm is as follows. The MTDOsa-MAB algorithm is carried out iteratively.

$$\sum_{(i,g') \in hh(t)} \hat{\theta}_{i,g'}(t) + \sqrt{\frac{2 \ln t}{k_{i,g'}}}(t). \quad (10)$$

Algorithm 1 is based on the idea of the UCB1 strategy and is divided into two phases: the initialization phase and the cyclic phase. To accumulate the information available to the helper nodes, lines 2 to 15 of algorithm 1 are the initialization phase. When a task node sends an offload data request R_i , the algorithm in the initialization phase predicts the helper node that can satisfy the offload request with the maximum tolerable offload delay within the communication range, and then each task node randomly executes all feasible policies and records the reward corresponding to each policy. Immediately after each feasible policy has been executed once, the task node enters the main loop phase. Lines 16 to 30 in the pseudo-code are the main loop phase. The main loop phase is the decision-making of the helper nodes using the historical offload information and offloads feedback results accumulated during the initial phase. Decision-making in this phase is where the task node learns the historical strategy and corresponding reward information through the UCB1 equation.

```

//Initialization
WHILE Broadcast data offload requests  $R_i$  DO
  FOR  $t = 1: H$  DO
    FOR  $i = 1: N$  DO
      Update the set of candidate helper nodes.
      Calculate the predicted time delay  $\widehat{D}_{i,h}$  for the nodes in the set.
      IF  $\widehat{D}_{i,h} \leq \text{delay}_i$  THEN
        Put the helper nodes that satisfy the time delay into the set  $G$ .
      END IF
    END FOR
  FOR  $g = 1: G$  DO
    Randomly select the helper node in the set  $G$ .
     $\theta_{i,g}(t) = X_{i,g}(t); k_{i,g}(t) = 1$ .
  END FOR
END FOR
//MAINLOOP
WHILE 1 DO
  FOR  $t = (H + 1): k$  DO
    Update the set of candidate helper nodes.
    Calculate the predicted time delay  $\widehat{D}_{i,h}$  for the nodes in the set.
    IF  $\widehat{D}_{i,h} \leq \text{delay}_i$  THEN
      Put the helper nodes that satisfy the time delay into the set  $G'$ .
    END IF
    FOR  $g' = 1: G'$  DO
      Based on the UCB policy, the UCB index is calculated for each pair of task and helper node pairs.
       $\sum_{(i,g') \in hh(t)} \widehat{\theta}_{i,g'}(t) + \sqrt{2 \ln t / k_{i,g'}(t)}$ .
      Run Algorithm 2 for matching task nodes and helper nodes.
      Update  $\theta_{i,g'}(t), K_{i,g'}(t)$  accordingly.
    END FOR
  END FOR
END WHILE

```

ALGORITHM 1: MTDOsa-MAB.

The main loop process entails deciding on a many-to-many pairing that is a strategy that maximizes the overall UCB index such that the best task node and helper node can be paired in the many-to-many set.

The fallback timer was introduced to be able to determine the timing of reselection after a selection conflict. The fallback timer allows the task node that has stopped sending data after a conflict, instead of waiting for the colliding helper node to be free and then sending data immediately, to postpone (called fallback) for a time. Otherwise, when the colliding helper node is free and each task node sends data at the same time, another conflict will arise. The fallback time is determined by the UCB index of the task node to the helper node. Assume that all task nodes choose the same fallback function, which is a monotonically decreasing function of the UCB index when task and helper nodes are paired. At the beginning of each time slot after the initialization phase, the task node calculates and sets a fallback timer based on its UCB index for a particular helper node. Each task node in the network calculates the UCB index $U_{i,h}$ and maps it to a fallback time $\tau_{i,h}$ based on a predetermined common decreasing function $f(U_{i,h})$. Figure 3 shows an example of such a fallback function. The first task node that reselects to send data after a conflict is the one with the highest UCB index to the helper node.

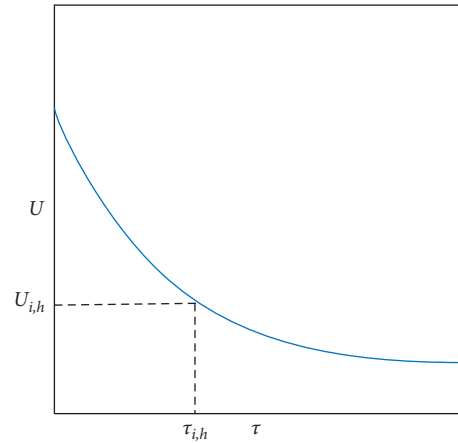


FIGURE 3: Example of a function that maps a higher UCB index to a shorter time.

The main steps of algorithm 2 are as follows: (1) In lines 3 to 5 of algorithm 2, the task node selects the helper node with the highest priority in its own preferences. (2) In lines 6 to 7 of algorithm 2, each helper node selects a particular task node from the task nodes that selected it, in accordance with each of its own preferences for task node offload requests,

```

INPUT:  $N, H$ , and preference list of bilateral elements according to Algorithm 1.
Output:  $hh(t)$ , the set contains  $N$  pairs of paired task nodes and helper nodes.
FOR  $i = 1: N$  DO
    Select the optimal helper node for each task node.
END FOR
FOR  $h = 1: H$  DO
    Rejection of redundant task nodes per helper node.
    IF determine whether  $\tau_{i,h}$  is the smallest THEN
        Rejected task node continues to select the helper node.
    ELSE
        Rejected task node enters the rejected queue.
    END IF
END FOR
WHILE rejection Queue.length! = 0 DO
    Take out  $N_i$  from rejection Queue
    FOR  $i = 1: N$  DO
        Select the optimal helper node for each task node.
    END FOR
    FOR  $h = 1: H$  DO
        Rejection of redundant task nodes per helper node.
        IF determine whether  $\tau_{i,h}$  is the smallest THEN
            Rejected task node continues to select the helper node.
        ELSE
            Rejected task node enters the rejected queue.
        END IF
    END FOR
END WHILE

```

ALGORITHM 2: Stable matching of task nodes and helper nodes.

accepts its offload data request, and then rejects the remaining task nodes' offload data requests. (3) Lines 8 to 27 of the Algorithm 2, for each task node rejected by a helper node in the previous phase, calculate the UCB index of each task node with respect to that helper node, map the UCB index to the fallback timer, and obtain the fallback time $\tau_{i,h}$. If the fallback time $\tau_{i,h}$ of this task node is the smallest among the conflicting task nodes, then the task node continues to wait for this helper node; otherwise, it enters the reject queue and continues to iterate according to its preference list. (4) When no task node is rejected, i.e., the length of the rejection queue is zero, the algorithm terminates the iteration. At the termination of the algorithm, all that is achieved is a stable match, i.e., the elements in the bilateral have no objections to this output match, and the maximum UCB index can be achieved with the task node tolerance delay requirement, the higher offload success rate and the maximum task node satisfaction are achieved.

3.2. Convergence Analysis of the MTDOsa-MAB. According to literature [32], the proposed data offloading strategy MTDOsa-MAB has the following conclusions regarding its regret value convergence analysis.

Theorem 1. *The expected regret of MTDOsa-MAB is at most*

$$\left[\frac{8NHInk}{(\Delta_{\min})^2} + N^2H^2 \left(1 + \frac{\pi^2}{3} \right) \right] \Delta_{\max}. \quad (11)$$

Proof. Each time a task node and a helper node pair up to complete a data offload, the task node receives a reward value $X_{i,h}$. Therefore, we define

$$\Delta_{i,h} \triangleq X^* - X_{i,h}, \quad (12)$$

where X^* is any maximal element in the set $\{X_{i,1}, \dots, X_{i,h}\}$. $T_{i,h}(k)$ is the number of choices for non-optimal task node and helper node pairings. That is, after the initialization process, there exists at least one task node and helper node pairing (i, h) that does not belong to the optimal set $hh^*(t)$ at time slot t when the non-optimal set $hh(t)$ is selected. $hh(t)$ is the set containing N pairs of task and helper node pairs in round t . $hh^*(t)$ is the optimal set containing N pairs of task and helper node pairs with optimal reward information. Note that the regret after k rounds can be written as

$$\sum_{X_{i,h} < X^*} \Delta_{i,h}^{hh} E[T_{hh}(k)] = \sum_{i=1}^N \sum_{h=1}^H \Delta_{i,h} E[T_{i,h}(k)]. \quad (13)$$

So, we can bound the regret by simply bounding each $E[T_{i,h}(k)]$. Denote $C_{t,k_{i,h}} = \sqrt{2\text{Int}/k_{i,h}}$. $I_{i,h}(t)$ means if $(i, h) \in hh(t)$ and $(i, h) \notin hh^*(t)$. Then, $I_{i,h}(t)$ is one; otherwise, it is zero. Because there will always be uncertainty in the estimation of the reward information generated by the helper nodes of the decision, an exploration phase is necessary. In the exploration phase of the algorithm, the set of helper nodes whose prediction delay satisfies the maximum tolerable condition is filtered and the elements in the set of helper nodes are decided by a random strategy. Ideally, in the

exploration phase, each helper node is decided at least once. In the exploitation phase, there is still a possibility for helper node h to be decided, and the number of times that helper node h is decided in the later rounds is represented by the indicator function $I_{i,h}(t)$. Then, the following equation holds:

$$T_{i,h}(k) = 1 + \sum_{t=H+1}^k \{I_{i,h}(t)\}. \quad (14)$$

Equation (14) represents the number of times a decision has been made for a particular helper node in an ideal situation. In fact, the aim of the stochastic strategy is to collect information about the historical offloading experience of the helper nodes to a limited extent. However, the stochastic strategy does not guarantee that each helper node will not be decided repetitively. Suppose l is a positive integer

of arbitrary size. Therefore, the number of times task node i decides on helper node h for data offloading is greater than or equal to equation (14), so the following equation can be obtained:

$$T_{i,h}(k) \leq l + \sum_{t=H+1}^k \{I_{i,h}(t), T_{i,h}(t-1) \geq l\}. \quad (15)$$

□

In each round of decision-making, there exists a possibility that the predicted reward information of the helper node paired with the final decision is greater than or equal to the reward information of the optimal helper node paired with that task node, so that the suboptimal helper node will be decided by the task node after learning. Therefore, the above inequality is restructured according to the UCB equation, which gives

$$T_{i,h}(k) \leq l + \sum_{t=H+1}^k \left\{ \widehat{\theta}_{hh^*(t-1)}(t-1) + C_{t-1, k_{hh^*(t-1)}(t-1)} \leq \widehat{\theta}_{hh(t-1)}(t-1) + C_{t-1, k_{hh(t-1)}(t-1)}, T_{i,h}(t-1) \geq l \right\}. \quad (16)$$

By exhaustive enumeration of $hh^*(t-1)$ and $hh(t-1)$, the following inequalities are obtained:

$$T_{i,h}(k) \leq l + \sum_{t=H+1}^k \left\{ \min_{0 < k_{i,h}^{hh^*} < t} \widehat{\theta}_{i,h}^{hh^*}(t) + C_{t, k_{i,h}^{hh^*}(t)} \leq \max_{l < k_{i,h}^{hh} < t} \widehat{\theta}_{i,h}^{hh}(t) + C_{t, k_{i,h}^{hh}(t)} \right\}. \quad (17)$$

In the first $t-1$ rounds, any helper node can be selected at most $t-1$ times; hence, $k_{i,h}^{hh^*} < t$. And, $T_{i,h}(t-1) \geq l$;

hence, $l < k_{i,h}^{hh}$. Expanding all possibilities yields the following inequality:

$$T_{i,h}(k) \leq l + \sum_{t=1}^{\infty} \sum_{k_{i,h}^{hh^*}=1}^{t-1} \sum_{k_{i,h}^{hh}=l}^{t-1} \left\{ \widehat{\theta}_{i,h}^{hh^*}(t) + C_{t, k_{i,h}^{hh^*}(t)} \leq \widehat{\theta}_{i,h}^{hh}(t) + C_{t, k_{i,h}^{hh}(t)} \right\}. \quad (18)$$

Using the converse method, it can be shown that for the situation described by the occurrence inequality $\widehat{\theta}_{i,h}^{hh^*}(t) + C_{t, k_{i,h}^{hh^*}(t)} \leq \widehat{\theta}_{i,h}^{hh}(t) + C_{t, k_{i,h}^{hh}(t)}$ to hold, at least one of the following three inequalities holds:

$$\widehat{\theta}_{i,h}^{hh^*}(t) \leq \theta_{i,h}^{hh^*}(t) - C_{t, k_{i,h}^{hh^*}(t)}, \quad (19)$$

$$\widehat{\theta}_{i,h}^{hh}(t) \leq \theta_{i,h}^{hh}(t) - C_{t, k_{i,h}^{hh}(t)}, \quad (20)$$

$$\widehat{\theta}_{i,h}^{hh^*}(t) \leq \theta_{i,h}^{hh}(t) + 2C_{t, k_{i,h}^{hh}(t)}. \quad (21)$$

For the case of $l = \lceil 8Ink / (\Delta_{i,h}^{hh}(t))^2 \rceil$, since $k_{i,h}^{hh}$ takes a range of values of $[l, +\infty)$ and therefore $k_{i,h}^{hh} \geq l \geq (8Ink / (\Delta_{i,h}^{hh}(t))^2)$, it follows that

$$\begin{aligned} & \widehat{\theta}_{i,h}^{hh^*}(t) - \theta_{i,h}^{hh}(t) - 2C_{t, k_{i,h}^{hh}(t)} \\ &= \widehat{\theta}_{i,h}^{hh^*}(t) - \theta_{i,h}^{hh}(t) - 2\sqrt{\frac{2Int}{k_{i,h}^{hh}(t)}} \\ &\geq \widehat{\theta}_{i,h}^{hh^*}(t) - \theta_{i,h}^{hh}(t) - 2\sqrt{\frac{2(\Delta_{i,h}^{hh}(t))^2 Int}{8Ink}} \\ &= \widehat{\theta}_{i,h}^{hh^*}(t) - \theta_{i,h}^{hh}(t) - \Delta_{i,h}^{hh}(t) = 0. \end{aligned} \quad (22)$$

Therefore, inequality (21) does not hold.

When $k_{i,h}^{hh} \geq (8Ink/(\Delta_{i,h}^{hh}(t))^2)$, at least one of inequalities (19) and (20) holds if it holds for inequality $\widehat{\theta}_{i,h}^{hh^*}(t) + C_{t,k_{i,h}^{hh^*}}(t) \leq \widehat{\theta}_{i,h}^{hh}(t) + C_{t,k_{i,h}^{hh}}(t)$. Applying the Chernoff–Hoeffding Boundary Theorem to inequalities (19) and (20), respectively, we get

$$\begin{aligned} P\left\{\widehat{\theta}_{i,h}^{hh^*}(t) \leq \theta_{i,h}^{hh^*}(t) - C_{t,k_{i,h}^{hh^*}}(t)\right\} &\leq e^{-4Int} = t^{-4}, \\ P\left\{\widehat{\theta}_{i,h}^{hh}(t) \leq \theta_{i,h}^{hh}(t) - C_{t,k_{i,h}^{hh}}(t)\right\} &\leq e^{-4Int} = t^{-4}. \end{aligned} \quad (23)$$

The bilateral set of the multinode data offloading policy model designed in this paper is composed of N task nodes and $H \geq N$ helper nodes. It is not difficult to obtain from the relation of inequality $\widehat{\theta}_{hh^*(t-1)}(t-1) + C_{t-1,k_{hh^*(t-1)}}(t-1) \leq \widehat{\theta}_{hh(t-1)}(t-1) + C_{t-1,k_{hh(t-1)}}(t-1)$ that at least one of the

following equations holds for $h \in [1, \dots, H]$ and $i \in \{1, \dots, N\}$ (it has NH pairing possibilities):

$$\begin{aligned} \widehat{\theta}_{1,h}^{hh^*}(t) + C_{t,k_{1,h}^{hh^*}}(t) &\leq \widehat{\theta}_{1,h}^{hh}(t) + C_{t,k_{1,h}^{hh}}(t), \\ \widehat{\theta}_{2,h}^{hh^*}(t) + C_{t,k_{2,h}^{hh^*}}(t) &\leq \widehat{\theta}_{2,h}^{hh}(t) + C_{t,k_{2,h}^{hh}}(t), \\ &\vdots \\ \widehat{\theta}_{N,h}^{hh^*}(t) + C_{t,k_{N,h}^{hh^*}}(t) &\leq \widehat{\theta}_{N,h}^{hh}(t) + C_{t,k_{N,h}^{hh}}(t), \\ \widehat{\theta}_{i,1}^{hh^*}(t) + C_{t,k_{i,1}^{hh^*}}(t) &\leq \widehat{\theta}_{i,1}^{hh}(t) + C_{t,k_{i,1}^{hh}}(t), \\ \widehat{\theta}_{i,2}^{hh^*}(t) + C_{t,k_{i,2}^{hh^*}}(t) &\leq \widehat{\theta}_{i,2}^{hh}(t) + C_{t,k_{i,2}^{hh}}(t), \\ &\vdots \\ \widehat{\theta}_{i,H}^{hh^*}(t) + C_{t,k_{i,H}^{hh^*}}(t) &\leq \widehat{\theta}_{i,H}^{hh}(t) + C_{t,k_{i,H}^{hh}}(t). \end{aligned} \quad (24)$$

Inequality $T_{i,h}(t) \geq l$ implies that $k_{i,h}(t) \geq T_{i,h}(t) \geq l$ holds. Thus, the following inequality can be obtained:

$$\begin{aligned} T_{i,h}(k) &\leq l + NH \sum_{t=H+1}^k \left\{ \widehat{\theta}_{i,h}^{hh^*}(t) + C_{t,k_{i,h}^{hh^*}}(t) \leq \widehat{\theta}_{i,h}^{hh}(t) + C_{t,k_{i,h}^{hh}}(t), T_{i,h}(t-1) \geq l \right\} \\ &\leq l + NH \sum_{t=H+1}^k \left\{ \min_{0 < k_{i,h}^{hh^*} < t} \widehat{\theta}_{i,h}^{hh^*}(t) + C_{t,k_{i,h}^{hh^*}}(t) \leq \max_{l < k_{i,h}^{hh} < t} \widehat{\theta}_{i,h}^{hh}(t) + C_{t,k_{i,h}^{hh}}(t) \right\} \\ &\leq l + NH \sum_{t=1}^{\infty} \sum_{k_{i,h}^{hh^*}=1}^{t-1} \sum_{k_{i,h}^{hh}=l}^{t-1} \left\{ \widehat{\theta}_{i,h}^{hh^*}(t) + C_{t,k_{i,h}^{hh^*}}(t) \leq \widehat{\theta}_{i,h}^{hh}(t) + C_{t,k_{i,h}^{hh}}(t) \right\}. \end{aligned} \quad (25)$$

Because of $l \geq 8Ink/(\Delta_{i,h}^{hh}(t))^2$, it follows that

$$\begin{aligned} E[T_{i,h}(k)] &\leq \left\lceil \frac{8Ink}{\Delta_{i,h}^{hh}(t)^2} \right\rceil + NH \sum_{t=1}^{\infty} \sum_{k_{i,h}^{hh^*}=1}^{t-1} \sum_{k_{i,h}^{hh}=l}^{t-1} \times \left(P\left\{\widehat{\theta}_{i,h}^{hh^*}(t) \leq \theta_{i,h}^{hh^*}(t) - C_{t,k_{i,h}^{hh^*}}(t)\right\} + P\left\{\widehat{\theta}_{i,h}^{hh}(t) \leq \theta_{i,h}^{hh}(t) - C_{t,k_{i,h}^{hh}}(t)\right\} \right) \\ &\leq \left\lceil \frac{8Ink}{(\Delta_{i,h}^{hh}(t))^2} \right\rceil + NH \sum_{t=1}^{\infty} \sum_{k_{i,h}^{hh^*}=1}^{t-1} \sum_{k_{i,h}^{hh}=l}^{t-1} 2t^{-4} \\ &\leq \frac{8Ink}{(\Delta_{i,h}^{hh}(t))^2} + NH \left(1 + \frac{\pi^2}{3} \right). \end{aligned} \quad (26)$$

Thus, the expression for the total regret value under the MTDOsa-MAB strategy is

TABLE 2: Main experimental parameter settings.

Parameters	Value
Task nodes i	6
Helper nodes h	12
Fog nodes f	2
Length of the time slot t/ms	20
Size of the offloaded data $data/MB$	$\forall_{i,data_i} \sim U(0.4, 0.6)$ [200, 600]
The volume of the data computation cycles i/M cycle	$delay_i/data_i \sim U(1.2e^{-6}, 1.5e^{-6})$
Tolerable delay of data $delay_i/s$	6
CPU processing capacity of fog nodes FC/GHz	$\forall_{h,r_h} = 12Mbits/s$
The transmission rate of helper nodes	$\forall_{f,r_f} = 12Mbits/s$
The transmission rate of fog nodes	

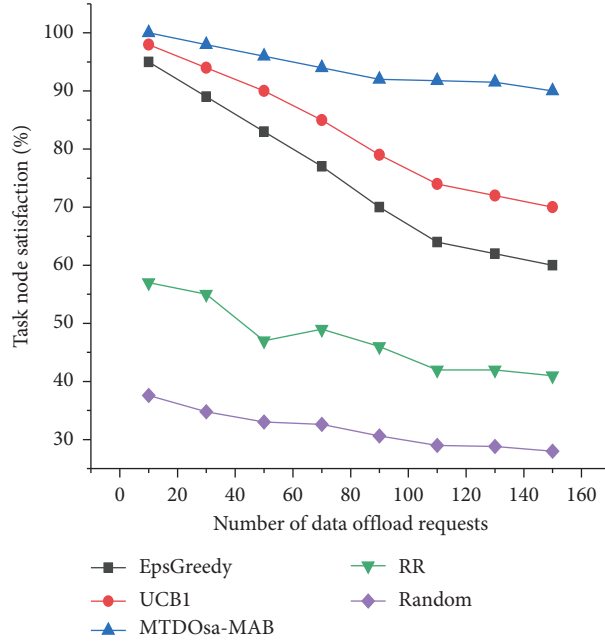


FIGURE 4: Impact of data offload requests on task node satisfaction.

$$\begin{aligned}
 R(\vartheta; k) &= k \sum_{(i,h) \in hh^*} \theta_{i,h} - E^\varphi \left[\sum_{t=1}^k S_{\varphi(t)}(t) \right] \\
 &= k\theta_{hh^*} - E^\varphi \left[\sum_{t=1}^k S_{\varphi(t)}(t) \right].
 \end{aligned} \tag{27}$$

With equations (12) and (13), equation (27) can be converted into a representation of the number of decisions made through helper nodes. Thus, the following equation can be obtained:

$$\begin{aligned}
 R(\vartheta; k) &= \sum_{X_{i,h} < X^*} \Delta_{i,h}^{hh} E[T_{hh}(k)] \leq \Delta_{\max} \sum_{X_{i,h} < X^*} E[T_{hh}(k)] = \Delta_{\max} \sum_{i=1}^N \sum_{h=1}^H E[T_{i,h}(k)] \\
 &\leq \Delta_{\max} \left[\sum_{i=1}^N \sum_{h=1}^H \left(\frac{8Ink}{(\Delta_{\min}^{hh}(t))^2} + NH \left(1 + \frac{\pi^2}{3} \right) \right) \right] = \Delta_{\max} \left[\sum_{i=1}^N \sum_{h=1}^H \frac{8Ink}{(\Delta_{\min}^{hh}(t))^2} + N^2 H^2 \left(1 + \frac{\pi^2}{3} \right) \right] \\
 &\leq \Delta_{\max} \left[\frac{8NHInk}{(\Delta_{\min})^2} + N^2 H^2 \left(1 + \frac{\pi^2}{3} \right) \right].
 \end{aligned} \tag{28}$$

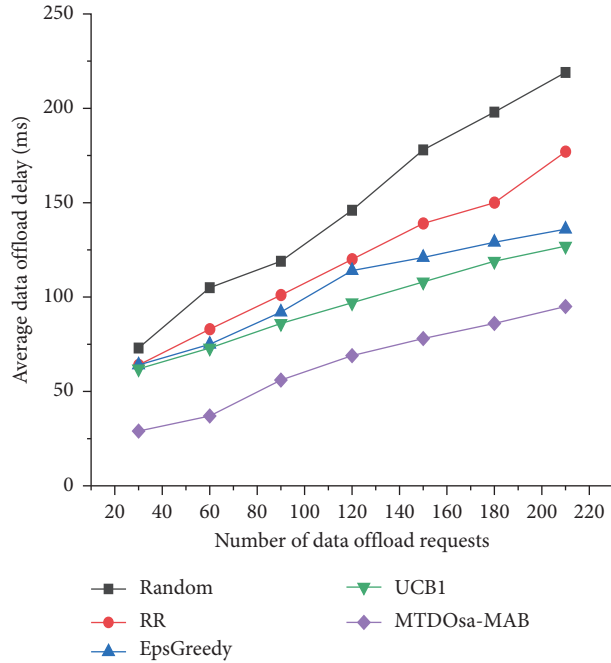


FIGURE 5: Impact of the number of data offload requests on the average offload latency.

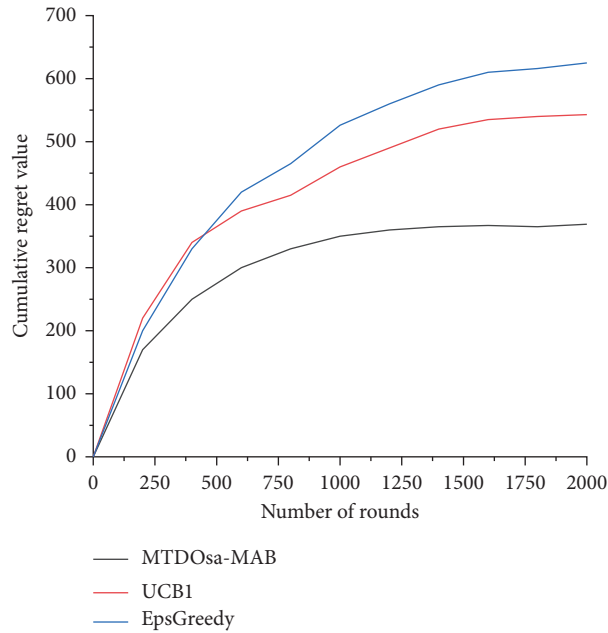


FIGURE 6: Impact of the experimental rounds on the cumulative regret value.

Therefore, the proof of equation (11) is completed.

4. Evaluation and Simulation

4.1. Data and Experimental Environment. In this paper, the effectiveness of the MTDOsa-MAB offloading strategy was evaluated by computer simulation in Python and PyCharm. The specific experimental simulation parameters of this paper are shown in Table 2.

Task nodes explore the merits of helper nodes with an unknown desired reward pattern $\theta_{i,h} = E_k[X_{i,h}]$. $\theta_{i,h}$ is the desired reward received by the task node for choosing a helper node. To simplify the process, it is assumed that the instantaneous return value $X_{i,h}$ obeys a Gaussian distribution.

The metrics evaluated in this paper are task node satisfaction, average data offload latency, cumulative regret value, and data loss rate due to selection conflicts. Task node satisfaction is the ratio of the number of data offload requests

that can be completed within a tolerable time delay to the total number of offload requests. Average data offload latency is the time taken by each policy to process various pieces of information to arrive at the offload decision and to calculate it. The cumulative regret value is the difference between the optimal offloading strategy and the actual offloading strategy regarding the reward as the number of experimental rounds increases. The loss rate due to the selection conflict is the percentage of data offload failures due to conflicts occurring against multiple nodes when different policies are used.

In order to verify the effectiveness of the MTDOsa-MAB policy, the MTDOsa-MAB policy was compared and validated with the following policies through simulation experiments.

- (1) EpsGreedy algorithm: the relationship between random numbers and a priori epsilon values is used to decide whether to select the helper node with the highest reward or to select the helper node at random.
- (2) The UCB1 algorithm considers the average reward and confidence interval of the arms. Each helper node corresponds to a confidence interval, and the helper node with the largest upper confidence interval is selected for data offloading.
- (3) The RR (round-robin) algorithm is based on round-robin scheduling; that is, helper nodes are selected in turn to offload data.
- (4) MTDOsa-MAB algorithm: learning and exploring through stable matching theory in game theory and backoff timer to improve the UCB1 strategy to select suitable helper nodes for data offloading.
- (5) Random algorithm: randomly select one of the nodes in the set of candidate helper nodes for data offloading.

4.2. Analysis of Experimental Results

4.2.1. Task Node Satisfaction. Task node satisfaction is one of the important evaluation metrics in this paper. It refers to the ratio of the number of data offload requests that can be completed within a tolerable time delay to the total number of offload requests. Figure 4 shows the impact of the number of offload requests on task node satisfaction under five different policies. From Figure 4, it can be seen that task node satisfaction under the random policy was maintained at around 31.8% when random helper nodes were selected for offloading when the main factor affecting task node satisfaction was selection conflict under the random policy, and conflicting task nodes were not rewarded. Compared to the random strategy, the RR strategy is based on time slice rotation to select helper nodes for offloading, and the probability of the selection conflict is reduced, so the satisfaction rate is around 49%. Task node satisfaction was higher for EpsGreedy, UCB1, and MTDOsa-MAB compared to both random and RR strategies. As the number of data offload requests increased, task node satisfaction tended to decrease under all three strategies. However, the rate of

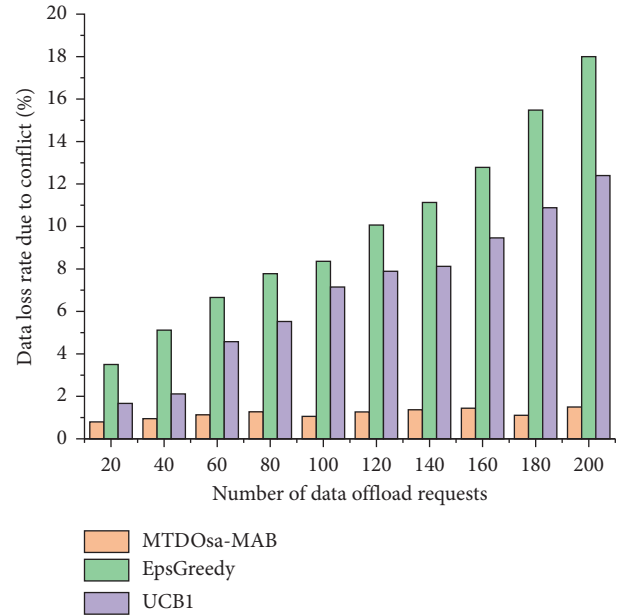


FIGURE 7: Impact of the number of data offload requests on the rate of data loss due to conflicts.

decline tended to be slower for MTDOsa-MAB, with task node satisfaction remaining above 90% when the number of tasks reached 85. Specifically, compared to EpsGreedy and UCB1, MTDOsa-MAB satisfaction increased by 32 and 22 percentage points when the number of data offload requests increased, respectively. This is due to the use of a stable matching one-to-one strategy, which effectively avoids conflict and thus rewards feedback for data offloading.

4.2.2. Average Offload Delay. Figure 5 shows the effect of the number of data offload requests on the average offload latency. As can be seen in Figure 5, the random offload policy and the RR offload policy have longer average offload latencies compared to the other three offload policies due to the nature of their policies. The EpsGreedy policy, the UCB1 policy, and the MTDOsa-MAB policy all take longer to execute as the number of tasks increases. Compared to EpsGreedy, MTDOsa-MAB saved approximately 5 ms in execution time when the number of requests was low and achieved a saving of approximately 32 ms as the number of tasks increased. This is because the EpsGreedy algorithm is based on the greedy idea of always using the current best helper node more than choosing to explore potential helper nodes that are better than the currently selected helper node; furthermore, the greed-based idea of always selecting a certain helper node frequently is prone to cause nodes due to insufficient energy consumption for wireless sensor networks “death” and therefore generates more offloading delay. Task nodes in MTDOsa-MAB always select the best choice under the current conditions based on a one-to-one matching mechanism and choose the next best choice after being rejected, with linearly correlated time complexity. In the UCB1 strategy, the confidence interval width of a helper node reflects its degree of uncertainty, i.e., the larger the

interval width, the higher the uncertainty, and vice versa, the lower the uncertainty. As the number of trials increases, the confidence intervals of the helper nodes become narrower, and the mean value of the reward and the confidence interval of each helper node are reestimated before each selection, feeling the historical results of the already tried trials. Compared to the UCB1 strategy, MTDOsa-MAB can save an average of about 9.75 ms in execution time. MTDOsa-MAB has a significant advantage in execution time and therefore can be effective in reducing latency expenditure for latency-sensitive applications.

4.2.3. Cumulative Regret Values for Several Bandit Strategies. The EpsGreedy offloading strategy and the UCB1 offloading strategy are classical stochastic bandit algorithms in the MAB framework. The MTDOsa-MAB strategy is an offloading strategy that uses stable matching theory and a fallback timer to improve the MAB framework. In the regret value comparison experiments, only three offloading strategies were considered: EpsGreedy, UCB1, and MTDOsa-MAB. Figure 6 illustrates the changes in the cumulative regret values of the three data offloading strategies as the number of experimental rounds increases. It is clear that the cumulative regret values for the three bandit algorithms grow logarithmically and increase with the number of experiments. In each round of experiments, the pairing of multiple task nodes and multiple helper nodes, whether or not they were optimal pairings, resulted in a feedback result regarding the data offloading reward information after the data offloading was completed. For each round, the difference between this feedback result and the reward feedback result generated by the optimal pairing strategy is the regret value. As the number of experimental rounds increases, the EpsGreedy and UCB1 algorithms have difficulty converging in the case of multitask node data offloading, while the cumulative regret value of MTDOsa-MAB converges more easily to a stable value due to the stable matching-based strategy that effectively solves the collision problem between nodes. In targeting the problem of multitask node offloading, a single UCB1-based strategy does not solve the conflict problem well, so the MTDOsa-MAB strategy, which improves on the UCB1 strategy, is rewarded by greatly reducing node conflicts.

4.2.4. Data Loss Rate due to Conflicts between Nodes. Figure 7 shows the rate of data loss due to selection conflicts for EpsGreedy, the UCB1 policy, and the MTDOsa-MAB policy for different numbers of offloaded data requests. It can be seen that, as the number of data offload requests increases, the percentage of data loss due to selection conflicts increases for all three strategies. Apparently, the MTDOsa-MAB strategy based on stable matching theory avoids selection conflicts of task nodes under this one-to-one selection mechanism, so its data loss rate is always below 1.5%. The data loss rates of UCB1 and EpsGreedy strategies are as high as around 12.4% and 18%, respectively. In addition, the MTDOsa-MAB strategy shows an almost constant data loss rate as the number of requests increases, while

the other two strategies show a gradual increase in data loss rate as the number of requests increases. This fluctuation is smoother in the case of the MTDOsa-MAB policy, which implies that the proposed MTDOsa-MAB policy has the potential to be extended to larger network deployments.

5. Conclusions

In this paper, for the problem of data loss in the UWSN environment, it is investigated how multiple task nodes can collaboratively offload data in a collegiate manner so that data loss due to selection conflicts can be avoided. By modelling this problem as a MAB problem, a multitask node data offloading strategy based on stable matching and fallback timers is proposed. Simulation experiments show that the MTDOsa-MAB algorithm is able to achieve higher task node satisfaction and a significant reduction in execution time and maintain a lower data loss rate compared to two classical bandit algorithms. Moreover, in the long run, its regret value converges to a smoother state. Subsequently, in addition to considering the selection conflict and competition issues, the energy demand of nodes in UWSNs is also an important factor affecting the overall network performance, which will be a major work worth investigating in the future.

Data Availability

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

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 Natural Science Foundation of China under Grant no. 62171413.

References

- [1] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, "Internet of things: vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.
- [2] M. Chiang and T. Zhang, "Fog and IoT: an overview of research opportunities," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854–864, 2016.
- [3] D. Yuan, S. S. Kanhere, and M. Hollick, "Instrumenting wireless sensor networks — a survey on the metrics that matter," *Pervasive and Mobile Computing*, vol. 37, pp. 45–62, 2017.
- [4] H. Gao, C. Liu, Y. Yin, Y. Xu, and Y. Li, "A hybrid approach to trust node assessment and management for VANETs cooperative data communication: historical interaction perspective," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2021.
- [5] T. Yu, X. Wang, and A. Shami, "A novel fog computing enabled temporal data reduction scheme in IoT systems," in

- Proceedings of the 2017 IEEE Global Communications Conference*, pp. 1–5, Singapore, December 2017.
- [6] H. Gao, Y. Zhang, H. Miao, R. J. D. Barroso, and X. Yang, *SDTIOA: Modeling the Timed Privacy Requirements of IoT Service Composition: A User Interaction Perspective for Automatic Transformation from BPEL to Timed Automata*, Mobile Networks and Applications, Netherlands, Europe, 2021.
 - [7] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, “Edge computing: vision and challenges,” *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.
 - [8] X. Ma, H. Xu, H. Gao, and M. Bian, “Real-time multiple-workflow scheduling in cloud environments,” *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4002–4018, 2021.
 - [9] A. V. Dastjerdi and R. Buyya, “Fog computing: helping the internet of things realize its potential,” *Computer*, vol. 49, no. 8, pp. 112–116, 2016.
 - [10] H. Gao, X. Qin, R. J. D. Barroso, W. Hussain, Y. Xu, and Y. Yin, “Collaborative learning-based industrial IoT API recommendation for software-defined devices: the implicit knowledge discovery perspective,” *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 6, no. 1, pp. 66–76, 2020.
 - [11] B. Rashid and M. H. Rehmani, “Applications of wireless sensor networks for urban areas: a survey,” *Journal of Network and Computer Applications*, vol. 60, pp. 192–219, 2016.
 - [12] Y. Lan, X. Wang, D. Wang, Z. Liu, and Y. Zhang, “Task caching, offloading, and resource allocation in d2d-aided fog computing networks,” *IEEE Access*, vol. 7, pp. 104876–104891, 2019.
 - [13] Y. Jiang, “Analysis and optimization of cache-enabled fog radio access networks: successful transmission probability, fractional offloaded traffic and delay,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5219–5231, 2020.
 - [14] S. Bi and Y. J. Zhang, “Computation rate maximization for wireless powered mobile-edge computing with binary computation offloading,” *IEEE Transactions on Wireless Communications*, vol. 17, no. 6, pp. 4177–4190, 2018.
 - [15] T. X. Tran and D. Pompili, “Joint task offloading and resource allocation for multi-server mobile-edge computing networks,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 856–868, 2019.
 - [16] C. Wang, C. Liang, F. R. Yu, Q. Chen, and L. Tang, “Computation offloading and resource allocation in wireless cellular networks with mobile edge computing,” *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 4924–4938, 2017.
 - [17] S. Balasubramanian and T. Meyyappan, *Game Theory Based Offload and Migration-Enabled Smart Gateway for Cloud of Things in Fog Computing*, *Computing in Engineering and Technology*, pp. 253–266, Springer, Singapore, 2020.
 - [18] S. Zhou and W. Jadoon, “The partial computation offloading strategy based on game theory for multi-user in mobile edge computing environment,” *Computer Networks*, vol. 178, Article ID 107334, 2020.
 - [19] Y. Wang, P. Lang, D. Tian, J. Zhou, and X. Duan, “A game-based computation offloading method in vehicular multi-access edge computing networks,” *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4987–4996, 2020.
 - [20] J. Li, H. Chen, Y. Chen, and Z. Lin, “Pricing and resource allocation via game theory for a small-cell video caching system,” *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 8, pp. 2115–2129, 2016.
 - [21] P. Kortoçi, L. Zheng, C. Joe-wong, M. D. Francesco, and M. Chiang, “Fog-based data offloading in urban IoT scenarios,” in *Proceedings of the IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, pp. 784–792, Paris, France, May 2019.
 - [22] S. Chen, X. Zhu, H. Zhang, C. Zhao, G. Yang, and K. Wang, “Efficient privacy preserving data collection and computation offloading for fog-assisted IoT,” *IEEE Transactions on Sustainable Computing*, vol. 5, no. 4, pp. 526–540, 2020.
 - [23] S. Chen, Y. Zheng, W. Lu, V. Varadarajan, and K. Wang, “Energy-optimal dynamic computation offloading for industrial IoT in fog computing,” *IEEE Transactions on Green Communications and Networking*, vol. 4, no. 2, pp. 566–576, 2020.
 - [24] Q. Wang and S. Chen, “Latency-minimum offloading decision and resource allocation for fog-enabled Internet of Things networks,” *Transactions on Emerging Telecommunications Technologies*, vol. 31, 2020.
 - [25] K. Guo, C. Yang, and T. Liu, “Caching in base station with recommendation via Q-learning,” in *Proceedings of the 2017 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, San Francisco, CA, USA, March 2017.
 - [26] B. Dab, N. Aitsaadi, and R. Langar, “Q-learning algorithm for joint computation offloading and resource allocation in edge cloud,” in *Proceedings of the 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, pp. 45–52, Washington DC, USA, April 2019.
 - [27] D. He, W. Chen, and L. Wang, “Online learning for auction mechanism in bandit setting,” *Decision Support Systems*, vol. 56, no. 1, pp. 379–386, 2013.
 - [28] P. Matikainen, P. M. Furlong, R. Sukthankar, and M. Hebert, “Multi-armed recommendation bandits for selecting state machine policies for robotic systems,” in *Proceedings of the 2013 IEEE International Conference on Robotics and Automation*, pp. 4545–4551, Germany, in Karlsruhe, March 2013.
 - [29] L. Weng, Y. Xu, Y. Li, and R. Nayak, “Distributed recommender profiling and selection with gittins Indices,” in *Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence (WI 2006 Main Conference Proceedings) (WI’06)*, pp. 790–793, Hong Kong, China, December 2006.
 - [30] B. Awerbuch and R. Kleinberg, “Competitive collaborative learning,” *Journal of Computer and System Sciences*, vol. 74, no. 8, pp. 1271–1288, 2005.
 - [31] R. Gross, A. I. Houston, E. J. Collins, and M. M. John, “Simple learning rules to cope with changing environments,” *Journal of The Royal Society Interface*, vol. 5, no. 27, p. 1193, 2008.
 - [32] P. Auer, N. Cesa-Bianchi, and P. Fischer, “Finite-time analysis of the multiarmed bandit problem,” *Machine Learning*, vol. 47, no. 2, pp. 235–256, 2002.
 - [33] Y. Y. Tan, L. Chen, and M. T. Zhou, “Online learning-based task offloading algorithms for dynamic fog networks,” *Journal of University of Chinese Academy of Sciences*, vol. 37, no. 5, pp. 688–698, 2020.
 - [34] D. Gale and L. S. Shapley, “College admissions and the stability of marriage,” *The American Mathematical Monthly*, vol. 120, no. 5, pp. 386–391, 2013.
 - [35] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, “A comprehensive survey on fog computing: state-of-the-art and research challenges,” *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 416–464, 2018.

- [36] S. Bubeck and N. Cesa-Bianchi, "Regret analysis of stochastic and nonstochastic multi-armed bandit problems," *Foundations and Trends® in Machine Learning*, vol. 5, 2012.
- [37] N. Chen and M Li, "Research and evolution of stable matching algorithm," *Communications of the CCF*, vol. 9, no. 10, pp. 15–18, 2013.

Research Article

Protecting Location Privacy in IoT Wireless Sensor Networks through Addresses Anonymity

Qiong Zhang ^{1,2} and Kewang Zhang ³

¹School of Computer Science and Technology, Xi'an University of Posts and Tele-communications, Xi'an 710121, China

²Shaanxi Key Laboratory of Network Data Analysis and Intelligent Processing, Xi'an 710121, China

³School of Computer Science, Xi'an Jiaotong University, Xi'an 710049, China

Correspondence should be addressed to Qiong Zhang; zhangqiong@xupt.edu.cn

Received 17 August 2021; Revised 1 December 2021; Accepted 27 March 2022; Published 18 April 2022

Academic Editor: Yuyu Yin

Copyright © 2022 Qiong Zhang and Kewang Zhang. 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.

Location privacy is very important for event-triggered type of Wireless Sensor Networks (WSNs) applications such as tracking and monitoring of wild animals. Most of the security schemes for WSNs are designed to provide protection for content privacy. Contextual privacy such as node identity anonymity has received much less attention. The adversary can fully explore such contextual information to disclose the location of critical components such as source nodes or base station. Most existing schemes provide location privacy at network layer. As no measures are taken to provide node identity anonymity at data link layer, the adversary can launch traffic analysis attacks to jeopardize location privacy. In this paper, a scheme named HASHA is proposed to defend against traffic analysis attacks through hashed one-time addresses. Hashed results of payload are used to create dynamic one-time MAC addresses between the communication pairs. Because of inevitable wireless frame errors, it is impossible for adversaries to track dynamic addresses. Therefore, HASHA can provide strong node identity anonymity, which makes traffic analysis attacks much more difficult and provides better location privacy. Simulations and analysis results show that HASHA can provide better location privacy with limited communication overheads, which is particularly suitable for resource-limited WSNs.

1. Introduction

A typical Wireless Sensor Network (WSN) is composed of dozens to thousands of tiny, low-cost, and resource-constrained sensor nodes that are self-organized as an ad hoc network to monitor the physical world. One type of applications of WSNs is wildlife habitat monitoring, in which all sensor nodes are deployed randomly to monitor the target of interests [1]. Detection events are reported from the source node to the base station in a multihop fashion. Unattended operation and open wireless communication channel make WSNs vulnerable to attacks. However, as sensor node has limited memory, energy, and communication resources, traditional security techniques cannot be used in WSNs. Light-weighted schemes are required to achieve secure communication for WSNs [2].

Security for WSNs has focused on security services that provide authentication, confidentiality, integrity, and availability [3, 4]. Such techniques belong to content privacy. Now, however, there is a growing interest in contextual privacy, which focuses on hiding the contextual information of WSNs. Location information of key components is one of the most important contextual privacy parts that should be protected.

In the wildlife monitoring application, all sensor nodes detect occurrence of the target animal to the base station. In the case that one sensor node (source node) detects target, a packet is generated and sent to the base station hop by hop to report occurrence of the target. In such applications, geographic locations of the source node and base station are sensitive information that should be protected [5]. The base station is the only gateway to outside networks, and the

source node reveals physical location of wildlife. If the location of base station is disclosed by the adversary, the capture of the base station can make the entire network nonfunctional. And if the location of source node is disclosed, the adversary can find the animal easily because the geographic location of source node and the target must be very close. Therefore, providing location privacy of source node and base station is of great importance in such applications.

Existing techniques provide location privacy at network layer. Random Walk has packets that follow random route while forwarding the packets from the source node to base station [6, 7]. As it is difficult to the adversary to backtrack to the source node while random route is used, location privacy of source node is achieved. Dummy Data Source scheme invites some fake source nodes into the WSNs to confuse the adversary and provide location privacy [8, 9]. However, both schemes introduce additional communication overheads, which consume much more energy. For example, if the average hops count from the source node to base station is twice than that of shortest path, the energy consumption is twice too. For the same reason, if one more fake source node is added to the network, the power consumption doubled.

The adversary may launch traffic analysis attacks to find the geographic locations of the source node. As the content information is protected by the encryption techniques, the adversary cannot decrypt its contents without keys. However, as the contextual information is not well protected, it can be used to launch successful traffic analysis attacks.

The adversary first captures frames around the base station. The structure of frame at the data link layer data is $\langle DA||SA||\text{payload}||FCS \rangle$. Payload is content from upper layer, FCS is the frame checksum, DA is receiver address, and SA is transmitter address. Supposing that the captured frame is $\langle BS||B||\text{payload}||FCS \rangle$, the adversary cannot get any information from the payload because it is encrypted. However, two addresses indicate that the frame is from node B to the base station. To find the geographic location of node B, the adversary captures a series of data packets from node B at different locations and moves towards locations where stronger Received Signal Strength (RSS) presents. After finding the geographic location of node B, the adversary can find the next node by the same way. To find the source node, the adversary continues such process until no more next nodes are detected. Source location privacy was compromised.

Two steps are used repeatedly by the adversary to locate the source node. The first is forwarding relationship analysis. The adversary knows the address of base station by traffic analysis. Then, it knows the forwarding node closer to the source node by analyzing frames to the base station. The second step is to move closer to the forwarding node by analyzing RSS. Apparently, the addresses in data link layer frames are vital for successful traffic analysis attacks. It is much more difficult or impossible for the adversary to launch traffic analysis attacks if the addresses in the frame are well protected.

One way to hide node address is to break the relevance between physical node and the address of the node. For example, if node X and node X' in WSN have the same

address ID_x, as two nodes have the same address but are deployed at different geographic location, the adversary cannot locate the node(s) by analyzing the RSS [9]. Thus, traffic analysis attacks can be eliminated. Of course, above simple scheme introduces great trouble to normal operation of networks. But breaking the relevance between physical node and the address is an effective way to defend against traffic analysis attack and provide location privacy [10–13].

Another way to break the relevance between physical node and the address is introducing more addresses to node that cannot be distinguished by the adversary. If node X communicates with base station using a serial of identities $\langle X_1, X_2, X_3, \dots, X_n \rangle$, and only node X and the base stations know that the addresses belongs to node X, the adversary cannot learn the communication relationship to track the source node by traffic analysis attacks [14].

Based on such observations, this paper proposes a novel scheme to provide location privacy at data link layer. The contributions of this paper are threefold: First, the proposed scheme protects location privacy at data link layer, which is more effective to defend against traffic analysis attacks. As compared to schemes at network layer, the proposed scheme introduces negligible communication overheads. Second, in tracking and monitoring applications, location privacy of the source node and that of base station are both very important. Exposure of base station will endanger the whole WSN, while source node location discloses the position of the target. Source location privacy and base station privacy are both provided in the proposed scheme. Existing schemes emphasize on either the source location privacy or base station location privacy. Third, the proposed scheme defends traffic analysis attacks through address anonymity, which can provide location privacy against both inner attackers and outside attackers. Protection against inner attackers is particularly important, because node compromise is fairly easy for unattended WSNs and the compromised node can be an inner attacker with some software modifications. Existing address anonymity schemes can only defend against outside attackers.

2. Related Works

Phantom Routing belongs to Random Walks type schemes that provide location privacy for WSNs [13–15]. To prevent being located by step-by-step tracing, the source node sends each packet to a randomly selected forward node. This forward node is called a Phantom node. On receiving the packet to be forwarded, the Phantom node routes the packet to the base station using broadcasting. Suppose that an adversary launches traffic analysis attacks to find the geographic location of the source node. As the Phantom node sends packets to base station via broadcasting instead of unicasting, it is fairly difficult for the adversary to trace to the Phantom node using traffic analysis. However, energy consumption in Phantom Routing is much greater than unicasting type of schemes, because broadcasting is used to forward packets from Phantom node to base station. To reduce power consumption of broadcasting, another scheme named Phantom Single-path Routing scheme (PSRS) is

proposed [16]. Different from original Phantom Routing, the Phantom node in PSRS routes packets to base station via unicast. As the source node selects different Phantom node for each packet, different paths are used for different packets. Therefore, it is still very difficult to locate source node via traffic analysis attacks. The PSRS can reduce power consumption because broadcasts are eliminated. But the randomly selected paths are much more power-consuming than the shortest ones.

Another type of schemes that provides location privacy is dummy source node [17, 18]. Fake source nodes are introduced to obfuscate real source node. The basic idea of such schemes is quite simple. There are many source nodes in the WSN, only one node is real source node, and other nodes are fake source nodes. The adversary can no longer see which one is real source node, even if success traffic analysis attacks are launched. Obviously, one additional fake source node introduces additional network traffic, which corresponds to additional energy consumption. The more fake source nodes introduced, the more power consumption.

Simple Anonymity Scheme (SAS) is the first scheme proposed to provide location privacy at data link layer by hiding the address. Each node communicates with neighbor using a pseudonym [19]. A large range of pseudonyms are used, and each node is assigned with a subspace of the pseudonym space. Both nodes of the communication pair at data link layer know each other's pseudonym spaces. Both nodes use different pseudonym within its pseudonym spaces. Therefore, the adversary cannot identify the physical node if the pseudonym space is unknown to it. The main drawback of SAS is that it cannot protect address anonymity if there is an internal attacker. For example, if the adversary has the full pseudonym space and the subspace allocation for each node, it can capture frame and compare each address with the pseudonym space and finally find out the physical node for each address. Another drawback of SAS is that each node must store pseudonym space for each neighbor, which introduces great storage overheads if many neighbors exist.

Cryptographic Anonymity Scheme (CAS) uses a keyed hash function to generate the pseudonym used for communication between the communication pairs at data link layer [20, 21]. Before deployment, the communication pairs are assigned a key k for pseudonyms generation. After deployment, the communication pairs create pseudonyms with a random number r and a sequence number seq . The i th pseudonym can be expressed as $ID_i = H_k(r \oplus seq)$. Before frame transmission, a different sequence number seq is used, so each frame has different pseudonym. CAS reduces storage overhead at the expense of additional computation overheads. Apparently, CAS cannot prevent internal attackers from finding out that some pseudonyms belong to a physical node if the key k is stolen by the adversary via compromising.

The schemes mentioned above either cannot protect location privacy in the presence of inner attackers or consume too much energy resource because of communication overheads. And most of the schemes proposed focused on protecting location privacy of source node. In this paper, the proposed scheme protects location privacy at data link layer by address anonymity. The address anonymity can resist

traffic analysis attackers launched by both outside attackers and inner attackers. With a modification to the network layer, the scheme can provide location privacy with much less energy consumption. Location privacy of both base station and source node can be protected with the proposed scheme.

3. Network and Adversary Models

3.1. Network Model. In this paper, it is assumed that many nodes are randomly deployed to monitor the geographic location of the target. Each node is capable of communication, computation, and sensing. All nodes in the network are powered by batteries and work in an unattended manner [21]. Therefore, power efficiency is the most important design consideration for both software and hardware. There is only one base station in the WSN, which is the gateway to outside networks.

All nodes in the WSN are working coordinately to detect the presence of a target. Any tracking approaches can be used to detect the target, provided that they are power efficient. The node that detects the target is called the source node. On detecting the target, the source node sends packets to the base station to report the information of the target. The source node reports to the base station for fixed time interval until the target moves outside the detection radius. Other nodes in the WSN sleep unless they are requested to forward the packets from the source node to the base station.

3.2. Adversary Model. Location privacy of the source node and that of base station are both important [21–23]. We consider two types of adversary. The first type of adversary is interested in catching the animals that are monitored by the WSN. Because the network traffic from the source node is an excellent guide to find the animals, the adversary attempts to find the node closer to the source node (and the animal) through traffic analysis attacks. The second type of adversary attempts to find the base station and damage it, which will make the entire WSN useless. With the same approach, the adversary can find the base station.

Only local adversary is considered in this paper. The reason is that global adversary requires much more expensive devices than the local adversary. Some researches suppose that the adversary is equipped with wireless devices that can cover the whole WSN. Such devices should be very expensive. Many nodes that are geographically separated in a WSN may transmit simultaneously without collision at the respective receivers. But as the wireless device of adversary can hear many simultaneous transmissions, collision may occur at the adversary. Expensive wireless device may not necessarily lead to better attack results. Therefore, we only consider local adversary.

Only passive adversary is considered in this paper. That means the adversary never transmits to avoid being detected by WSNs. To locate the source node and base station, the adversary captures and analyzes frames to get the communication relationship among nodes. To move closer to the source node or base station, the adversary may move closer to a node by comparing RSS from different locations.

The adversary may launch another traffic analysis attack named time correlation [24–27]. After detecting the target, the source node sends a packet to the next node closer to the base station to notify the event. The next node also relays the packet to a node closer to the base station. The adversary can observe the correlation in transmitting time between one node and the next node to find the route to the source node or base station. For a simple example, if the adversary notices that after node A transmits a packet, node B transmits a packet with the same size, it can learn that node A is closer to the source node, and node B is closer to the base station. The reason is that, in a typical tracking and monitoring application, only the source node generates packets and the base station is the only destination.

As nodes in a WSN are frequently deployed in unattended environment, node may be captured by the adversary. The adversary can analyze the software and hardware of the node. It is possible for the adversary to get the pairwise shared keys or other sensitive information [28, 29]. Even more, modification to the software is also possible if the adversary has enough skills [30–34]. The captured node then becomes an internal attacker. Protecting attacks launched by an internal attacker is much more difficult than that launched by outside attackers [35–37].

4. Proposed Location Privacy Scheme

4.1. Address Anonymity Scheme. A node may have different identity at different layers of the network protocol stack. Identity at network layer and upper layers can be protected by cryptographic system. However, identity at data link layer has not been well protected in popular wireless standards such as 802.15.4 and Lora [31, 32]. Without introducing confusion, identity and Media Access Control (MAC) address are used interchangeably in this paper. The frame structure at data link layer can be illustrated in Figure 1.

DA is destination address of the frame. SA is the address of the sender. Payload is data from upper layer. Upper layer of data link layer is network layer. Therefore, payload at data link layer is usually packet at network layer plus control information. FCS is frame checksum.

As wireless channel is error prone, Automatic Repeat request (ARQ) is used to provide reliable data transmission. On receiving DATA frame, the receiver responses an ACK frame to inform the sender that it has received the DATA frame successfully. Structure of ACK frame is illustrated in Figure 2.

As compared to DATA frame, the ACK frame is much shorter. But both destination address and source address are included in the ACK frame. Destination address is the address of DATA frame sender, and source address is the address of receiver.

As elaborated in the adversary model, SA and DA of each node are known to the adversary who captures frames through eavesdropping. By analyzing these addresses, the adversary knows how many nodes in the WSN and the MAC address of each node. Furthermore, based on such captured frames, the adversary can deduce the routing information of the network or even locate a certain node in the network.

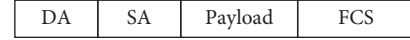


FIGURE 1: DATA frame at the data link layer is composed of destination address, source address, payload, and frame checksum.



FIGURE 2: ACK frame at the data link layer is used for reliable communication.

Therefore, unprotected addresses at data link layer are the root factor jeopardizing location privacy.

To protect the addresses in the DATA frame and ACK frame, a hash function Hash() and a keyed hash function HMAC() are used. For DATA frames from node a to node b , both nodes keep the following variables: Key[$a > b$], IDS[$a > b$], IDD[$a > b$], where Key[$a > b$] is a secret key to protect the addresses in MAC frames. IDS[$a > b$] is the source address assigned to DATA frame and IDD[$a > b$] is the destination address assigned to DATA frame.

Nodes in the WSN know each other by beacon broadcasting. For example, node a knows ID b after receiving beacons from node b . Node a and node b initialize these variables as follows:

- (i) Key[$a > b$] \leftarrow 0xFFFFFFFF
- (ii) IDS[$a > b$] \leftarrow HMAC(Key[$a > b$], ID a)
- (iii) IDD[$a > b$] \leftarrow HMAC(Key[$a > b$], ID b)

For the first DATA frame from node a to node b , two hashed addresses IDS[$a > b$] and IDD[$a > b$] are used. After ACK frame from node b to node a , both nodes update key and addresses:

- (i) Key[$a > b$] \leftarrow Key[$a > b$] \oplus Hash(payload)
- (ii) IDS[$a > b$] \leftarrow HMAC(Key[$a > b$], ID a)
- (iii) IDD[$a > b$] \leftarrow HMAC(Key[$a > b$], ID b)

As payload of the first frame is received successfully by node b , it has the same Key[$a > b$], IDS[$a > b$], and IDD[$a > b$] as node a . We call this a secret key update process.

As it is well known, wireless channel is error prone. Both DATA frame and ACK frame may be corrupted. On receiving corrupted DATA frame, node b will not acknowledge node a with ACK frame. Both nodes will not update the key. Node a retransmits the DATA frame using the old key as described above.

In another scenario, DATA frame is received correctly by node b , but the ACK frame to node a is corrupted or lost. Node a retransmits the DATA frame as it does not receive the ACK frame correctly. But node b has already updated the key. Key mismatch problem occurs.

To address key mismatch problem, two temporary addresses are used by node b to avoid key mismatching. Node b keeps a copy of old address on receiving DATA frame successfully. If the received address in next DATA frame does not match the **new** address, it will try to match the **OLD** temporary address. If the old one matches, that means this DATA frame is a retransmission. Just reply node a with the ACK frame that already transmitted.

Node a and node b repeat such process for all the frames from node a to node b . Such process creates one-time source address and destination address. We call it a dynamic address or hashed address (HASHA) (Algorithm 1).

HASHA updates key for the communication pairs after a successful data transmission. And the one-time secret is further used to update the addresses, which creates dynamic addresses. Such process can create great difficulty to the adversary.

Figure 3 illustrates a typical scenario that an adversary captures frames from node A to node B. Initially, as the adversary knows MAC addresses node A and node B through capturing beacons. The adversary knows the initial value of $\text{Key}[a \rightarrow b]$. Both node B and the adversary receive DATA1 and DATA2 successfully.

At time $t1$, ACK3 is corrupted and node B does not receive it correctly; node B receives the retransmission with backup key. This will not introduce trouble to the adversary.

At time $t3$, DATA4 is not received correctly by the adversary; as the adversary is passive attacker, it cannot ask node A for retransmission. Thereafter, the adversary cannot trace frame from node A to node B after time $t3$. The reason is that the addresses used by node A and node B are created by HMAC function with key5. Key5 is created by all previous payloads from node A to node B. The result is that the dynamic one-time addresses of the following frames from node A to node B are indistinguishable to the adversary. Address anonymity is achieved.

As wireless frames are error prone because of collision and interference, corrupted frames at the adversary will prevent it from identifying nodes in the WSN. Therefore, with HASHA, the eavesdropping adversary cannot identify number of nodes in the WSN. Therefore, it cannot retrieve the routing information. Without forward routing information, the adversary cannot trace the source node and base station.

4.2. Possible Attacks against HASHA and Countermeasures.

Even though the addresses are hidden by address anonymity, the adversary can still launch two types of attacks to jeopardize the source node and base station location privacy. The first attack is time correlation attack. The adversary can deploy several attack nodes in the target WSN. These nodes are carefully deployed so as all communications in the WSN can be captured. The geographic coordinates of these nodes are recorded in a center control point. The attack nodes can communicate with each other to report captured frames to the center control point. Time synchronization algorithm can be used to distribute global time to these nodes. Therefore, the resulting attack network can be used to detect transmission all over the network.

In a typical event-triggered monitoring type of WSN, network traffic in the networks is triggered by event detected by the source node. The source node reports event to the base station with the help of the forwarding nodes. On forwarding the event to the base station, transmission time of the forwarding nodes may disclose the location of source node and the base station.

As illustrated in Figure 4, nodes $a1$, $a2$, and $a3$ are nodes of the attack network to monitor network traffic.

Node S is source node and node D is base station. Node A and node B are relay nodes. To report event from node S to base station D, node S sends packet to node A, and node A sends packet to base station D with the help of node B. The transmission time is illustrated in Figure 5. By analyzing the transmissions time serial, the adversary can find that node S is the source node and node D is the base station, which are located near node $a1$ and node $a3$, respectively. The location privacy of source node and that of base station are jeopardized. Of course, with the help of address anonymity, the adversary cannot identify node S, node A, and node B. But it can still detect that the source node is close to $a1$ and the base station is close to node $a3$. As locations of node $a1$ and node $a3$ are known to the adversary, address anonymity cannot eliminate such time correlation attacks.

Time correlation attacks use the pattern of occurrence of transmissions along the forwarding path to find the source node and base station. For example, for each event, transmission of node S is always followed by transmission of node A, because node A is the next hop of the forwarding path. Transmission serial $\{S1, A1, B1\}$, $\{S2, A2, B2\}$, and $\{S3, A3, B3\}$ disclose forwarding relationship among nodes, which can be used to jeopardize source node and base station location privacy. Breaking the transmission pattern is important to eliminate time correlation attacks. The solution is to introduce random delay while forwarding packet. As illustrated in Figure 6, node S and node A delay random time for packets. The resulting transmissions serial $\{S1, A1, S2, A2, S3, B1, B2, A3, B3\}$ does not disclose any forwarding relationship anymore. With the help of address anonymity, it is more difficult for the adversary to locate the source node and base station via time correlation attacks.

The formal description of random delay can be expressed as follows.

Each node forwards packets with random delay, which is effective to prevent time correlation attacks. Of course, random delays may introduce delay to event reporting to base station. In some applications, timely delivery of important packet to base station is very important. To provide higher priority to such important data, a smaller random delay $rand$ in Algorithm 2 can be selected.

Another traffic analysis attack is traffic outlining attack. As address anonymity and random delay are used to prevent traffic analysis attack and time correlation attack, respectively, it is much difficult for adversary to launch attacks based on node address and forwarding relationship. But the adversary can still attack the target network via traffic outlining attack. As mentioned above, the adversary can deploy many attack nodes in the network to launch a distributed attack. For example, in the network illustrated in Figure 7, source node S reports to base station B. The adversary can deploy many attack nodes to monitor network traffic. As network traffic of event-triggered WSN is characterized from source node to base station, it is impossible for the adversary to outline the traffic without the help of distributed attack nodes. All attack nodes report to the adversary only in the presence of traffic in a certain time period. As the geographic location of attack nodes is known to the adversary, the adversary knows geographic


```

if node is sender then
  Key[a->b] ← 0xFFFFFFFF;
  if node has frame to be transmitted then
    IDS[a->b] ← HMAC(Key[a->b], IDa);
    IDD[a->b] ← HMAC(Key[a->b], IDb);
    Send DATA frame { IDS[a->b], IDD[a->b],payload, FCS};
    Create timer Stimer with a certain timeout;
  end
  if an ACK frame is received then
    for each neighbors do
      if FCS checksum OK and IDS[a->b] from ACK frame == IDS[a->b] then
        //generate new key
        Key[a->b] ←Key[a->b] ⊕ Hash(payload);
        //generate new addresses
        IDS[a->b] ←HMAC(Key[a->b], IDa);
        IDD[a->b] ←HMAC(Key[a->b], IDb);
        kill timer Stimer;
      end
    end
  end
  if Stimer timeout then
    Send DATA frame { IDS[a->b], IDD[a->b],payload, FCS};
  end
end
if node is receiver then
  Key[a->b] ← 0xFFFFFFFF;
  IDS[a->b] ← HMAC(Key[a->b], IDa);
  IDD[a->b] ← HMAC(Key[a->b], IDb);
  IDSo[a->b] ← HMAC(Key[a->b], IDa);
  IDDo[a->b] ← HMAC(Key[a->b], IDb);
  if a DATA frame is received then
    for each neighbor do
      if FCS checksum OK and IDD[a->b] from frame == IDD[a->b] then
        //save old addresses
        IDSo[a->b] ← IDS [a->b];
        IDDo[a->b] ← IDD [a->b];
        //generate new key
        Key[a->b] ←Key[a->b] ⊕ Hash(payload);
        //generate new addresses
        IDS[a->b]←HMAC(Key[a->b], IDa);
        IDD[a->b]←HMAC(Key[a->b], IDb);
        deliver frame to upper layer;
        send ACK frame { IDDo[a->b], IDSo[a->b], FCS};
      else if FCS checksum OK and IDD[a->b] from frame == IDDo[a->b] then
        //DATA frame already delivered
        send ACK frame { IDDo[a->b], IDSo[a->b], FCS};
      end
    end
  end
end

```

ALGORITHM 1: Address anonymity.

distribution of traffic in a certain time period. If the attack nodes are deployed dense enough, the network traffic outline can be drawn by the adversary. Figure 7 illustrates such attack. Obviously, traffic outlining attack cannot be eliminated by address anonymity and random delay.

The solution to traffic outlining attack is circular traffic, which is illustrated in Figure 8. Network traffic from the source node to the base station follows two semicircle paths.

And the two semicircle paths form a circular path. Source node selects one of the two semicircles randomly to forward packet. As to the adversary, traffic outlining attack cannot find the source node and base station because traffic in the networks forms a circular path (Algorithm 3).

The proposed solution can eliminate traffic outlining attacks effectively, because the source node and base station are hidden in a circular traffic outline. Combined with

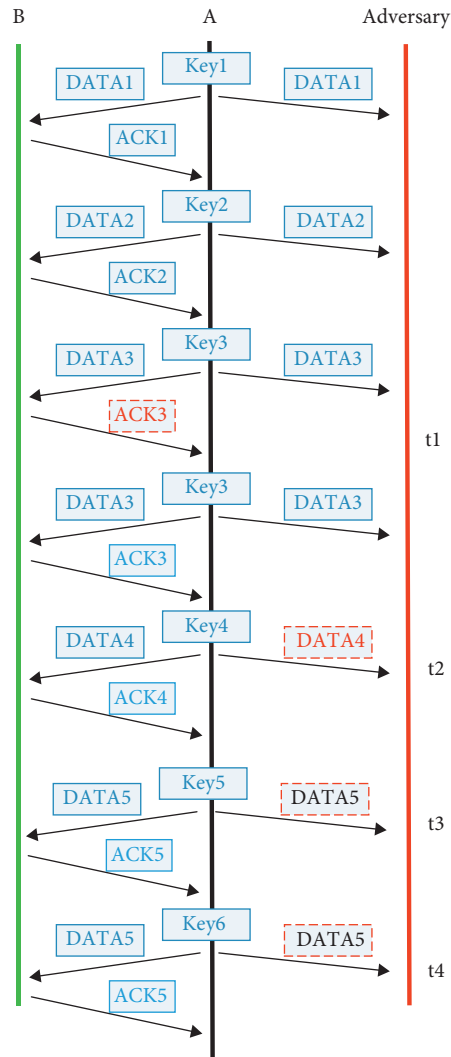


FIGURE 3: Frame error leads to address confusion.

address anonymity and random delays, traffic analysis attacks can be well addressed.

4.3. Performance Analysis. Efficiency is among the most important design considerations for data link layer schemes. Two different hash functions are used in HASHA, hash(), and HMAC(). hash() is used to generate hash value of payload, and the output is further used to create the key for HMAC(). According to the characteristics of HMAC() function, the computation complexity of brute-force attacks on hash key is 2^k , where k is the length of the key. Long key improves security strength. Therefore, the hashed results of hash() should be long enough to defend against brute-force attacks. Tiger/192 [38] is a good candidate for hash() because it is almost as fast as CRC32, but the width of the output is 192 bits. As HMAC() is used to create one-time address, performance is the top design consideration for HMAC() selection. Efficient MAC functions such as UMAC/32 [39] are a good candidate for HMAC().

Suppose that UMAC/32 is used for HMAC() and Tiger/192 is used for hash() in HASHA. According to the performance analysis of hash functions [38], the performance of UMAC/32 is 1 cycle per byte and Tiger/192 is 8.1 cycles per byte. From the illustrated HASHA process, hash() is called 1 time and HMAC() is called 2 times for both the sender and the receiver to transmit one frame. Supposing that the length of frame is len bytes and the MAC address is fixed to 6 byte, HASHA requires $len * 8.1 + 2 * 1$ cycles for one frame transmission and reception.

5. Performance Simulation

We use ns-2 to evaluate the energy consumption of HASHA. Several nodes are deployed over 200 m * 200 m network field, and the base station is located at the center. The nodes' radio transmission radius is 50 m.

We deploy only one source node to report event to the base station. The total number of nodes in WSN changes from 50 to 400 in 50 steps. We record the average power

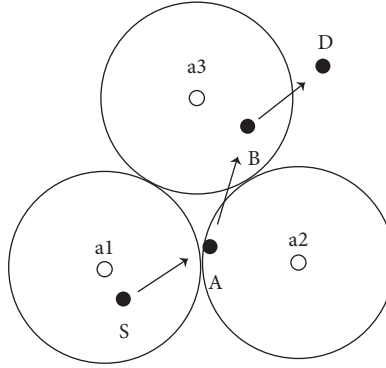


FIGURE 4: Example topology for time correlation attacks.

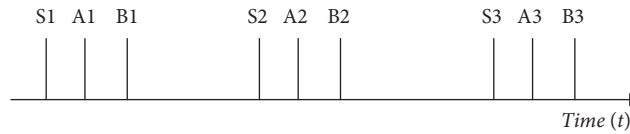


FIGURE 5: Time serial for reporting event from the source node to base station.

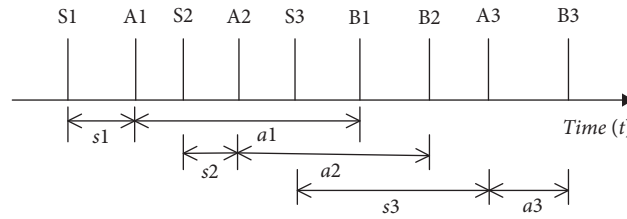


FIGURE 6: Nodes forwarding packets with random delays.

```

Node maintains a table with entry  $\langle data, time\_to\_transmit \rangle$  to store data to be forwarded;
Node maintains clock timer, which is used for data transmission;
For data requested to be transmitted:
  Generate a random time  $rand$ ;
  Insert into the table with entry  $\langle data, timer + rand \rangle$ ;
Node search the table to find data that could be transmitted:
  for each entry in the table do.
    if timer  $\geq$  entry. time_to_transmit then
      Transmit the data;
    end
  end

```

ALGORITHM 2: Forwarding random delay.

consumption of HASHA and Phantom Routing [19], a well-known random location privacy preserve scheme. The power consumption of hash functions and wireless transmission and reception is listed in Table 1.

Figure 9 illustrates the overall power consumption of HASHA and Phantom Routing under different network size. While the size of the network is small (for example, 20 or 50 nodes), HASHA consumes more power than Phantom Routing. The reason is that hash operation is required for

both transmitter and receiver, which introduce additional power consumption. Phantom Routing creates routing path longer than the shortest path. But as the network size is fairly small, the additional energy consumption for additional path is much less than hash operation. Therefore, the energy consumption of Phantom Routing is lower. As the size of network increased, the energy wasted on additional path increased dramatically. And that portion of energy cost is much greater than energy cost for hash operations.

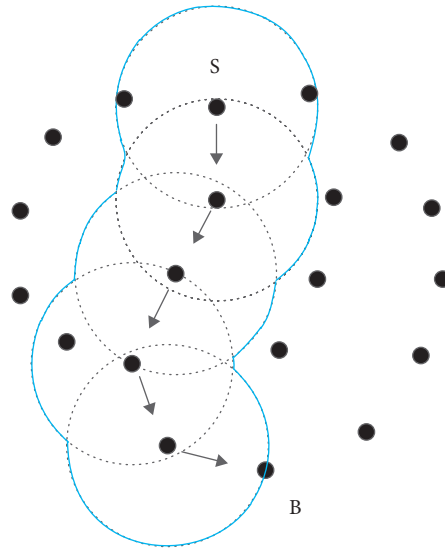


FIGURE 7: Traffic outlining attacks against event-triggered WSNs.

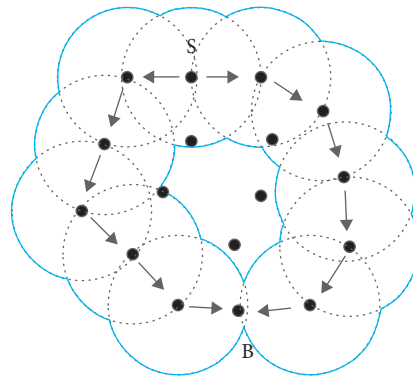


FIGURE 8: Circular traffic against traffic outlining attacks.

- (1) Find the shortest path from the source node to base station according to routing protocol such as dijkstra.
- (2) The base station calculates hops n from source node to base station and requests the node $n/2$ hops away to initiate a circular forwarding path.
- (3) The selected node broadcasts beacons which includes a counter with initial value $n/2$.
- (4) All nodes that received the broadcasts decrease the value and forward it.
- (5) All nodes that received the broadcasts with value 0 are candidates for circular forwarding.
- (6) On having data to be sent, the source node selects one of the paths randomly to forward the data to the base station.

ALGORITHM 3: Circular forwarding against traffic outlining attacks.

TABLE 1: Power consumption of key operation.

Operation	Consumed energy
UMAC/32 hashing	0.143 uJ/byte
Tiger/192 hashing	0923 uJ/byte
Transmitting	5.623 uJ/byte
Receiving	6.39 uJ/byte

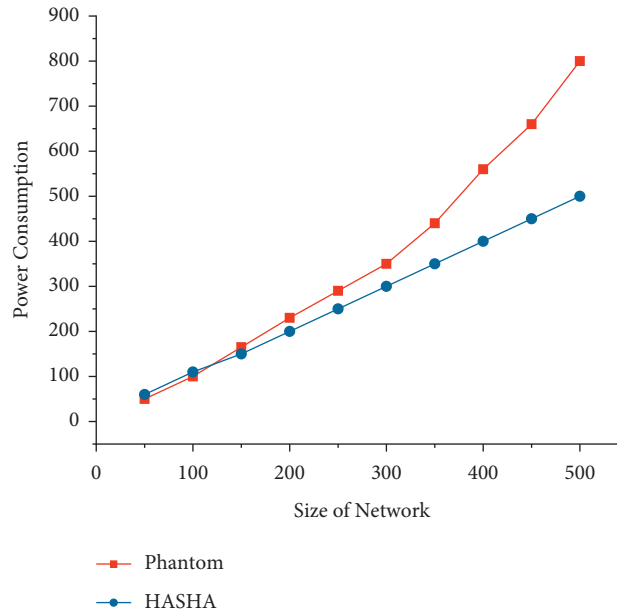


FIGURE 9: Power consumption of HASHA and Phantom Routing.

6. Conclusions

In this paper, we have identified that location privacy cannot be preserved efficiently at network layer, because address at data link layer is not protected well. The address at data link layer exposes node identity and packet routing information to the adversary. Traffic analysis attacks can be easily launched to jeopardize location privacy. HASHA scheme, which hides the addresses at data link layer, is proposed to protect location privacy. Analytical and simulation results show that HASHA is more energy efficient than traditional approaches [40, 41].

Data Availability

The simulation source file data used to support the findings of this study are available from the corresponding author upon request.

Disclosure

The initial version of this paper was published on IEEE International Conference on High Performance Computing and Communications. This is a substantial extension to the conference paper. The conference paper can be accessed at <https://ieeexplore.ieee.org/document/8622908> [41].

Conflicts of Interest

The authors declare no conflicts of interest.

Authors' Contributions

Qiong Zhang had the initial idea for this paper and rewrote the manuscript. Kewang Zhang conducted analysis and experiments.

References

- [1] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras, "Applications of wireless sensor networks: an up-to-date survey," *Applied System Innovation*, vol. 3, no. 1, p. 14, 2020.
- [2] S. Ali, T. Al Balushi, Z. Nadir, and O. K. Hussain, *WSN Security Mechanisms for CPS*, *Cyber Security for Cyber Physical Systems*, pp. 65–87, Springer, New York, NY, USA, 2018.
- [3] W. Al Shehri, "A survey on security in wireless sensor networks," *International journal of Network Security & Its Applications*, vol. 9, no. 1, pp. 25–32, 2017.
- [4] Q. Shafi, "Cyber physical systems security: a brief survey," in *Proceedings of the 12th IEEE International Conference on Computational Science and Its Applications*, pp. 146–150, Brazil, June 2012.
- [5] Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks," in *Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 1–9, IEEE, Italy, June 2009.
- [6] L. Zhou and Y. Shan, "Multi-branch source location privacy protection scheme based on random walk in WSNs," *IEEE*, in *Proceedings of the 2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis*, pp. 543–547, IEEE, China, April 2019.
- [7] M. Conti, J. Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1238–1280, 2013.
- [8] A. Tsitroulis, D. Lampoudis, and E. Tsekles, "Exposing WPA2 security protocol vulnerabilities," *International Journal of Information and Computer Security*, vol. 6, no. 1, pp. 93–107, 2014.
- [9] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks*, ser. *SASN '04*, ACM, Washington, DC, USA, October 2004.

- [10] D. Braginsky and D. Estrin, "Rumor routing algorithm for sensor networks," in *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, ser. WSNA '02, ACM*, vol. 9, pp. 22–31, ACM, New York, NY, USA, September 2002.
- [11] E. Ekici, S. Vural, J. McNair, and D. Al-Abri, "Secure probabilistic location verification in randomly deployed wireless sensor networks," *Ad Hoc Networks*, vol. 6, no. 2, pp. 195–209, 2008.
- [12] Y. Li, L. Lightfoot, and J. Ren, "Routing-based source-location privacy protection in wireless sensor networks," in *Proceedings of the IEEE International Conference on Electro/Information Technology*, vol. 6, pp. 29–34, IEEE, Canada, January 2009.
- [13] I. Shaikh, H. Jameel, B. dAuriol, H. Lee, S. Lee, and Y.-J. Song, "Achieving network level privacy in wireless sensor networks," *Sensors*, vol. 10, no. 3, pp. 1447–1472, 2010.
- [14] W. Yang and W. T. Zhu, "Protecting source location privacy in wireless sensor networks with data aggregation," *Ubiquitous Intelligence and Computing*, vol. 10, pp. 252–266, 2010.
- [15] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Towards a statistical framework for source anonymity in sensor networks," *IEEE Transactions on Mobile Computing*, vol. 10, no. 12, pp. 1–12, 2011.
- [16] M. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 10, pp. 1805–1818, 2012.
- [17] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *Proceedings of the 25th IEEE international conference on distributed computing systems*, pp. 599–608, IEEE, June 2005.
- [18] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in *Proceedings of the The 27th Conference on Computer Communications, ser. INFOCOM 2008*, vol. 4, pp. 51–55, IEEE, Columbus, OH, USA, March 2008.
- [19] H. Chen and W. Lou, "From nowhere to somewhere: protecting end-to-end location privacy in wireless sensor networks," in *Proceedings of the Performance Computing and Communications Conference, IEEE 29th International*, vol. 12, pp. 1–8, IEEE, Piscataway, USA, December 2010.
- [20] S. Tilak, N. B. Abu-Ghazaleh, and W. Heinzelman, "A taxonomy of wireless micro-sensor network models," *ACM SIGMOBILE - Mobile Computing and Communications Review*, vol. 6, no. 2, pp. 28–36, 2002.
- [21] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards event source unobservability with minimum network traffic in sensor networks," *ACM in Proceedings of the first ACM conference on Wireless network security, ser. WiSec '08*, vol. 4, pp. 77–88, ACM, New York, NY, USA, March 2008.
- [22] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems*, pp. 599–608, Columbus, OH, USA, June 2005.
- [23] X. Hong, P. Wang, J. Kong, Q. Zheng, and J. Liu, "Effective probabilistic approach protecting sensor traffic," in *Proceedings of the IEEE Military Communication Conference*, pp. 169–175, Atlantic City, NJ, USA, 2005.
- [24] S. Jiang and N. H. Vaidya, W. Zhao, "Routing in packet radio networks to prevent traffic analysis," in *Proceedings of the IEEE Information Assurance and Security Workshop*, West Point, NY, USA, February 2000.
- [25] J. Deng, R. Han, and S. Mishra, "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks," in *Proceedings of the IEEE International Conference on Dependable Systems and Networks*, Florence, Italy, July 2004.
- [26] J. Deng, R. Han, and S. Mishra, "INSENS: intrusion-tolerant routing for wireless sensor networks," *Computer Communications*, vol. 29, no. 2, pp. 216–230, 2006.
- [27] J. Deng, R. Han, and S. Mishra, "Decorrelating Wireless sensor network traffic to inhibit traffic analysis attacks," *Pervasive and Mobile Computing*, vol. 2, no. 2, pp. 159–186, 2006.
- [28] H. Gao, C. Liu, Y. Yin, Y. Xu, and Y. Li, "A hybrid approach to trust node assessment and management for VANETs cooperative data communication: historical interaction perspective," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2021.
- [29] H. Gao, L. Zhou, J. Y. Kim, Y. Li, and W. Huang, "The behavior guidance and abnormality detection for A-MCI patients under wireless sensor network," *ACM Transactions on Sensor Networks*, 2021.
- [30] S. Olariu, M. Eltoweissy, and M. Younis, "ANSWER: autonomous wireless sensor network," in *Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks (Q2SWinet'05)*, pp. 88–95, Montreal, Quebec, Canada, October 2005.
- [31] J. Kong, X. Hong, and M. Gerla, "An identity-free and on-demand routing scheme against anonymity threats in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 8, pp. 888–902, 2007.
- [32] Y. Yanchao Zhang, W. Wei Liu, W. Wenjing Lou, and Y. Fang, "MASK: anonymous on-demand routing in mobile ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 5, no. 9, pp. 2376–2385, 2006.
- [33] H. Gao, Y. Zhang, H. Miao, R. J. D. Barroso, and X. Yang, "SDTIOA: modeling the timed privacy requirements of IoT service composition: a user interaction perspective for automatic transformation from bpel to timed automata," *Mobile Networks and Applications*, vol. 26, no. 6, pp. 2272–2297, 2021.
- [34] H. Gao, X. Qin, R. J. D. Barroso et al., "Collaborative learning-based industrial IoT API recommendation for software-defined devices: the implicit knowledge discovery perspective," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 6, no. 1, pp. 66–76, 2022.
- [35] J. Al-Muhtadi, R. Campbell, A. Kapadia, and M. Dennis, "Routing through the mist: privacy preserving communication in ubiquitous computing environments," in *Proceedings of the 22nd International Conference on Distributed Computing Systems*, p. 74, Vienna, Austria, July 2002.
- [36] Y. Huang, H. Xu, H. Gao, X. Ma, and W. Hussain, "SSUR: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 670–681, 2021.
- [37] X. Ma, H. Xu, H. Gao, and M. Bian, "Real-time multiple-workflow scheduling in cloud environments," *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4002–4018, 2021.
- [38] J.-H. Park, Y. Jung, H. Ko, J. Kim, and M. Jun, "A privacy technique for providing anonymity to sensor nodes in a sensor network," in *Proceedings of the International*

- Conference on Ubiquitous Computing and Multimedia Applications*, Springer, Berlin, Heidelberg, 2011.
- [39] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, "UMAC: fast and secure message authentication," in *Advances in Cryptology - CRYPTO'99*, M. Wiener, Ed., vol. 1666, pp. 216–233, Springer, Berlin, Germany, 1999.
 - [40] S. Misra and G. Xue, "Efficient anonymity schemes for clustered wireless sensor networks," *International Journal of Sensor Networks*, vol. 1, no. 1/2, pp. 50–63, 2006.
 - [41] K. Zhang and Q. Zhang, "Preserve location privacy for cyber-physical systems with addresses hashing at data link layer," in *Proceedings of the 2018 IEEE 20th International Conference on High Performance Computing and Communications*, pp. 1028–1032, Exeter, UK, June 2018, <https://ieeexplore.ieee.org/document/8622908>.

Research Article

A Power Transformer Fault Prediction Method through Temporal Convolutional Network on Dissolved Gas Chromatography Data

Mengda Xing ^{1,2,3} Weilong Ding ^{1,3} Han Li ^{1,3} and Tianpu Zhang ^{1,3}

¹School of Information Science and Technology, North China University of Technology, Beijing, China

²Artificial Intelligence on Electric Power System State Grid Corporation Joint Laboratory (GEIRI),
Global Energy Interconnection Research Institute Co. Ltd., Beijing 102209, China

³Beijing Key Laboratory on Integration and Analysis of Large-Scale Stream Data, Beijing, China

Correspondence should be addressed to Weilong Ding; dingweilong@ncut.edu.cn

Received 24 December 2021; Revised 26 January 2022; Accepted 18 February 2022; Published 11 April 2022

Academic Editor: Yuyu Yin

Copyright © 2022 Mengda Xing 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 power transformer is an example of the key equipment of power grid, and its potential faults limit the system availability and the enterprise security. However, fault prediction for power transformers has its limitations in low data quality, binary classification effect, and small sample learning. We propose a method for fault prediction for power transformers based on dissolved gas chromatography data: after data preprocessing of defective raw data, fault classification is performed based on the predictive regression results. Here, Mish-SN Temporal Convolutional Network (MSTCN) is introduced to improve the accuracy during the regression step. Several experiments are conducted using data set from China State Grid. The discussion of the results of experiments is provided.

1. Introduction

As key equipment, the power transformer is directly related to the system availability and enterprise security of power grid. Dissolved gas analysis (DGA) is one of the most reliable means for condition estimation and fault diagnosis of oil-immersed transformers and is recommended for condition evaluation by standards from the International Electrotechnical Commission (IEC) and the National Energy Administration. Through the gas chromatography online monitoring technology, business analyses such as transformer fault detection can be done in quasi-real time, which improve the safety and stability of power grid [1].

However, it faces challenges in predicting power transformer faults due to inherent limitations in practice. First, the low quality of raw data makes direct data usage infeasible because transmission links may be interrupted and data packets may be lost [2]. Due to the equipment or communication network problems, incomplete, missing, and outlier records exist in gas chromatography data. Availability is usually an essential requirement [3], and such defective data makes fault prediction more difficult. Second, traditional methods like

widely used binary classification are not accurate enough, because such threshold-based fault detection technology ignores the data below the threshold and lacks historical trends employment. The oscillatory values around threshold may imply potential fault but cannot be found only by those methods. Third, the model is hard to be learned on small samples. The faults of power transformers appear casually, and related data must be a small proportion, and traditional models trained have to perform poorly due to the fact that too few features can be learned.

In this work, a fault prediction method is proposed for power transformers, which converts the classification problem for power transformers into a regression problem. Our contributions can be summarized as follows: (1) Missing imputation and outlier detection during the data preprocessing step guarantee completeness and continuity for gas chromatography data, which improve data quality obviously. (2) MSTCN proposed during regression step can learn features from data below fault threshold, which avoids overfitting through small sample learning. (3) On real-world data, our work shows convincing benefits and has been adopted in a practical business project.

The rest of this work is organized as follows: Section 2 discusses related work. Section 3 presents research background including motivation and methodology, as well as the transformer fault diagnosis method, AKA the three-ratio rule. Section 4 elaborates transformer fault prediction method based on MSTCN model. Section 5 evaluates the effects in extensive experiments. Section 6 summarizes the conclusion.

2. Related Work

Power transformer fault prediction is significant nowadays, but its discovery still faces challenges in efficiency and accuracy. Many works have adopted deep learning techniques in specific domains [4, 5]. We categorize related work into two technical perspectives: one is traditional algorithms through machine learning methods, and the other is deep learning methods, including recurrent neural networks (RNNs) and Temporal Convolutional Networks (TCNs).

2.1. Machine Learning Method. Machine learning methods can learn the fault occurrence pattern and then predict the possible faults. The literature [6] compared and analyzed MLP (Multilayer Perceptron), RBF (radial basis function), fuzzy logic, and support vector machine (SVM) for fault prediction of power transformers. However, their parameters are mainly selected empirically, which limits the efficiency of modeling. The *F1*-score of these methods is not more than 90% as evaluated by our data set.

Machine learning methods combined with DGA for transformer fault prediction have achieved many results. Dukarm [7] shows how fuzzy logic and neural networks are used to automate standard DGA methods. Furthermore, Wang et al. [8] conducted a combined artificial neural network and expert system tool (ANNEPS) developed for transformer fault diagnosis using dissolved gas-in-oil analysis. Huang et al. [9] introduced an evolutionary programming (EP) based fuzzy logic technique to identify the incipient faults of the power transformers. Yang et al. [10] employed bootstrap and genetic programming to improve the interpretation accuracy for DGA of power transformers. Hellmann [11] applied fuzzy logic (FL) that allows intermediate values to be defined between conventional evaluations like true/false, yes/no, high/low, and so forth. Souahlia et al. [12] applied the support vector machine (SVM) based decision for power transformers fault diagnosis.

However, these works have common problems, including the too small amount of data, few types of data, and only simple classification rules. For example, the fault categories are shallow, including overheating, discharging, and overheating with discharging. Advanced transformer fault prediction is required on Big Data fully using DGA data.

2.2. Deep Learning Method. In recent years, deep learning networks combined with DGA have further improved the accuracy of transformer fault prediction. Recurrent neural networks (RNNs) have been widely adopted in research areas concerned with sequential data, such as text, audio,

and video [13]. Among RNNs methods, in particular Long Short-Term Memory (LSTM) [14] and Gated Recurrent Units (GRU) [15] are excellent in fully exploiting the time-varying features of time series data. Although the gradient problem of RNN has been solved to some extent in LSTM and GRU, it will still be tricky for longer sequences [13].

Bai et al. [16] proposed the Temporal Convolutional Networks (TCNs) model, a deep learning model for sequence modeling tasks. TCN combines convolutional neural network (CNN) and recurrent neural network ideas for processing time series type data. Almqvist [17] compared the performance of RNN and TCN for time series forecasting. Instead of using a cell state to preserve information from previous outputs as in LSTMs, TCNs use connection between previous hidden layers configured with two hyper-parameters: dilation factor and filter size. Zhang et al. [18] proposed a multiscale temporal convolutional network for fault prediction. They extracted multiscale time-frequency information with the discrete wavelet transform, and each piece of scale data is handled by different TCN, respectively. Zhang et al. [19] presented an attention mechanism enhanced Temporal Convolutional Network for fault prediction. They utilized an attention mechanism to make the TCN-based fault prediction model focus on more essential input variables to enhance the fault prediction performance. Zai et al. [20] put forward a predictive method for dissolved gas content in transformer oil based on Temporal Convolutional Network (TCN) and graph convolutional network (GCN). They designed a GCN to analyze the correlations among all gases and then established a topological graph for their correlations.

However, these models did not solve the problem caused by the rectified linear unit (ReLU) and weight normalization layers. The rectified linear unit (ReLU) based activation function applied in TCN is underutilization of negative values leading to vanishing gradient. Meanwhile, the weight normalization applied in TCN is sensitive to initial values leading to overfitting. Meanwhile, these models used binary classification for fault prediction, which might not thoroughly learn the information below the threshold and lacks historical trends employment.

Inspired by the works in [21, 22], we propose a Mish-SN Temporal Convolutional Network (MSTCN) for dissolved gas regression to predict transformers' fault. We apply the Mish activation function and switchable normalization to MSTCN to solve the problems caused by ReLU and weight normalization. Meanwhile, the dissolved gas regression can explore the numerical fluctuations before the threshold value and learn historical fault feature patterns.

3. Preliminary

3.1. Motivation. Our work is originated from a practical project of China State Grid.

This work utilizes the dissolved gas chromatography data set provided by China State Grid as the data set for experimentation. The data set comes from the gas chromatography online monitoring equipment of the power grid, which is based on an integrated, high-speed two-way

communication network [23]. The data set covers roughly 600 transformers. With the explosive growth in Internet of Things (IoT) devices, applications have also substantially expanded in recent years [24]. Some of the data is a relatively long time series, containing more than 60 months of monitoring data, while others are short, only three or four months of monitoring data. In addition, each data item in the dissolved gas chromatography data is a multidimensional vector rather than a single number in some stock market and house price analysis data sets. The main fields in the dissolved gas chromatography data set of transformer oil are shown in Table 1. The data are all collected and measured automatically through the gas chromatography online monitoring technology.

Definition 1. Status code. In this work, a status code is used to identify each sample's possible fault categorical value. Status code is used as the classification label for the later transformer fault classification. The possible status code is summarized in Table 2.

The appearance of dissolved gas in the transformer oil indicates transformer faults. The gas formation comes from three conditions: overheating, discharge, and moisture. The amount of gas inside the transformer oil can be measured frequently by technical means to keep track of the operating health of the transformer. If any of the gases has a tendency to exceed a notice value, the gas production rate should be observed. However, if all the gases are lower than the notice value, the transformer is considered to be working properly. Based on the recommendations of the data provider, the notice values of our data set in this work are shown in Table 3.

3.2. The Three-Ratio Rule. We apply the three-ratio rule to converse dissolved gas regression to the status code in our proposed method. The three-ratio rule is proposed by the National Energy Administration of China [25]. By studying the trend of the dissolved gas amount in transformer oil, the status of the transformer can be determined based on the gas chromatography combined with the three-ratio rule. The conversion of three-ratio rule is shown in Tables 2 and 4.

Table 4 shows ratio code of two gases. For example, if the ratio of C_2H_2 to C_2H_4 is 0.2, the ratio code for C_2H_2/C_2H_4 is 1. Similarly, the other ratio codes for CH_4/H_2 and C_2H_2/C_2H_6 can be calculated. Table 2 shows the three-ratio codes and their corresponding faults. For example, if the ratio codes of C_2H_2/C_2H_4 , CH_4/H_2 , and C_2H_2/C_2H_6 are 1, 1, and 2, that is, the three-ratio code 112, the corresponding type of fault is low energy discharge, with the status code 6.

4. Power Transformer Fault Prediction Method

4.1. Overview. The fault prediction method based on dissolved gas regression proposed in this work is shown in Figure 1. Our method is divided into three steps. The first step is data preprocessing. Inspired by the work of Ding et al. [26], we convert data from different sources in the dissolved gas chromatography data set into a uniform format and

resolve problems such as missing values and outliers in the data as much as possible. The second step is to predict gas amounts using a deep learning model. We apply MSTCN to dissolved regression gas regression to obtain future gas amounts. The third step is fault classification. The predicted transformer status code is calculated based on regression results of the second step and three-ratio rule mentioned above.

On the basis of transformer fault prediction studies, fault prediction methods usually use machine learning models or statistical tools to predict transformer fault. Instead of directly using deep learning models to predict transformer fault, we add a gas regression step between data preprocessing and fault classification. The usual fault prediction uses binary classification as predicting labels to do classification prediction, and the fault classification is judged based on the threshold value, ignoring the fluctuation of the value before the threshold value. The final prediction model might not learn the prethreshold value fluctuation information.

4.2. Data Preprocessing. In the domain of gas chromatography online monitoring technology of power transformer, there are problems such as network instability and server performance bottlenecks in processing extensive data. We mainly address the problem of missing data and outliers that exist in the dissolved gas chromatography data set.

Definition 2. Missing data. The missing data types include negative number, not a number (NaN), and null. Let $\mathbf{X} \in \mathbb{R}^{n \times m}$ be a feature matrix consisting of n data points and m features of dissolved gases. The t -th data point is denoted as \mathbf{x}_t . The j -th feature value of \mathbf{x}_t is denoted as \mathbf{x}_{tj} . \mathbf{x}_{tj} is defined as missing data if $\mathbf{x}_{tj} \notin [0, \infty)$.

The definition of outlier points combined with the characteristics of the data set and 3 σ -rule is shown as follows.

Definition 3. Outlier. Let $\mathbf{X} = \{\mathbf{x}_{t-k}, \dots, \mathbf{x}_{t-1}, \mathbf{x}_{t+1}, \dots, \mathbf{x}_{t+k}\}$ be defined as a set of the k -nearest neighbors of \mathbf{x}_t . Each of \mathbf{X} is recorded at a specific time point $t \subseteq \mathbb{U}^+$ and consists of m observations that could be denoted as $\mathbf{x}_t = (x_{t1}, \dots, x_{tm})$, each dimension j of m -dimensional vectors at a certain data point t could be denoted as x_{tj} , the expected value of x_{tj} could be denoted as \hat{x}_{tj} , the Euclidean distance of two data points can be denoted as d , and the highest distance threshold between a true data point and its expected data point could be denoted as 3σ . The outlier could be denoted as

$$\mathbf{x}_t \text{ is an outlier} \Leftrightarrow \{\forall \mathbf{x}_t \in X, \exists j \in \{1, \dots, m\} | d(x_{tj}, \hat{x}_{tj}) \geq 3\sigma\}. \quad (1)$$

With the definitions above, missing data and outlier problems are explicitly defined to be handled. Properly imputed data and corrected outliers could lower the regression errors and further promote fault prediction effectiveness:

TABLE 1: The main fields in the dissolved gas chromatography data set.

Collection date	C ₂ H ₂	C ₂ H ₄	C ₂ H ₆	CH ₄	CO	CO ₂	H ₂	Status code
2012-11-15	0.0	0.38	3.51	3.11	653.71	3391.83	6.74	0 (normal)
2012-11-16	0.0	0.47	2.885	11.5075	641.685	229097.165	5.555	2 (low temperature overheating)

TABLE 2: Fault category and status code through ratio code [25].

Three-ratio code	Nonfault and fault	Status code
000	Nonfault	0
001	Low temperature overheating (below 150°C)	1
020	Low temperature overheating (150~300°C)	2
021	Medium temperature overheating (300~700°C)	3
0* 2	High temperature overheating (above 700°C)	4
010	Partial discharge	5
10* 11*	Low energy discharge	6
12*	Low energy discharge and overheating	7
20* 21*	Arc discharge	8
22*	Arc discharge and overheating	9

*0, 1, and 2 for simplicity.

TABLE 3: Gas and threshold.

Gas	Threshold
H ₂	10000
C ₂ H ₂	10000
C ₂ H ₄	5000
C ₂ H ₆	1000
CH ₄	5000
CO	10000
CO ₂	20000

TABLE 4: Ratio code [25].

Gases ratio range	Code of ratio		
	C ₂ H ₂ /C ₂ H ₄	CH ₄ /H ₂	C ₂ H ₂ /C ₂ H ₆
(0, 0.1)	0	1	0
[0.1, 1)	1	0	0
[1, 3)	1	2	1
[3, +∞]	2	2	2

Missing Data Imputation. For the missing data mentioned earlier, considering the data characteristics of gas amount, in this work, we took a modification of the EM algorithm proposed by Junger [27]. The algorithm comprises the following steps: (i) replace the missing values by estimates; (ii) estimate parameters μ and σ ; (iii) estimate the level for each of the univariate pieces of data; (iv) reestimate the missing values using updated estimates of the parameters and the level of the data. These steps are iterated until some convergence criterion is reached.

Let \mathbf{x}_t be the t data point of m features matrix \mathbf{X} . After $k+1$ iteration, the revised maximum likelihood estimates $\tilde{\mathbf{x}}_t = \{\tilde{x}_{t1}^{(k+1)}, \mathbf{x}_{t2}\}$.

Outlier Correction. $\mathbf{X} = \{\mathbf{x}_{t-k}, \dots, \mathbf{x}_{t-1}, \mathbf{x}_{t+1}, \dots, \mathbf{x}_{t+k}\}$ is a set of the k -nearest neighbors of \mathbf{x}_t . Each of \mathbf{X} is recorded at a specific time point $t \in \mathbb{Z}^+$ and consists of

m real-valued observations that could be denoted as $\mathbf{x}_t = (x_{t1}, \dots, x_{tm})$, each dimension j of m -dimensional vectors at a certain data point t could be denoted as x_{tj} , the expected value of x_{tj} could be denoted as \hat{x}_{tj} , and the highest distance threshold between a true data point and its expected data point could be denoted as 3σ . In the outlier equation (1), the expected value \hat{x}_{tj} and the highest distance threshold 3σ are defined in the two following equations:

$$\hat{x}_{tj} = \frac{1}{2k} \left(\sum_{i=1}^k (x_{t+i,j} + x_{t-i,j}) \right), \quad (2)$$

$$\sigma_j = \sqrt{\frac{1}{2k} \sum_{i=1}^k \left((x_{t-i,j} - \hat{x}_{tj})^2 + (x_{t+i,j} - \hat{x}_{tj})^2 \right)}. \quad (3)$$

The expected value \hat{x}_{tj} is also the corrected value of the outlier \mathbf{x}_t .

4.3. Dissolved Gas Regression. In order to fully explore the numerical fluctuations before the threshold value and learn historical fault feature patterns, we proposed a regression model called Mish-SN Temporal Convolutional Networks.

On the other hand, if the predicted value of dissolved gas is obtained from the prediction model, the conversion from the predicted value of dissolved gas to the predicted value of the status code can be achieved with very few calculations.

Figure 2 shows a complete MSTCN map formed by stacking h residual blocks. The input is denoted as $\mathbf{X} = (\mathbf{x}_1, \dots, \mathbf{x}_t)$. In this work, we use a common technique in RNNs modeling called **time step** to improve predictive accuracy. The time step length could be denoted as L . The number of features is denoted as m . Let $\mathbf{v}_t \in \mathbb{R}^{L*m} = (\mathbf{x}_{t-L+1}, \dots, \mathbf{x}_t)$ be defined as a new data point. For any \mathbf{v}_t , its gas regression label is denoted as $\mathbf{y}_t = (\mathbf{x}_{t+1}, \dots, \mathbf{x}_{t+L})$.

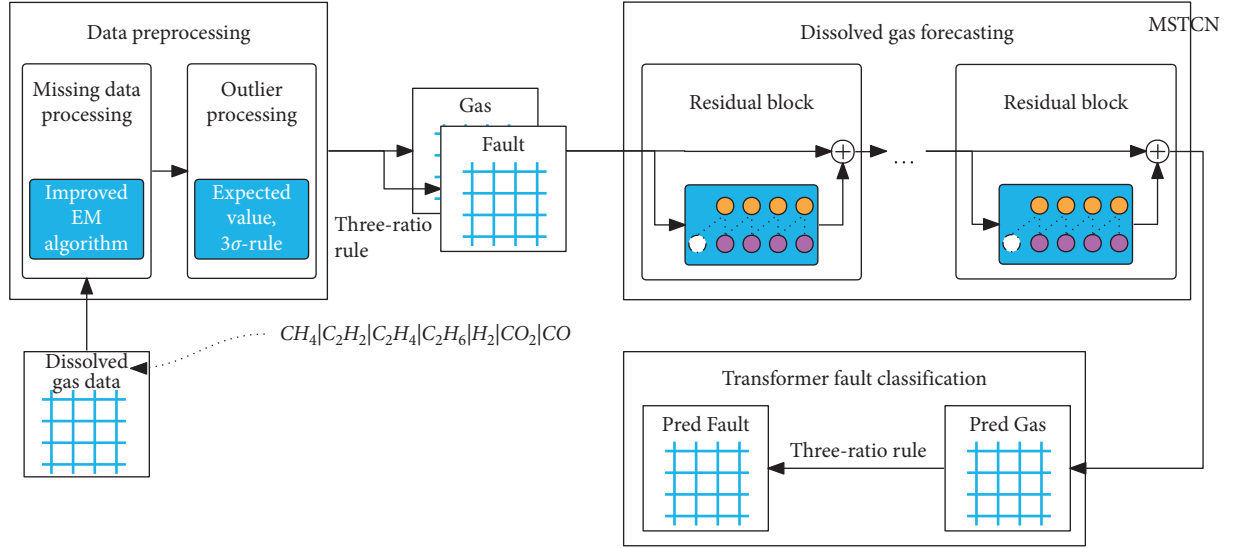


FIGURE 1: The architecture of our method.

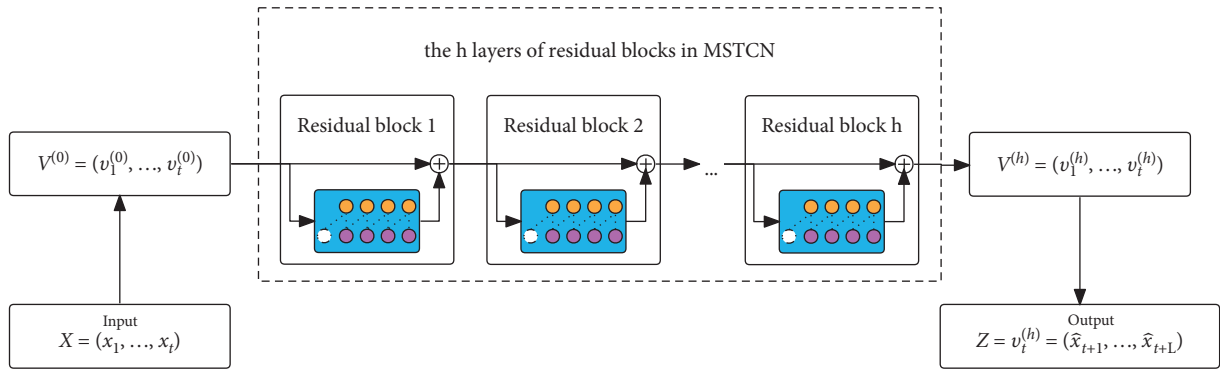


FIGURE 2: The architecture of MSTCN.

Therefore, the regression result of \mathbf{v}_t is denoted as $\hat{\mathbf{y}}_t = (\hat{x}_{t+1}, \dots, \hat{x}_{t+L})$. The convoluted result of the h -th residual block layer is denoted as $\mathbf{V}^{(h)} = (\mathbf{v}_1^{(h)}, \dots, \mathbf{v}_t^{(h)})$. However, to solve the real-world problem, we are only interested in the last case \mathbf{v}_t . $\mathbf{v}_t^{(h)} = (\hat{x}_{t+1}, \dots, \hat{x}_{t+L})$ represents L regression points of input $\mathbf{X} = (\mathbf{x}_1, \dots, \mathbf{x}_t)$. The output \mathbf{Z} of MSTCN regression result is shown as follows:

$$\begin{aligned} \mathbf{Z} &= \mathbf{V}^{(h)}[:, -1] = (\mathbf{v}_1^{(h)}, \dots, \mathbf{v}_t^{(h)})[:, -1] \\ &= \mathbf{v}_t^{(h)} = (\hat{x}_{t+1}, \dots, \hat{x}_{t+L}). \end{aligned} \quad (4)$$

Residual Block. In order to solve the vanishing gradient problem, in a deep convolution network, a well-known technique called residual blocks is applied in MSTCN shown in Figure 3. Residual blocks have been proven to be an effective method for training deep networks, which enables the network to transmit information in a cross-layer manner.

In Figure 3, the upper branch of the residual block presents dilated causal convolution $\mathcal{H}(\cdot)$ with the input $\mathbf{V}^{(h)} = (\mathbf{v}_1^{(h)}, \dots, \mathbf{v}_t^{(h)})$. The lower branch is the skip

connections added to solve the vanishing gradient problem. In this work, we replace weight normalization with switchable normalization. Through the switchable normalization self-learning method, let the MSTCN decide which normalizer to use to obtain the best prediction effect. The MSTCN also introduces the Mish activation function to replace the ReLU for solving the dead ReLU problem in order to make the activation function smooth and derivable at 0 points and to improve the generalization of the model. Let $\delta(\cdot)$ be the activation layer. The output $\mathbf{V}^{(h)}$ could be expressed as

$$\mathbf{V}^{(h)} = \delta(\mathcal{H}(\mathbf{V}^{(h-1)}) + \mathbf{V}^{(h-1)}). \quad (5)$$

Dilated Casual Convolution. Figure 4 presents the structure of the dilated causal convolution stack from a residual block with filter size $k = 2$ and dilation factor $d = 3$. In Figure 4, the other layers and skip connection are omitted. The input of dilated causal convolution is denoted as $\mathbf{V}^{(h-1)} \in \mathbb{R}^{t \times L} = (\mathbf{v}_1^{(h-1)}, \dots, \mathbf{v}_t^{(h-1)})$. The output of dilated casual convolution is denoted as $\mathbf{V}^{(h)} \in \mathbb{R}^{t \times L} = (\mathbf{v}_1^{(h)}, \dots, \mathbf{v}_t^{(h)})$. Inspired by the idea of

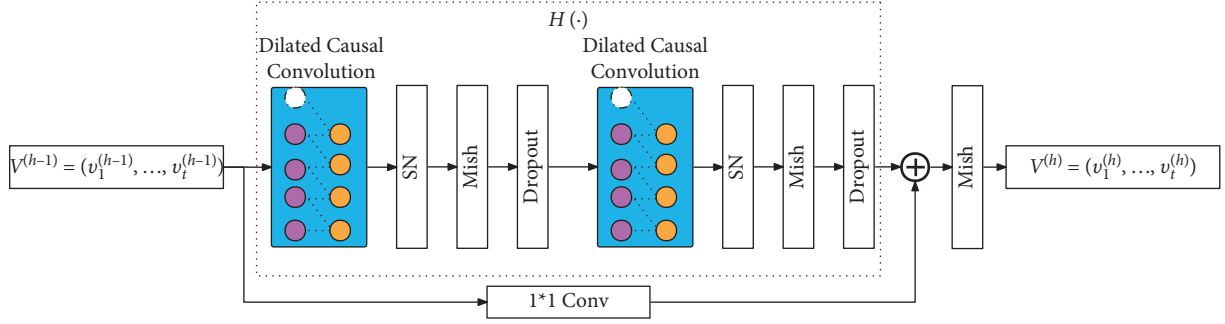
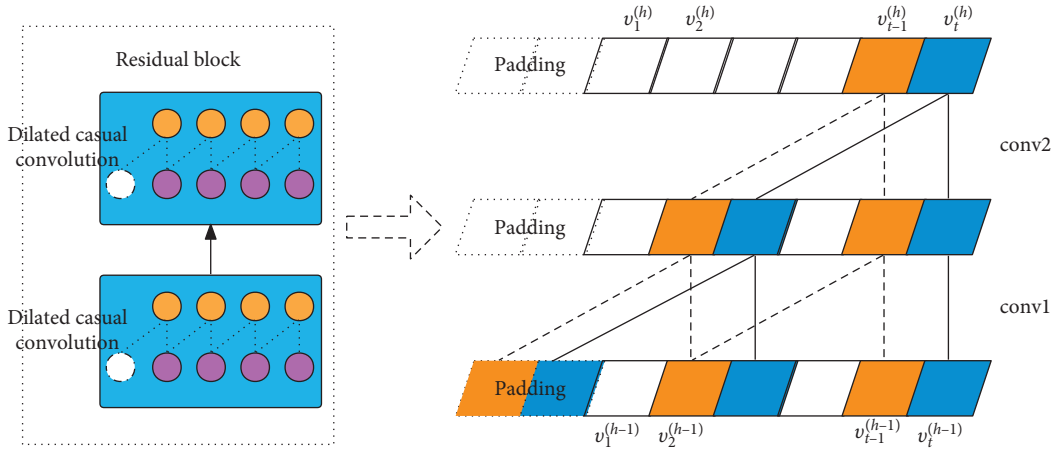


FIGURE 3: The architecture of the residual block in MSTCN.

FIGURE 4: A dilated causal convolution with dilation factor $d=3$ and filter size $k=2$.

dilated convolution [28] and casual convolution [29], we set a constraint according to concept of casual convolution that any $\mathbf{v}_t^{(h)}$ only depends on $\mathbf{v}_1^{(h-1)}, \dots, \mathbf{v}_t^{(h-1)}$ and not on future $\mathbf{v}_{t+1}^{(h-1)}, \dots$. Meanwhile, to enlarge receptive field without deepening the structure, we apply concept of dilated convolution to the residual block.

A constraint according to concept of casual convolution that any $\mathbf{v}_t^{(h)}$ only depends on $\mathbf{v}_1^{(h-1)}, \dots, \mathbf{v}_t^{(h-1)}$ and not on future $\mathbf{v}_{t+1}^{(h-1)}, \dots$ is shown in Figure 4. To enlarge receptive field without deepening the structure, the MSTCN introduces dilated convolution.

4.4. Fault Classification. The guidelines [25] stipulate that, in the oil chromatographic analysis, if the content of each gas has a tendency to increase or exceeds a notice value, the gas production rate should be observed, and the gas production rate should be observed based on the three-ratio rule; it could be preliminarily judged that there is an overheating fault or a discharging fault, according to the three-ratio rule of gas chromatography in Table 4.

Let $\mathbf{U} \in \mathbb{R}^L = \{u_t, \dots, u_{t+L}\}$ be defined as the status code. Let $\mathbf{Z} \in \mathbb{R}^{L \times n_{\text{gas}}} = \{\hat{x}_t, \dots, \hat{x}_{t+L}\}$ be defined as a set of L regression results. Let $\text{gas} \in \{\text{C}_2\text{H}_2, \text{C}_2\text{H}_4, \text{C}_2\text{H}_6, \text{H}_2, \text{CH}_4\}$; $\{r_1, r_2, r_3\} \in \mathbb{Z}^3$. Let n_{gas} be denoted as the feature numbers of \hat{x}_t . Let $\hat{x}_{t,\text{gas}} \in \mathbb{R}$ be denoted as the regression value of

dissolved gas. The fault classification algorithm is defined in Algorithm 1.

5. Evaluation

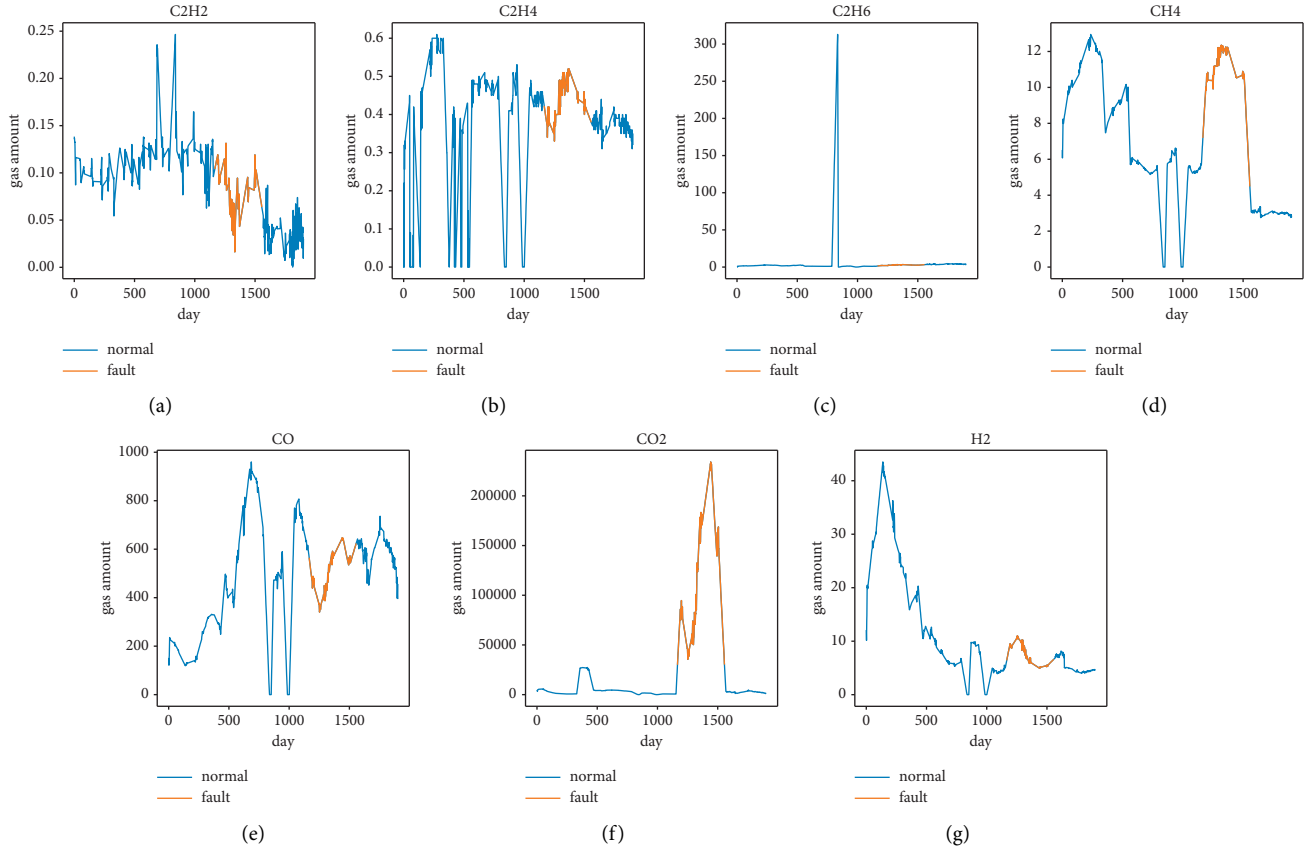
5.1. Setting. The experiments in this work are running on a server with CentOS 7 operating system installed with Intel Core i7-6700 CPU, 16 GB RAM, and 1 TB storage. The experiments are written in Python 3.9.6, implementing JupyterLab 3.1.11, TensorFlow 2.5.0, and Matplotlib 3.3.4.

The data set was collected from oil-immersed power transformers in different substations in China, with 200,000 records covering the period from 2012 to 2017. The data set contains 7 fault-related gases ($\text{H}_2, \text{C}_2\text{H}_2, \text{C}_2\text{H}_4, \text{C}_2\text{H}_6, \text{CH}_4, \text{CO}, \text{CO}_2$), the time of collection, other gases (N_2, O_2), substation and transformer information, and so forth. The distribution of 7 faulty gases is shown in Figure 5. The horizontal axis is the date. The vertical axis is the amount of gas. The blue curve indicates no fault on the corresponding date. The orange curve indicates a fault status on the corresponding date because the CO_2 amount has reached its notice value.

We selected a subset composed of 100 transformers of about 170,000 records from the data set, divided into 80 training sets, 10 validation sets, and 10 test sets. The time range of the subset is from November 2012 to September 2017. The reason for the selection is that it has high data

Input: Regression result $Z = \{\hat{x}_{t+1}, \dots, \hat{x}_{t+L}\}$
Output: Status code $U = \{u_{t+1}, \dots, u_{t+L}\}$
(1) **for** $t + 1$ to $t + L$
(2) compute three ratios: $r_1 = \hat{x}_{tC_2H_2} / \hat{x}_{tC_2H_4}$, $r_2 = \hat{x}_{tCH_4} / \hat{x}_{tH_2}$, $r_3 = \hat{x}_{tC_2H_4} / \hat{x}_{tC_2H_6}$
(3) look up Table 4 to convert the gas ratio to ratio code
(4) combine the three-ratio code get combination $r = 100 \cdot r_1 + 10 \cdot r_2 + r_3$ and look up Table 2 to get the status code u_t
(5) **end for**
(6) **return** U

ALGORITHM 1: Fault classification algorithm.

FIGURE 5: The gas distribution from 2012-08-21 to 2017-11-05 of a transformer. (a) C_2H_2 . (b) C_2H_4 . (c) C_2H_6 . (d) CH_4 . (e) CO . (f) CO_2 . (g) H_2 .

integrity and few missing values. In every transformer sequence of this data set, each record has attributes of collection date, 7 different dissolved gas values, and the status code label according to the three-ratio rule as shown in Table 1.

5.2. Experiment. In order to accurately evaluate the performance of the proposed transformer fault prediction model based on the MSTCN, we carried out dissolved gas regression and transformer fault classification experiments on the dissolved gas chromatography data set. First, we verify the average accuracy of dissolved gas regression based on the improved MSTCN. Second, we verify our proposed method by comparing it with other fault classification

models based on binary classification and analyze the effectiveness of the models.

Experiment 1. Dissolved Gas Regression. The experiment applies MSTCN, TCN, LSTM, and GRU, respectively, on the test set to verify the effectiveness of the MSTCN model. The final parameters of MSTCN are defined in configuration: number of epochs is 100, batch size is 32, time step is 12, and learning rate is 0.001. The final parameters of residual block in MSTCN are shown in Table 5. For the TCN, LSTM, and GRU methods, they have roughly the same parameters as MSTCN, considering the rigour of the experiment. This work applies the root mean square error (RMSE) as the loss function shown in equation (6) and Adam as the

TABLE 5: Hyperparameter of the residual block.

Layer	Parameter	Value
conv1, conv2	Filters	10
	Kernel size	3
	Stride	1
	Padding	Same
	Dilation	1, 2, 4, 8, 16
dropout1, dropout2	Dropout rate	0.5

optimization algorithm. m represents the total m records, y_i represents the actual gas amount of record i , and \hat{y}_i represents the predicted gas amount.

m represents the total m records, y_i represents the actual gas amount of record i , \bar{y} represents the average value of actual gas amount, and \hat{y}_i represents the predicted gas amount. The minimum of RMSE, MAE, and MAPE is 0, and the closer the metric is to 0, the better the predictive effect is. The maximum of R^2 is 1; the closer to 1 the better.

In order to measure the predictive performance of the models, RMSE, MAE, MAPE, and R^2 are used as the models' metrics. The calculation formulas of those metrics are shown in equation (6).

Figure 6 shows the actual gas amount curves and the regression curves predicted by different models, including MSTCN, TCN, LSTM, and GRU. It can be seen from Figure 6 that the fit curve of MSTCN is more accurate than the curves of the other models. Although, in the predictions from (g) H_2 , LSTM performed better, overall, the MSTCN error is smaller than those in other models.

We have calculated above metrics of MSTCN, TCN, LSTM, and GRU. The results are listed in Table 6.

Table 6 shows the comparison of the MSTCN model and other deep learning models (TCN, LSTM, and GRU) as regards gas regression effect. MSE, MAE, and MAPE are used to measure the error between the true value and the predicted value of the data; R^2 is also used to measure the difference between the true value and the predicted value of the data and to standardize this difference to $[0, 1]$. For the predictions of C_2H_4 , C_2H_6 , CH_4 , CO , CO_2 , H_2 , MSTCN has achieved a relatively good evaluation index. Although the prediction of C_2H_2 TCN has more minor prediction errors (RMSE), MSTCN is overall significantly better than other models.

$$\begin{aligned}
 \text{RMSE} &= \sqrt{\frac{1}{m} \sum_{i=1}^m (\hat{y}_i - y_i)^2}, \\
 \text{MAE} &= \frac{1}{m} \sum_{i=1}^m |\hat{y}_i - y_i|, \\
 \text{MAPE} &= \frac{100\%}{m} \sum_{i=1}^m \left| \frac{\hat{y}_i - y_i}{y_i} \right|, \\
 R^2 &= 1 - \frac{\sum_{i=1}^m (y_i - \hat{y}_i)^2}{\sum_{i=1}^m (y_i - \bar{y})^2}.
 \end{aligned} \tag{6}$$

Experiment 2. Fault Classification. In order to further verify the superiority of the transformer fault prediction method proposed in this work, this experiment uses the regression value of the previous experiment as input. It converts the predicted gas amount to the status code according to the three-ratio rule. The control group uses TCN, LSTM, and GRU models and uses actual gas amount as input to directly classify the fault of the transformer.

In order to measure the accuracy of fault classification under different models, according to the confusion matrix, this experiment denotes faulty status as positive (P) and normal status as negative (N). Therefore, the correct fault classification could be denoted as true positive (TP) and true negative (TN), and the incorrect prediction could be denoted as false positive (FP) and false negative (FN) [30]. This experiment introduces three metrics to measure the model's accuracy on the test set. The precision, recall, and F1-score are expressed in equations (7)–(9). The F1-score is a harmonic mean of precision and recall, whose value is also between 0 and 1, as well as precision and recall. The more the three metrics are close to 1, the better predictive effect the model has.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}, \tag{7}$$

$$\text{recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}, \tag{8}$$

$$\text{F1-score} = 2 \times \frac{\text{precision} \times \text{recall}}{\text{precision} + \text{recall}}. \tag{9}$$

Comparing the accuracy of fault classification under different models, the evaluation metrics are shown in Table 7.

Table 7 shows the comparison of transformer fault classification results between the MSTCN model and other deep learning models (TCN, LSTM, and GRU). The first column indicates the transformers participating in the experiment. Each transformer is an independent and complete experiment. The second column presents the evaluation metrics. The following columns are a comparison of the four model evaluation metrics. Overall, the prediction results of each model are satisfactory. This is caused by the faulty gas three-ratio algorithm and the gas attention value. For example, although the model has a deviation between the predicted gas value and the true value, it is still in the same ratio range, or the failure attention value is not reached at all, so the final predicted failure state will not change easily, resulting in an excellent overall prediction effect. For different transformers, the difference in fault prediction effect is more significant than the difference between models. The effect of model prediction is more affected by the data set than the model difference. For different models, the difference in failure prediction effects is relatively small. Overall, MSTCN is slightly higher than other models.

With the proposed transformer fault prediction method in this work in Figure 2, it can reduce or eliminate the impact of low accuracy of classification caused by threshold-based

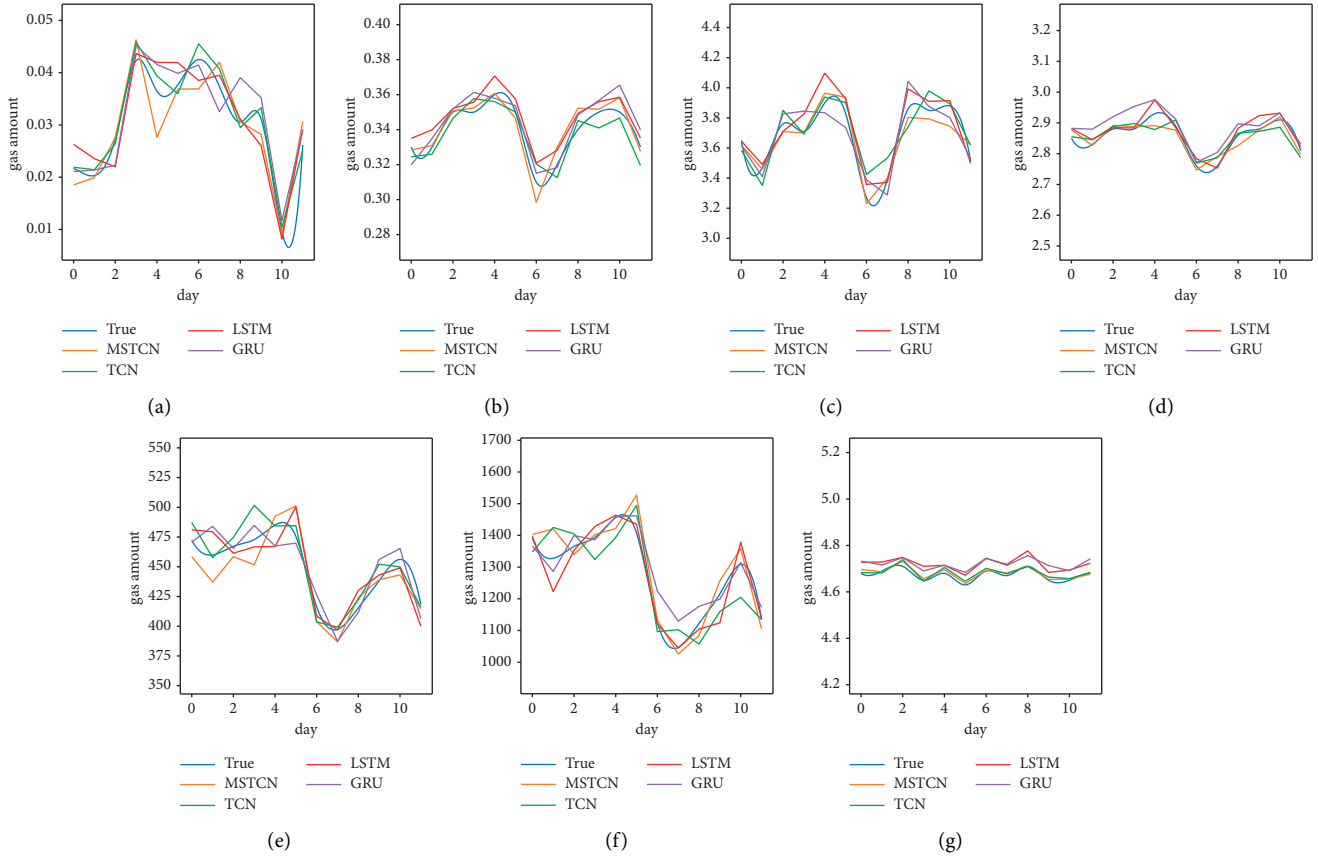


FIGURE 6: Comparison of gas regression between MSTCN and other models. (a) C_2H_2 . (b) C_2H_4 . (c) C_2H_6 . (d) CH_4 . (e) CO . (f) CO_2 . (g) H_2 .

TABLE 6: Gas regression results of transformer no. 1.

Gas	Metrics	MSTCN	TCN	LSTM	GRU
C_2H_2	RMSE	0.0051	0.0026	0.0065	0.0042
	MAE	0.0043	0.0020	0.0055	0.0036
	MAPE	14.07%	5.80%	17.96%	11.66%
	R^2	0.7091	0.9254	0.5218	0.7975
C_2H_4	RMSE	0.0056	0.0058	0.0089	0.0065
	MAE	0.0045	0.0045	0.0071	0.0052
	MAPE	1.32%	1.31%	2.05%	1.51%
	R^2	0.8503	0.8393	0.6161	0.7967
C_2H_6	RMSE	0.0494	0.0567	0.0768	0.0721
	MAE	0.0450	0.0491	0.0646	0.0630
	MAPE	1.24%	1.33%	1.76%	1.73%
	R^2	0.9419	0.9237	0.8599	0.8764
CH_4	RMSE	0.0138	0.0200	0.0284	0.0350
	MAE	0.0116	0.0155	0.0230	0.0314
	MAPE	0.41%	0.54%	0.81%	1.10%
	R^2	0.9294	0.8516	0.7019	0.5483
CO	RMSE	12.2925	12.3431	13.9061	16.6197
	MAE	8.8837	10.1510	11.9101	13.2390
	MAPE	2.03%	2.26%	2.65%	2.87%
	R^2	0.8095	0.8079	0.7562	0.6518
CO_2	RMSE	44.8718	50.1873	47.7348	53.6491
	MAE	31.9983	40.4018	40.1977	41.3562
	MAPE	2.56%	3.11%	3.07%	3.25%
	R^2	0.8856	0.8569	0.8705	0.8364
H_2	RMSE	0.0083	0.0108	0.0535	0.0468
	MAE	0.0062	0.0095	0.0524	0.0458
	MAPE	0.13%	0.20%	1.12%	0.98%
	R^2	0.8810	0.7981	-3.9776	-2.8074

TABLE 7: Classification metrics of different models.

Transformers	Metrics	MSTCN	TCN	LSTM	GRU
Transformer no. 1	Precision	99.20%	98.59%	98.55%	98.55%
	Recall	99.12%	98.29%	98.24%	98.24%
	F1-score	0.9914	0.9837	0.9831	0.9831
Transformer no. 2	Precision	99.33%	99.08%	98.87%	98.95%
	Recall	99.18%	98.76%	98.35%	98.53%
	F1-score	0.9922	0.9885	0.9850	0.9865
Transformer no. 3	Precision	98.67%	98.40%	98.23%	98.21%
	Recall	98.06%	97.41%	96.94%	96.88%
	F1-score	0.9823	0.9770	0.9733	0.9728
Transformer no. 4	Precision	98.16%	98.03%	97.94%	97.84%
	Recall	97.12%	96.76%	96.53%	96.24%
	F1-score	0.9741	0.9713	0.9694	0.9671

binary classification. It can use the data information before the threshold and enhance the usage of historical fault data because the proposed method is based on the dissolved gas regression value. At the same time, this classification step does not introduce additional errors because it uses the same judgment criteria as the existing fault diagnosis methods.

6. Conclusions

In this work, we propose a power transformer fault prediction method based on dissolved gas regression, which cleverly converts the transformer fault prediction problem into a regression problem for dissolved gas amount. First, through data preprocessing, we overcome the difficulties in directly using raw data. Second, by dissolved gas regression, we achieve more efficient learning of the data below threshold than binary classification and avoid small sample learning caused by a large amount of preventive maintenance. Compared with the traditional binary-based classification fault prediction model, the fault prediction method based on gas amount prediction has better results with F1-score more than 0.9741. This novel method provides new insights for power transformer fault prediction.

In summary, the fault prediction method based on dissolved gas regression using MSTCN has excellent potential. In future work, we will continue to research this concept and shorten the training time with more advanced deep learning techniques. In addition to the fault prediction method proposed, we plan to tune the procedure to simplify the method.

Data Availability

The oil chromatography data used to support the findings of this study were supplied by China State Grid under license and so cannot be made freely available. Requests for access to these data should be made to the corresponding author for an application of joint research.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the science and technology project of State Grid Corporation of China: "Research on Data Governance and Knowledge Mining Technology of Power IOT Based on Artificial Intelligence" (Grant No. 5700-202058184A-0-0-00).

References

- [1] N. Muhamad, B. Phung, T. Blackburn, and K. Lai, "Comparative study and analysis of DGA methods for transformer mineral oil," in *Proceedings of the 2007 IEEE Lausanne Power Tech*, pp. 45–50, IEEE, Lausanne, Switzerland, July 2007.
- [2] H. Gao, C. Liu, Y. Yin, Y. Xu, and Y. Li, "A hybrid approach to trust node assessment and management for VANETs cooperative data communication: historical interaction perspective," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2021.
- [3] Y. Huang, H. Xu, H. Gao, X. Ma, and W. Hussain, "SSUR: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 670–681, 2021.
- [4] dH. Faria Jr, J. G. S. Costa, and J. L. M. Olivias, "A review of monitoring methods for predictive maintenance of electric power transformers based on dissolved gas analysis," *Renewable and Sustainable Energy Reviews*, vol. 46, pp. 201–209, 2015.
- [5] S. Yu, D. Zhao, W. Chen, and H. Hou, "Oil-immersed power transformer internal fault diagnosis research based on probabilistic neural network," *Procedia Computer Science*, vol. 83, pp. 1327–1331, 2016.
- [6] K. Bacha, S. Souahlia, and M. Gossa, "Power transformer fault diagnosis based on dissolved gas analysis by support vector machine," *Electric Power Systems Research*, vol. 83, no. 1, pp. 73–79, 2012.
- [7] J. J. Dukarm, "Transformer oil diagnosis using fuzzy logic and neural networks," in *Proceedings of the Canadian Conference on Electrical and Computer Engineering*, pp. 329–332, IEEE, Vancouver, BC, Canada, September 1993.
- [8] Z. Wang, Y. Liu, and P. J. Griffin, "A Combined ANN and Expert System Tool for Transformer Fault Diagnosis," in *IEEE Transactions on Power Delivery*, vol. 13, no. 4, pp. 1261–1269, IEEE, 2000.

- [9] Y. C. Huang, H. T. Hong-Tzer Yang, and C. L. Ching-Lien Huang, "Developing a new transformer fault diagnosis system through evolutionary fuzzy logic," *IEEE Transactions on Power Delivery*, vol. 12, no. 2, pp. 761–767, 1997.
- [10] X. Yang, W. Chen, A. Li, C. Yang, Z. Xie, and H. Dong, "BA-PNN-based methods for power transformer fault diagnosis," *Advanced Engineering Informatics*, vol. 39, pp. 178–185, 2019.
- [11] M. Hellmann, "Fuzzy logic introduction," *Université de Rennes*, vol. 1, pp. 1–9, 2001.
- [12] S. Souahlia, K. Bacha, and A. Chaari, "SVM-based decision for power transformers fault diagnosis using Rogers and Doernenburg ratios DGA," in *Proceedings of the 10th International Multi-Conferences on Systems, Signals & Devices 2013 (SSD13)*, pp. 1–6, IEEE, Hammamet, Tunisia, March 2013.
- [13] Y. Yu, X. Si, C. Hu, and J. Zhang, "A review of recurrent neural networks: LSTM cells and network architectures," *Neural Computation*, vol. 31, no. 7, pp. 1235–1270, 2019.
- [14] F. A. Gers, J. Schmidhuber, and F. Cummins, "Learning to forget: continual prediction with LSTM," *Neural Computation*, vol. 12, no. 10, pp. 2451–2471, 2000.
- [15] K. Cho, B. Van Merriënboer, C. Gulcehre et al., "Learning Phrase Representations Using RNN Encoder-Decoder for Statistical Machine Translation," <https://arxiv.org/abs/1406.1078>.
- [16] S. Bai, J. Z. Kolter, and V. Koltun, "An Empirical Evaluation of Generic Convolutional and Recurrent Networks for Sequence Modeling," *CoRR*, vol. abs/1803.01271, 2018, <https://arxiv.org/abs/1803.01271>.
- [17] O. Almqvist, "A comparative study between algorithms for time series forecasting on customer prediction: an investigation into the performance of ARIMA," *RNN, LSTM, TCN and HMM*, , Thesis vol. 52, 2019.
- [18] J. Zhang, Y. Wang, J. Tang, J. Zou, and S. Fan, "A multiscale temporal convolutional network for fault diagnosis in industrial processes," in *Proceedings of the 2021 American Control Conference (ACC)*, May 2021.
- [19] J. Zhang, Y. Chang, J. Zou, S. Fan, and T. C. N Ame, "Attention mechanism enhanced temporal convolutional network for fault diagnosis in industrial processes," in *Proceedings of the 2021 Global Reliability and Prognostics and Health Management (PHM-Nanjing)*, IEEE, Nanjing, China, October 2021.
- [20] H. Zai, W. Chen, H. He et al., "Prediction for dissolved gas in power transformer oil based on temporal convolutional and graph convolutional network," in *Proceedings of the 2021 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia)*, pp. 1160–1168, IEEE, Chengdu, China, July 2021.
- [21] M. D. Mish, "A self regularized non-monotonic neural activation function," vol. 4, p. 2, 2019, <https://arxiv.org/abs/1908.08681>.
- [22] P. Luo, J. Ren, Z. Peng, R. Zhang, and J. Li, "Differentiable learning-to-normalize via switchable normalization," in *Proceedings of the International Conference on Learning Representation (ICLR)*, 2019.
- [23] W. Ding, Z. Wang, Y. Xia, and K. Ma, *An Efficient Interpolation Method through Trends Prediction in Smart Power Grid*, Springer, Berlin, Germany, pp. 79–92, 2021.
- [24] H. Gao, X. Qin, R. J. D. Barroso, W. Hussain, Y. Xu, and Y. Yin, "Collaborative learning-based industrial IoT API recommendation for software-defined devices: the implicit knowledge discovery perspective," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 6, no. 1, 2020.
- [25] oN. E. A. China, "Guide to the analysis and the diagnosis of gases dissolved in transformer oil," *Tech. Rep.*, 2014.
- [26] W. Ding, X. Wang, Z. Zhao, and S. T. A. R Co, "CO-STAR: a collaborative prediction service for short-term trends on continuous spatio-temporal data," *Future Generation Computer Systems*, vol. 102, pp. 481–493, 2020.
- [27] W. L. Junger and A. Ponce de Leon, "Imputation of missing data in time series for air pollutants," *Atmospheric Environment*, vol. 102, pp. 96–104, 2015.
- [28] F. Yu and V. Koltun, "Multi-scale context aggregation by dilated convolutions," <https://arxiv.org/abs/1511.07122>.
- [29] T. J. Brazil, "Causal-convolution-a new method for the transient analysis of linear systems at microwave frequencies," *IEEE Transactions on Microwave Theory and Techniques*, vol. 43, no. 2, pp. 315–323, 1995.
- [30] W. Ding, Z. Wang, J. Chen, Y. Xia, J. Wang, and Z. Zhao, "Potential trend discovery for highway drivers on spatio-temporal data," *Wireless Networks*, vol. 27, no. 5, pp. 3407–3422, 2021.

Research Article

A Blockchain-Based Privacy Preservation Scheme in Mobile Medical

Haiying Wen , Meiyang Wei , Danlei Du , and Xiangdong Yin 

School of Information Engineering, Hunan University of Science and Engineering, Yongzhou 425199, China

Correspondence should be addressed to Haiying Wen; wenhaiying1022@huse.edu.cn

Received 21 June 2021; Revised 8 October 2021; Accepted 27 January 2022; Published 22 March 2022

Academic Editor: Honghao Gao

Copyright © 2022 Haiying 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.

With the rapid development of mobile medical, how to establish an effective security mechanism to protect data security and privacy while users enjoy medical services has become an urgent problem to be solved. Aiming at the easy leakage of privacy in mobile medical terminals and untrustworthy data, we make use of a role-separated mechanism to generate trusted anonymous certificates. We propose a lightweight identity authentication scheme and adopt blockchain to protect the security of medical data. Meanwhile, in view of the problems of transparency and visibility of blockchain information, we adapt the searchable encryption algorithm to realize ciphertext processing in the whole life cycle. Experiments show that our scheme can reduce the cost of computation on the basis of ensuring traffic. In the process of dynamic updating of ciphertext keywords, except the keyword identifier, less information is leaked to the server, which protects privacy of users.

1. Introduction

Medical problems including medical care access and quality are common around the world. Medical resources are in short supply and it is difficult to distribute them evenly. Large numbers of individuals do not receive the quality care that they need [1]. Even geographical problems such as economic differences between different regions, topography, and topography bring various difficulties to medical health. These problems are especially obvious in the developing countries with large populations. It is obvious that the traditional medical model with major hospitals as the core has been unable to adapt to the development needs of the current era. Mobile medical, which mainly uses mobile communication technologies such as PDAs, smart phones, and satellite communications to provide users with medical services and data exchange, has successfully replaced the traditional medical model as the new darling, with the help of cloud center [2].

The concept of mobile medical originated from the telemedicine monitoring and medical treatment for astronauts conducted by NASA. Later applications such as the use of portable mobile devices to collect various body data have

it further developed. As an innovative technology in the Internet plus medical mode, mobile medical can realize applications such as medical rescue, remote monitoring, and intelligent medical care. It is of great significance for promoting medical reform.

Mobile service composition [3, 4] meets the needs of people for medical services under the current social development. This demand is mainly reflected in the two aspects of distribution and data. To a certain extent, mobile medical has broken through the limitation of space and time in the traditional medical mode. Mobile medical empowers patients and health providers proactively to address medical conditions through near real-time monitoring and treatment, no matter the location of the patient or health provider.

In addition, a large amount of data (Internet traffic) is generated in the process of physical examination and treatment of patients, and doctors can use these data to make more reliable and accurate diagnoses. Mobile medical not only saves a lot of time spent on queuing up for registration, but also greatly reduces the pressure on the infrastructure brought by disease treatment. Through mobile sensors, medical devices, and remote patient monitoring products,

there are avenues through which medical care delivery can be improved. Mobile medical can help lower costs and connect people to care providers.

However, these mobile medical-related technologies are still incomplete [5]. They have certain flaws in the preservation of privacy. With the development of mobile medical, medical data are showing exponential growth. Meanwhile, these data collected by terminal equipment in mobile medical mode are closely related to users' physiological characteristics, geographic locations, images, and other private information [6].

In addition, with the rapid development of network intrusion technologies, personal medical data are facing risks of intentional or unintentional intrusion and access by unauthorized users. Due to the incomplete privacy preservation technologies, lacks, data security, and privacy preservation have become the main reason restricting the development of modern medical services. Due to the limitation of terminal resources and the sensitivity of medical information, existing privacy preservation technologies are difficult to directly apply. The design of specific security authentication, information integration, data access control, and data integrity verification schemes for mobile health environment is an important topic in the field of mobile health at present and in the future, and it is also a key link for the large-scale application of mobile medical in practice.

In this paper, we mainly discuss privacy preservation solutions of mobile terminals in Internet medical, which integrates the application of lightweight authentication, blockchain technology, anonymous certificates, and searchable encryption technology to realize the encrypted calculation and ciphertext of mobile medical device data. Data sharing has been implemented, and privacy preservation of medical data has been implemented.

2. Related Works

For the storage and transmission of medical data, scholars around the world have conducted a lot of researches. In 2012, Patra et al. [7] proposed a cloud-based model to process private data for patients. Through his framework, medical personnel and policy makers can use the cloud-based model to provide remote medical services to patients. This model stores all necessary data in a single cloud. By encouraging patients to share data in the cloud, patients can obtain medical staff services. Disease diagnosis and control can be performed through remote treatment. In 2014, Ye et al. [8] proposed a well-organized authentication and access control scheme based on the attributes of the perceived IoT access control layer.

In 2015, Zyskind et al. [9] proposed a privacy preservation platform, which uses third-party equipment to provide services and allows users to modify authorization while following the access control policies reserved on the blockchain. The proposed decentralized platform contains three objects: service providers, mobile phone users, and nodes that maintain the blockchain. Two types of transactions can be defined in the blockchain network in the platform: Tdata for data storage and recovery and access

time and Taccess for access control management. The data collected through the user's mobile phone is encrypted and saved outside the blockchain. In the public chain, only data hashes are saved. Both users and services can query the data in Tdata transactions. In 2016, to solve the problems of slow medical record information access, data fragmentation, and user privacy preservation, Azaria et al. [10] completed a medical data sharing platform MedRec based on Ethereum. Peterson et al. proposed a blockchain-based participant in advance. A medical data sharing plan with a well-defined rule structure is agreed. Although this solution realizes the sharing of medical data, it lacks a universal access control strategy.

In 2017, Omar et al. [11] proposed data management system for patient healthcare. By adopting blockchain to protect privacy storage, it solves the problem of losing control when storing encrypted data in the system. In addition, by using encryption on the blockchain, the framework will not be affected by data preservation vulnerabilities. Do and Ng [12] proposed a system that uses blockchain technology to provide secure distributed data storage with keyword search services.

In 2018, Magyar [13] designed an integrated health information model that builds a decentralized and openly scalable network based on the blockchain operating environment, making access to data more secure. In order to handle the protected health information (PHI) generated by these devices, Griggs et al. [14] proposed utilizing blockchain-based smart contracts to facilitate secure analysis and management of medical sensors. Using a private blockchain based on the Ethereum protocol, they created a system where the sensors communicate with a smart device that calls smart contracts and writes records of all events on the blockchain. This smart contract system would support real-time patient monitoring and medical interventions by sending notifications to patients and medical professionals, while also maintaining a secure record of who has initiated these activities. This would resolve many security vulnerabilities associated with remote patient monitoring and automate the delivery of notifications to all involved parties in a HIPAA compliant manner. Liang et al. [15] proposed an innovative user-centric health data sharing solution, which uses the blockchain mechanism to protect privacy, strengthen identity management, and collect data in conjunction with mobile applications. Zhang and Lin [16] proposed a personal health record sharing scheme based on blockchain. This solution builds two different blockchains to realize the safe sharing of medical data. The plan separately builds a private chain and a consortium chain. The private chain realizes the encrypted storage of personal medical data. The consortium chain saves the security index corresponding to the personal medical data and secures the data sharing by verifying the doctor's identity token, which protects the medical data. However, using two types of blockchains will not only increase costs, but also reduce their execution efficiency. Ji et al. [17] investigated the location sharing based on blockchains for telecare medical information system. Firstly, they define the basic requirements of blockchain-based location sharing, including

decentralization, unforgeability, confidentiality, multilevel privacy preservation, retrievability, and verifiability. Then, using order-preserving encryption and Merkle tree, they proposed a blockchain-based multilevel location sharing scheme.

In 2019, Wang et al. [18] combined homomorphic encryption and proxy reencryption technology to implement outsourcing computing solutions in healthcare systems. In this solution, there are several clients with different public keys, an electronic medical cloud platform, and an auxiliary cloud server. The electronic medical cloud platform can provide services to patients and regularly analyze data to provide better services. The HGD architecture based on blockchain proposed by Yue et al. [19] enables patients to safely control and share medical data. Aiming at the privacy of medical data, Tian et al. [20] proposed to establish a shared key that can be reconstructed by legitimate parties before the diagnosis and treatment process begins.

At present, a large number of excellent schemes [21–23] have emerged in mobile medical, and their security and flexibility have been continuously enriched. The characteristics of activity and diversification can better meet the needs of practical application, but there are still some deficiencies. Some schemes encrypt the patient information and store it on the blockchain, and some schemes use anonymous certificates to protect user information. But the doctor cannot read the relevant information. Therefore, it is necessary to design a scheme that can authenticate the device.

3. Scheme

3.1. Structure. As shown in Figure 1, the local computer of the mobile medical model generates the relevant parameters and sends them to the smart wearable device to start the authentication scheme. After a series of simple calculations, the smart wearable device feeds back the relevant parameters to the local computer. The local computer and the local blockchain node undergo a similar calculation process, and the blockchain node obtains the relevant parameters and sends them to the local computer; the local computer forwards the parameters to the smart wearable device. The smart wearable device performs decryption calculation and passes the verification, and the identity authentication ends smoothly. There are many kinds of mobile medical devices, including bracelets, watches, mobile phones, portable computers, etc. These devices can collect a variety of physiological signals of users, such as blood pressure, blood glucose, blood oxygen, body temperature, etc. After the authentication, the intelligent devices will upload those collected information to the blockchain.

The alliance chain is a blockchain that is jointly managed by multiple institutions, and the joining of network nodes requires the approval of the organization. It completes mutual authentication of the internal membership of the system through the PKI system. The user binds his real identity with the self-signed certificate issued by the CA in the PKI system. We divide the authority of CA into TCA and regulator, and TCA and regulator jointly issue anonymous

certificates. After the anonymous certificate is generated, the local device successfully joins the blockchain network.

In order to ensure the privacy of users' medical and health data, the data on the chain is encrypted. For users who need to perform operations such as searching encrypted data, we adopt searchable encryption technology. It can support users to carry out keyword retrieval in ciphertext and realize keyword based secure search. It enables users to store encrypted data in the blockchain, perform keyword search through the ciphertext domain, and selectively retrieve relevant documents from it, so as to ensure the security of data.

3.2. Module

3.2.1. Anonymous Certificate Generation. A user submits the real-name certificate application and his real identity information to the CA. After the CA verifies, the real-name certificate E_{cert} will be issued by the user and saved in the CA database U . Then he generates his own anonymous identity AID, public and private key pair (APK, SPK), and random numbers p, r_1 and calculates the serial number of the anonymous certificate: $SN = H(APK, p)$. Then anonymous certificate header $b = (AID, SN, APK)$ and content $M = (b, h(E_{cert}))$ are generated. After calculating the formula $u = g^{r_1}$, the user sends u and the real-name public key signature $SigPK(u)$ to the supervisor Admin. Verifying the signature information sent by the user, Admin calculates the formula $w = u_{d_1}$ and sends w to the user, which will be saved in the supervisor database in the form of key-value pairs $\langle E_{d_1}(u): ID \rangle$. After the user accepts w , he uses ASK to perform signature calculation on M which is $Sig_{ASK}(M)$ and send random numbers r_1 and w to TCA. Then the TCA verifies the parameters sent by the user and, after the verification passes, calculates the formula $z = w_{d_2}$ and judges whether $Q = zr_1^{-1}$ is true. If $Q = zr_1^{-1}$, save $\langle SN: E_{d_2}(z) \rangle$ in the database in the form of key-value pairs. Then it generates a random number r_2 , calculates the joint signature: $Usigd = (g^{r_2}, (h^{-1}(M) + g^{r_2 * d_1 * d_2}) \cdot r_2^{-1})$, and sends it to the user. Then the user gets the anonymous certificate $(M, Usigd)$.

3.2.2. Lightweight Authentication. Relevant parameters in this section are shown in Table 1.

First the local computer generates a random number x and a timestamp t_R and sends them to the smart wearable device. After receiving the parameters, the device calculates whether $|t_R - t_R^*| \leq \Delta T$ is true. If not, the communication delay is greater than the maximum delay allowed by the system, so the authentication stops. If $|t_R - t_R^*| \leq \Delta T$, the smart wearable device generates a random number y and a timestamp t_T and performs the following calculations based on ID and K :

$$N_1 = \text{ROL}(K \oplus y, x), \quad (1)$$

$$N_2 = \text{ROL}(ID \oplus y, x). \quad (2)$$

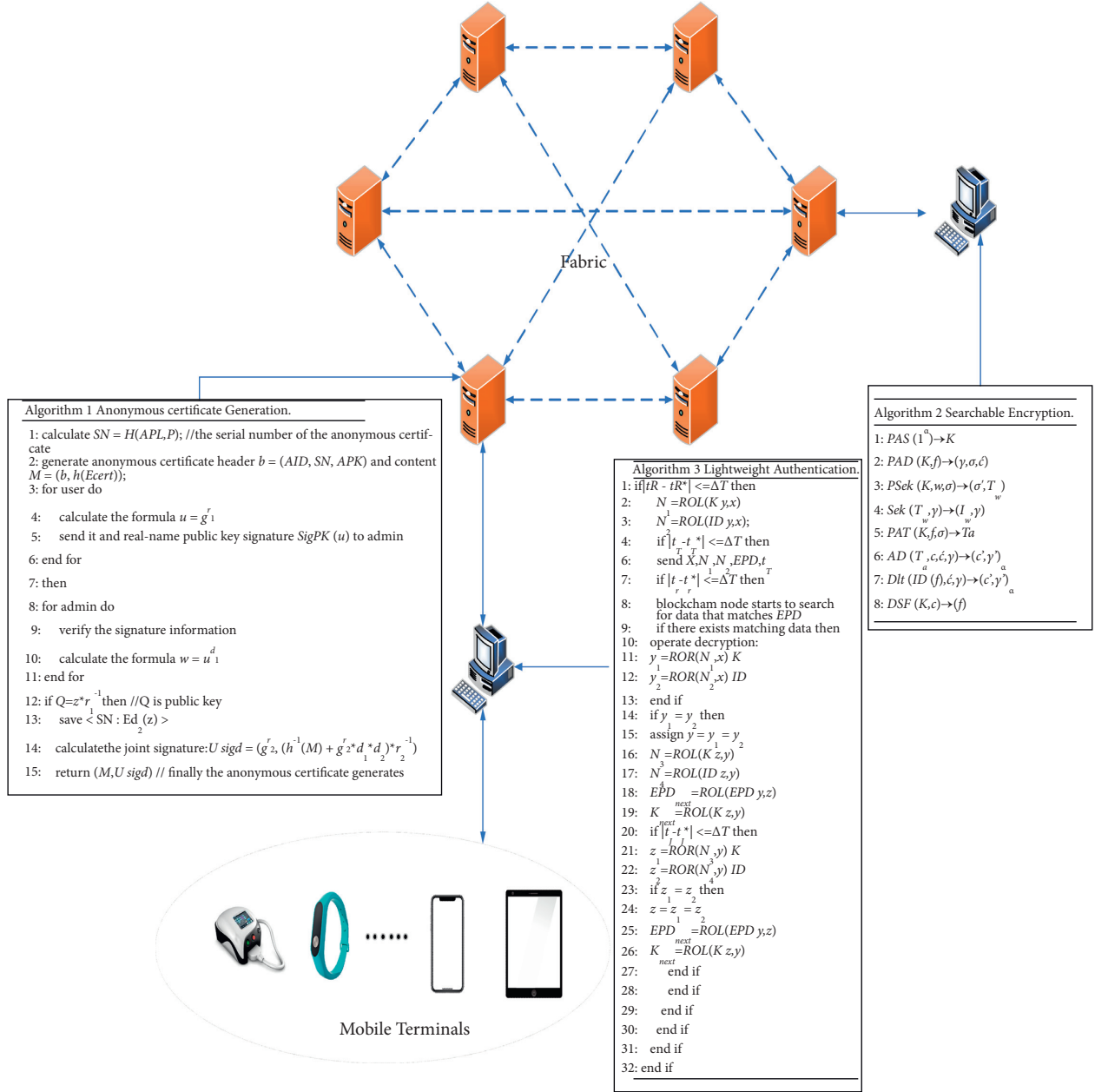


FIGURE 1: The system structure.

The smart wearable device feeds N_1, N_2, EPD, t_T, x to the local computer. When receiving those parameters, the local computer calculates whether $|t_T - t_T^*| \leq \Delta T$ is true. If true, the local computer generates a timestamp t_r and sends N_1, N_2, t_r, x , and EPD to the blockchain node. If not, the authentication stops.

When $|t_T - t_T^*| \leq \Delta T$ and the blockchain node receives the parameters, the node calculates whether $|t_T - t_T^*| \leq \Delta T$ is true. If $|t_T - t_T^*| \leq \Delta T$, the blockchain node starts to search for data that matches EPD ; else the authentication stops. If there is no matching data, we can obtain the matching ID and K for decryption operation. Perform the following calculations $y_1 = ROR(N_1, x) \oplus K$ and $y_2 = ROR(N_2, x) \oplus ID$. Then judge whether y_1 and y_2 are equal. If $y_1 \neq y_2$, it indicates that the data is not credible, and

the authentication stops. If $y_1 = y_2$, the blockchain node authentication continues and assigns $y = y_1 = y_2$. The blockchain node generates a random number z and a timestamp t_j to perform the following calculations: $N_3 = ROL(K \oplus z, y)$ and $N_4 = ROL(ID \oplus z, y)$. After that, the following operation formulas $EPD_{next} = ROL(EPD \oplus y, z)$ and $K_{next} = ROL(K \oplus z, y)$ can be obtained.

The blockchain node sends N_3, N_4, t_T to the local computer. After the local computer receives the parameters, it first calculates whether $|t_j - t_j^*| \leq \Delta T$ is true. If not, the communication delay is greater than the maximum delay allowed by the system, and the authentication fails. Otherwise, the local computer will send N_3, N_4 to the smart wearable device. After receiving the parameters, the smart wearable device decrypts N_3 and N_4 . Then, it is judged

TABLE 1: Parameters of the lightweight authentication.

Symbol	Explanation
t^*_R	The time when the smart wearable device first received a local computer message
ΔT	Maximum transmission delay allowed in the system
t^*_T	The time when the local computer first received the smart wearable device
t^*_r	The time when the blockchain node first received a local computer message
EPD	Pseudonyms for smart wearable devices
$hm(X)$	Represent the Hamming weight of binary string X
$ROR(X, Y)$	X and Y are binary strings with a length of L bits. Circulate the binary string Y to the right to move $hm(X)$ bits of the binary string X , then get the result of $ROR(X, Y)$
ID	Identifier of smart wearable device
K	Shared key value between smart wearable device and blockchain node
$hm(Y)$	Represent the Hamming weight of binary string Y
$ROL(X, Y)$	X and Y are binary strings with a length of L bits. Circulate the binary string X to the right to move $hm(Y)$ bits of the binary string Y , then get the result of $ROL(X, Y)$

whether $z_1 = z_2$ is true while $z_1 = ROR(N_3, \gamma) \oplus K$, and $z_2 = ROR(N_4, \gamma) \oplus ID$. If not, it indicates that the data is not credible, and the authentication stops. If $z_1 = z_2$, the smart wearable device authentication is passed, and the value $z = z_1$ or $z = z_2$ is assigned. Perform the following calculations: $EPD_{next} = ROL(EPD \oplus \gamma, z)$ and $K_{next} = ROL(K \oplus z, \gamma)$. Finally, the update and the identity authentication are finished.

3.2.3. *Searchable Encryption.* Relevant parameters in the section are shown in Table 2.

We first perform the formula $PAS(1^\alpha)$ which is just a probabilistic algorithm, and then we can get the key $K = (k_1, k_2)$ while $k_1 = \{0, 1\}^\alpha$ and $k_2 = PAS(1^\alpha)$. If we want to query the search index γ and search history σ , we need to create three empty hash linked lists $\gamma_f, \gamma_w, \gamma_d$ and an empty set σ firstly. For any file $f \in \mathcal{f}$, the unique keyword set of f is \bar{f} and $f \supseteq \bar{f} = (w_1, \dots, w_{\text{lenth}(\bar{f})})$. Generate a string of pseudorandom sequences $s_1, \dots, s_{\text{lenth}(\bar{f})}$ through the pseudorandom number generator. Set $\tau_{w_i} = F_{k_1}(w_i)$ and $\tilde{c}_i = H_{\tau_{w_i}}(s_i) \parallel s_i$ if $w_i \in \bar{f}$ and $1 \leq i \leq \text{lenth}(\bar{f})$. $\bar{c} = (c_1, \dots, c_{\text{lenth}(\bar{f})})$ is sorted by dictionary order and saved in γ_f . Then set $\gamma_f[ID(f)] = \bar{c}$. Calculate the formula: $c = SKE.PAD_{k_2}(f)$. For the keyword w to be searched, calculate the search label: $\tau_w = F_{k_1}(w)$ and $\sigma' = \sigma \cup \{\tau_w\}$. Then, output the updated search history σ' and search credentials τ_w . First set $\gamma = (\gamma_f, \gamma_w, \gamma_d)$. Then figure out whether there is a key value related to τ_w in hash list γ_w , and whether there is key value related to τ_w in the hash chain table γ_w . If a key value is related to τ_w in the hash chain table γ_w , set $I_w = \gamma_w[\tau_w]$ and $\gamma_w' = \gamma_w$. If not, generate an empty list I_w for any $\bar{c} \in \gamma_w$.

For any $\tilde{c}_i \in \bar{c}$, $1 \leq i \leq \text{lenth}(\bar{c})$, set $\tilde{c}_i = l_i \parallel r_i$, and verify whether $H_{\tau_w}(r_i) = l_i$ is true. If true, insert the file identifier $ID(f)$ which is corresponding to \bar{c} into I_w , and add τ_w to $\gamma_d[ID(f)]$. Update $\gamma_w[\tau_w] = I_w$, and set updated indexes as γ_f' and γ_d' . We get I_w and $\gamma' = (\gamma_f, \gamma_w', \gamma_d')$ at last. For the file f to be added and its unique keyword set \bar{f} , a series of pseudorandom sequences $s_1, \dots, s_{\text{lenth}(\bar{f})}$ is generated by the pseudorandom number generator. Create an empty list X , for any $w_i \in \bar{f}$, $1 \leq i \leq \text{lenth}(\bar{f})$. Calculate the formula below.

$$\tau_{w_i} = F_k(w_i). \quad (3)$$

If $\tau_{w_i} \in \sigma$, it means this keyword has been searched. Insert τ_{w_i} into list X , and its formula can be expressed as follows:

$$\tilde{c}_i = H_{\tau_{w_i}}(s_i) \parallel s_i, \quad (4)$$

$\bar{c} = (\tilde{c}_1, \dots, \tilde{c}_{\text{lenth}(\bar{f})})$ is sorted by dictionary order which means $\bar{c} = SKE.Enc_{k_2}(f)$. While $\tau_\alpha = (ID(f), \bar{c}, c, X)$ and $\gamma = (\gamma_f, \gamma_w, \gamma_d)$, add $\gamma_f[ID(f)] = \bar{c}$ to the index γ_f , for any $x_i \in X$, and $ID(f)$ is added to $\gamma_w[x_i]$. Then set $\gamma_d[ID(f)] = X$. The updated index is $\gamma_f', \gamma_w', \gamma_d'$. Add c to c . The updated ciphertext collection is marked as c' and then (c', γ') will be output where $\gamma' = (\gamma_f', \gamma_w', \gamma_d')$. When we want to decrypt the file ciphertext c , we input the key, and then we get the decrypted file; the formula can be expressed as follows: $f = SKE.DSF_{k_2}(c)$.

4. Experiment and Analysis

In this section, we discussed the performance of our scheme and analyzed the results of simulated experiments. We tested and compared the performance efficiency and storage cost of the lightweight authentication with others. We also compared our lightweight searchable encryption with others.

We compared Fabric with Corda, FISCO BCOS, and Quorum. The result is shown in Table 3. Considering that our scheme is oriented to mobile medical, we chose ‘‘Fabric’’ as our blockchain framework in the end.

Hyperledger Fabric is managed by the Linux Foundation, hoping to change the single common network mode of the public chain. By establishing multiple interconnected blockchain networks to cover all kinds of different business scenarios, it realizes the flexibility of design, meets the diversified requirements, and realizes the interaction between networks. This idea is reflected in its unique channel mechanism design. Hyperledger Fabric aims to build an open source framework for general blockchain regardless of industry and has the largest consensus in the consortium chain. FISCO BCOS originates from the enterprise blockchain platform BCOS. As a branch of the financial version, it pays more attention to the financial industry while retaining its universality and takes more account of the particularity of regulators. It is applicable to a wide range of distributed

TABLE 2: Parameters of the searchable encryption.

Symbol	Explanation
$\{0, 1\}$	Binary sequence with length n
$\{0, 1\}$	Binary sequence of arbitrary length
$\text{len}(u)$	Bit length of binary sequence u
$u\ v$	Connection of binary sequences u and v
$z \leftarrow A$	Z is the output of probabilistic algorithm A
α	Security parameters
SKE (PAS, PAD, DSF)	Symmetric encryption scheme against indistinguishable selective plaintext attack

TABLE 3: Comparison of blockchain platform.

Name	Data model	Consensus mechanism	Smart contract	Database
Fabric	Account based	Solo/Kafka/PBFT	Go/Node.js/Java	LevelDB/CouchDB
BCOS	Account based	Raft/PBFT	Solidity	Level DB
Corda	Transaction based	Notary	Java/Kotlin	Relational database
Quorum	Account based	Raft/PBFT	Solidity	Level DB

business scenarios. Corda is aimed at the financial industry and clearly stated that it will not consider other industries for at least a certain period of time. Corda hopes to provide a global logical account with uniqueness and authority that can record all the agreements between enterprises. The core is to achieve a noncentral database with the minimum trust mechanism between nodes. Corda advocates fully considering the combination with the existing business system rather than dismantling the existing business system. Quorum is an alliance chain scheme, an enterprise-level distributed ledger, and intelligent contract platform developed by JPMorgan. It is developed on the basis of Ethereum, providing private intelligent contract execution scheme and meeting the performance requirements of the enterprise, applicable to scenarios requiring high-speed transactions and private transactions between high-throughput processing alliances, designed primarily to address the special challenges of blockchain applications in finance and other industries.

In the current medical industry, we need to build licensed blockchains, such as hospitals, which need to operate under strict regulatory requirements, and cannot let unknown users view transaction data. In addition, medical information is very important, so unauthorized viewing will leak patient information in the future. At the same time, Fabric is a framework that requires prior permission. All participants have known identities and are verified according to the organization's identity management system. There are no anonymous or pseudonymous users.

As a result, we chose Fabric finally.

We analyzed the security and privacy of our proposed scheme. The details are as follows. The specific experimental environment is shown in Table 4.

4.1. Test

4.1.1. Lightweight Authentication. In this section, the performances of mobile medical devices are compared with classical authentication schemes.

TABLE 4: The experimental environment.

CPU	AMD Ryzen 5900x
GPU	NVIDIA GeForce GTX 2080Ti
Memory of single pc	16G
Blockchain architecture	Fabric 2.0
System version	Ubuntu 18.04
Database	MySQL 8.0

Assume that the length of communication, traffic, and storage parameters are the same. There are four kinds of information, that is, IDS, ID, K, and ΔK saved in mobile terminal devices in the medical system. In our scheme, there are 14 session messages in a complete session. At the same time, there are 14 session messages in [24] and 10 session messages in [25]. Reference [26] has 16 session messages. Reference [27] and reference [28] have 10 messages. Therefore, the communication traffic size is 14 in our scheme. It can be seen from Figure 2 that our scheme can reduce the computing burden.

From the point of view of the computing burden, our scheme and the scheme in [28] are both ultralightweight. The algorithms used in other comparative references are all lightweight, so the scheme in this paper has great advantages in reducing the calculation time. The result is shown in Table 5.

In the scheme of [28], the computation of shared secret key and pseudonym updating is more complex, which increases the number of CMO operations, so the overall calculation cost is higher than our scheme. In our scheme, the steps of calculation are as follows. Firstly, we generate a random number x ($\Delta y/\Delta x$) to operate RAN. Secondly, in the process of calculating messages N_1 and N_2 , we perform CMO operations on N_1 and N_2 , respectively. Thirdly, the third and fourth CMO operations and the first and second DIG operations are needed to decrypt messages N_3 and N_4 . Lastly, we perform the last two CMO operations to update the shared secret values and pseudonyms. Therefore, the total computing burden in our scheme is $6\text{CMO} + 2\text{DIG} + 1\text{RAN}$.

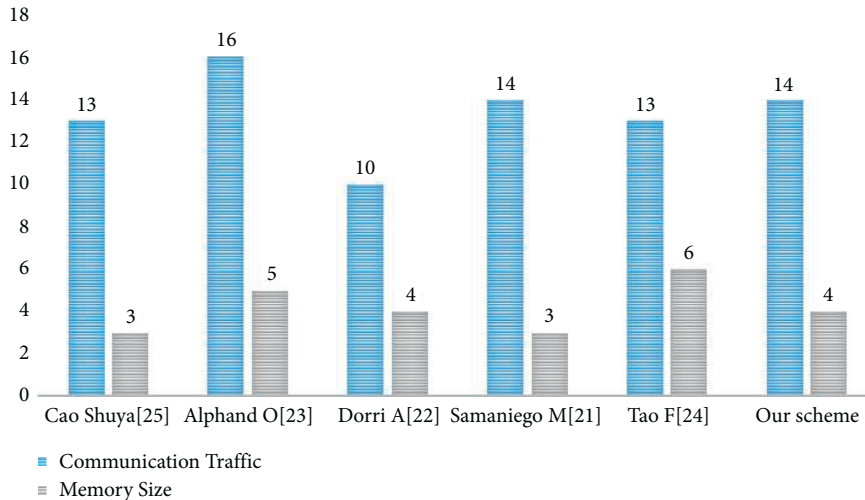


FIGURE 2: Comparison of communication.

TABLE 5: Performance comparison of different schemes.

Symbol	Explanation
Reference [24]	5PUF + 5DIG + 1RAN
Reference [25]	7MOD + 2DIG + 2RAN
Reference [26]	6HASH + 3DIG + 1RAN
Reference [27]	7PRNF + 4DIG + 2RAN
Reference [28]	11CMO + 4DIG + 1RAN
Our scheme	6CMO + 2DIG + 1RAN

Symbols of lightweight authentication are shown in Table 6.

4.1.2. Searchable Encryption. The performances of our scheme are compared with other references, and the results are shown in Table 7.

Our scheme gradually builds indexes in the search process. At the beginning, maintain a regular index γ_f and store the encrypted keywords for each file. Once a keyword w is retrieved, the identifier of all the files containing the keyword is moved into a reverse index γ_w , and a delete index γ_d is constructed to store the keywords that have been searched for in the files appearing in γ_w . A search history is maintained at the client to record which keywords have been searched. The searched keywords can directly query the index γ_w to obtain the search results. This disperses the time and storage cost of building index tables into each search process, saving search time.

Descriptions of the relevant symbols are as shown in Table 8.

The biggest improvement of our scheme compared with scheme [33] is the deletion of index γ_d , which reduces the execution time of deletion operation to a certain extent. We mainly compare the deletion operations of the two schemes.

For each file deleted in the scheme of [33], traverse each item in γ_w and find each node in $\gamma_w[\tau_w]$ one by one until the identifier of the deleted file is found or the end node is reached. In this scheme, delete index γ_d is used. When deleting a file, read $\gamma_d[\text{ID}(f)]$ directly. For any x_i in

$\gamma_d[\text{ID}(f)]$, only find each node in the list of $\gamma_w[x_i]$ in γ_w until finding the identifier of the deleted file.

We select 51 English documents. First, we convert all uppercase to lowercase, remove all punctuation, and separate words only with space. According to statistics, there are 3711262 words in 51 documents, removing duplicate words in each document, leaving a total of 373221 unique words. We search for 5000 words; that is, there are 5000 input items in the search index γ_w , 51 documents are searched, and 51 input items in the index γ_d are deleted. We delete five files, respectively, and give the traversal times and time consumption of the two schemes when deleting files, as shown in Table 9. The traversal times are the comparison times of nodes in the list in tables γ_w and γ_d when deleting files. The result is shown in the following table.

4.1.3. Blockchain. Due to the dependence and mobility on massive data, the performance index of blockchain is quite important, which includes latency, energy consumption, throughput, and scalability.

In our experiment, we used the Caliper to test the performance. Caliper is a blockchain performance testing framework that currently supports testing for processing traffic (TPS), latency, and resource utilization. After each round of test, users can obtain a series of test results and reports by Caliper. The result is shown in Figure 3.

As shown in Figure 4, the throughput increased steadily with the increase of transaction times. It reached the peak when the transaction times reached 5000, the throughput is

TABLE 6: Parameter values.

Symbol	Explanation
PUF	Computation amount of physical unclonable function
DIG	Computation amount of physical unclonable function
RAN	The amount of calculation to generate random numbers
MOD	Modular calculation amount
HASH	Calculation amount of hash function
PRNF	The amount of calculation to generate a pseudorandom function
CMO	Calculation amount of circular movement operation

TABLE 7: Parameter values.

Literature	Search time	Index space	Update leak	Update cost
Literature [29]	$O(m/n)$	$O(m+n)$	$ID(w)$	$O(m+n)$
Literature [30]	$O(\log f \bullet m/n)$	$O(f \bullet n)$		$O(\log f \bullet m/n)$
Literature [31]	$O(m/n)$	$O(m+n)$		$O(m+n)$
Literature [32]	$O(m/n)$	$O(m+n)$	$ID(w)$	$O(m+n)$
Literature [33]	$O(m/n)$	$O(m+n)$		$O(m+n)$
Our scheme	$O(m/n)$	$O(m+n)$		$O(m+n)$

TABLE 8: Parameter values.

Symbol	Explanation
n	The total number of unique keywords
m	The total number of all keywords
$ID(w)$	Fixed identifier for the keyword
$ f $	Total number of files

TABLE 9: Comparison of our scheme and scheme of [33].

Document		f_1	f_2	f_{20}	f_{40}	f_{51}
Scheme [33]	Number of traversals	34656	32474	39447	32495	47693
	Time (ms)	4.7	2.8	1.9	5.1	1.1
Our scheme	Number of traversals	25160	17919	15734	11353	7
	Time (ms)	3.2	1.8	1.7	1.9	0.01

296.4TPS, and the average latency is 215.4 ms. Then it began to decline slowly when the transactions times exceed 5000. At present, there is no national standard for blockchain performance indicators, and China Institute of Information and Communications is actively formulating it. According to the existing blockchain industry standards (Table 10), the performance of our system meets the requirements.

4.2. Security

- (1) In design of the authentication scheme, the pseudonym of a smart wearable device is introduced, which is transferred during each communication, and the pseudonym is updated after each communication, so that the pseudonym of each round is different. Additionally, other private information that needs to be sent is encrypted before it can be sent, which makes it impossible for attackers to obtain useful and valid information. Therefore, attackers cannot learn the real identity information of a smart wearable device user. Hence, this scheme can

provide the anonymity of entities. At the same time, our scheme uses the method of mixing random numbers in the message encryption. The random number is randomly generated by the system, and it is unpredictable and inconsistent. Therefore, the attacker cannot analyze the value of the next round of communication messages by intercepting the current message or deduce the user's privacy information in the previous round of communication messages, which makes the scheme more secure.

- (2) In process of anonymous certificate generation, TCA is visible to the content of the certificate but invisible to the user's identity, while regulators are visible to the user's identity but invisible to the content of the certificate, which enhances the anonymity of the user. In addition, in the process of tracking the user's real identity, TCA and regulators need to provide their own key information, which reduce the threat of unilateral dishonesty and single point attack on the security of anonymous certificates. In our scheme, we disclose specific information to the server during the operations of query and update. Next, we use the following leak functions L_{search} , L_{add} , L_{delete} , $L_{encrypt}$ to give the leaked information.

In our scheme,

$$L_{search}(f, w) = (ACCP_t(w), ID(w)), \quad (5)$$

$$L_{delete}(f, w) = (ID(f), SRCH_HIS(\bar{f})), \quad (6)$$

$$L_{encrypt}(f) = \text{length}(f), \quad (7)$$

$$L_{add}(f, f) = (ID(f), \text{lenth}(\bar{f}), SRCH_HIS(\bar{f})). \quad (8)$$

According to the above leak functions, except the access model, our scheme does not disclose more information to the server. The relevant parameters are shown in Table 11.

```

###test result:###
+-----+-----+-----+-----+-----+-----+-----+-----+
| Name   | Succ  | Fail  | Send Rate (TPS) | Max Latency (s) | Min Latency (s) | Avg Latency (s) | Throughput (TPS) | Avg Response (s) |
+-----+-----+-----+-----+-----+-----+-----+-----+
| writeAsset | 11719 | 0     | 275.3          | 2.11             | 0.06            | 0.48           | 256.1            | 0.48             |
+-----+-----+-----+-----+-----+-----+-----+-----+

### resource stats ###
+-----+-----+-----+-----+-----+-----+-----+-----+
| Name           | CPU% (max) | CPU% (avg) | Memory (max) [MB] | Memory (avg) [MB] | Traffic In [MB] | Traffic Out [MB] | Disc Write [MB] | Disc Read [MB] |
+-----+-----+-----+-----+-----+-----+-----+-----+
| dev-peer1.org2.fabComm... | 2.55       | 1.89       | 9.13            | 9.11             | 8.91            | 2.63            | 0.00            | 0.00            |
| dev-peer0.org1.fabComm... | 2.95       | 1.93       | 11.2           | 11.2            | 9.02            | 2.66            | 0.00            | 0.00            |
| dev-peer0.org2.fabComm... | 0.00       | 0.00       | 10.1           | 10.1            | 0.000479       | 0.000542       | 0.00            | 0.00            |
| cli            | 0.00       | 0.00       | 7.35           | 7.35            | 0.00            | 0.00            | 0.00            | 0.00            |
| peer0.org2.fabComm.com   | 14.23      | 7.93       | 342            | 315             | 34.2           | 0.484          | 102             | 0.00            |
| orderer.fabComm.com     | 10.19      | 7.44       | 120            | 104             | 36.6           | 69.9           | 70.2            | 0.00            |
| peer0.org1.fabComm.com   | 21.10      | 16.10      | 332            | 312             | 45.1           | 20.2           | 102             | 0.00            |
| peer1.org2.fabComm.com   | 20.30      | 15.29      | 321            | 295             | 44.8           | 50.3           | 102             | 0.00            |
| peer1.org1.fabComm.com   | 12.76      | 9.02       | 334            | 311             | 34.4           | 37.9           | 102             | 0.00            |
+-----+-----+-----+-----+-----+-----+-----+-----+
    
```

FIGURE 3: One round of test.

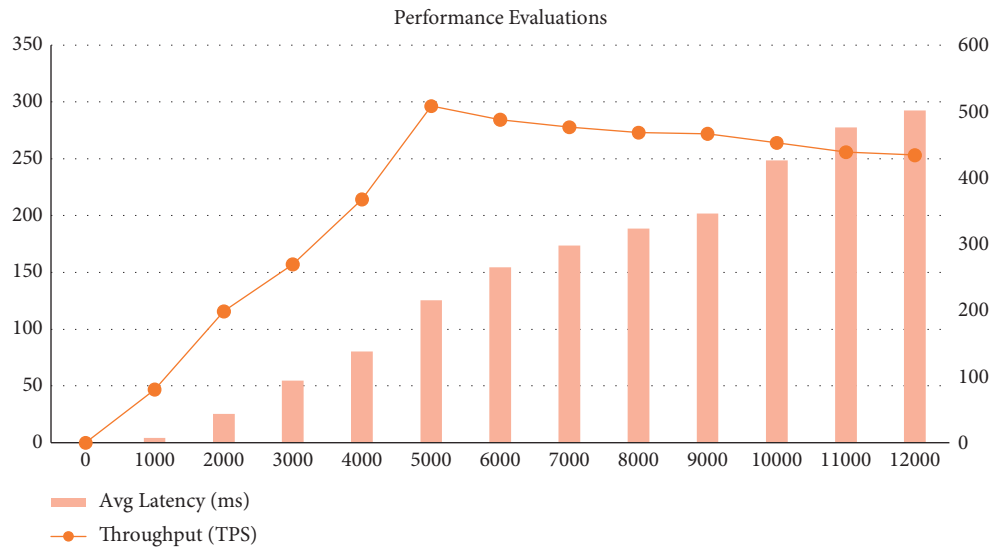


FIGURE 4: Performance evaluations.

TABLE 10: Blockchain industry standards.

Name	Requirement cost
Success	Rate >95%
Average	Response time <0.5 s
Average latency	<1 s
Throughput (TPS)	200–300
Success rate	>95%

TABLE 11: Symbols of leak functions.

Symbol	Explanation
$ACCP_t(w)$	Access pattern, the file identifier of the file in f_w when the keyword w is queried at time t , that is, the set $\{ID(f_i): w \in f_i, f_i \in f\}$
\bar{f}	Unique keyword set of files f
$SRCH_HIS(\bar{f})$	The set of identifier $ID(w)$ of keywords that have been searched in time t file f , that is, the set $SRCH_HIS(\bar{f}) = \{ID(w_i): w_i \in f, \tau_{w_i} \in \sigma\}$

5. Conclusion

As an intelligent product at this stage, mobile intelligent terminal integrates the existing information system of the hospital through mobile Internet technology, shares and exchanges clinical business data, and provides a new way of diagnosis and treatment for the hospital. To solve the problem of privacy leakage of medical patients, we design a privacy preservation scheme based on mobile terminals in Internet medical by combining privilege separation, authentication scheme, lightweight loop operation, and improved searchable encryption algorithm in the model system, and we conducted a comparative experiment on data from different systems. Compared with the original anonymous authentication system, we separate the regulator and TCA authority and improve the efficiency of certificate generation by 34.8% compared with the scheme. The results show that the model trained by our scheme has less calculation burden, better stability, and higher security. Further works are as follows.

- (1) To improve the efficiency of searchable encryption.
- (2) To expand the diversified search functions. Except the basic search function, we also need to support some special functions, such as approximate search, wildcard search, fuzzy search, multikeyword search, and so on. Increasing the diversity of search functions is an important research direction in the future.

Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

- [1] D. M. West, *Improving health care through mobile medical devices and sensors*, Brookings Institution Policy Report, vol. 10, , pp. 1–13, 2013.
- [2] Y. Huang, H. Xue, H. Gao, X. Ma, and W. Hussain, “SSUR: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center,” *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 670–681, 2021.
- [3] H. Gao, W. Huang, and Y. Duan, “The cloud-edge-based dynamic reconfiguration to service workflow for mobile ecommerce environments,” *ACM Transactions on Internet Technology*, vol. 21, no. 1, pp. 1–23, 2021.
- [4] X. Yang, S. Zhou, M. Cao, and Applications, “An approach to alleviate the Sparsity problem of hybrid collaborative filtering based recommendations: the product-attribute perspective from user reviews,” *Mobile Networks and Applications*, vol. 25, no. 2, 2020.
- [5] S. Deng, Z. Xiang, J. Taheri et al., “Optimal Application Deployment in Resource Constrained Distributed Edges,” *IEEE Transactions on Mobile Computing*, vol. 99, p. 11, 2020.
- [6] J. Xiao, H. Xu, H. Gao, M. Bian, and Y. Li, “A weakly supervised Semantic Segmentation network by aggregating seed cues: the multi-object proposal generation perspective,” *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 17, no. 1s, pp. 1–19, 2021.
- [7] M. R. Patra, R. K. Das, and R. P. Padhy, “CRHIS: cloud based rural healthcare information system,” in *Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance*, pp. 402–405, New York, NY, United States, 2012.
- [8] N. Ye, Y. Zhu, R.-c. Wang, R. Malekian, and Q.-m. Lin, “An efficient authentication and access control scheme for perception layer of internet of things,” *Applied Mathematics & Information Sciences*, vol. 8, no. 4, 2014.
- [9] G. Zyskind, O. Nathan, and A. S. Pentland, “privacy: using blockchain to protect personal data,” in *Proceedings of the IEEE Security & Privacy Workshops*, p. 180 184, San Jose, CA, USA, May 2015.
- [10] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: using blockchain for medical data access and permission management,” in *Proceedings of the International Conference on Open & Big Data*, Vienna, Austria, August 2016.
- [11] A. A. Omar, M. S. Rahman, A. Basu, and S. K. MediBchain, “A blockchain based privacy preserving platform for healthcare data,” in *Proceedings of the International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, Zhangjiajie, China, November 2017.
- [12] H. G. Do and W. K. Ng, “Blockchain-based system for secure data storage with private keyword search,” in *Proceedings of the IEEE World Congress on Services (SERVICES)*, pp. 90–93, Honolulu, HI, USA, May 2017.
- [13] G. B. Magyar, “Solving the Privacy and Research Availability Tradeoff for EHR Data,” in *Proceedings of the A New Disruptive Technology in Health Data Management*, pp. 000135–000140, IEEE 30th Neumann Colloquium, Budapest, Hungary.
- [14] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, “Healthcare blockchain system using smart contracts for secure automated remote patient monitoring,” *Journal of Medical Systems*, vol. 42, no. 7, pp. 130–137, 2018.
- [15] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, “Integrating blockchain for data sharing and collaboration in mobile healthcare applications,” in *Proceedings of the The 28th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1–5, IEEE PIMRC, Montreal QC Canada, June 2017.

- [16] 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.
- [17] Y. Ji, J. Zhang, J. Ma, C. Yang, and X. Yao, "BMPLS: blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems," *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–13, 2018.
- [18] Q. Wang, D. Zhou, S. Yang, P. Li, and Q. Guan, "Privacy preserving computations over healthcare data," in *Proceedings of the 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*, pp. 635–64, SmartData, Atlanta, GA, USA, July 2019.
- [19] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of Medical Systems*, vol. 40, no. 10, pp. 218–8, 2016.
- [20] 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.
- [21] S. Gao, Q. Wang, Y. Liu, Z. Liu, W. Ou, and W. Han, "A Privacy-Preservation Scheme Based on Mobile Terminals in Internet Medical," *ResearchGate. Preprint*, 2021.
- [22] S. A. Chaudhry, A. Irshad, J. Nebhen et al., "An anonymous device to device access control based on secure certificate for internet of medical things systems," *Sustainable Cities and Society*, vol. 75, no. 1, Article ID 103322, 2021.
- [23] A. Arasan, R. Sadaiyandi, F. Al-Turjman, A. k. Rajasekaran, and K. S. Karuppuswamy, "Computationally efficient and secure anonymous authentication scheme for cloud users," *Personal and Ubiquitous Computing*, pp. 1–11, 2021.
- [24] M. Samaniego, R. Deters, and U Jamsrandorj, "Blockchain as a Service for IoT," in *Proceedings of the Blockchain as a service for IoT. in IEEE International*, pp. 433–436, Chengdu, China, December 2016.
- [25] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized BlockChain for IoT," in *Proceedings of the The Second IEEE/ACM Conference on Internet of Things Design and Implementation*, pp. 173–178, Pittsburgh, PA, USA, April 2017.
- [26] O. Alphand, M. Amoretti, T. Claeys, S. Dall'Asta, and F. Z. IoTChain, "A blockchain security architecture for the internet of things," in *Proceedings of the IEEE Wireless Communications and Networking Conference*, pp. 1–6, WCNC, Barcelona, Spain, April 2018.
- [27] F. Tao, D. Zhao, Y. Hu, and Z. Zhou, "Resource service composition and its optimal-selection based on particle swarm optimization in manufacturing grid system," *IEEE Transactions on Industrial Informatics*, vol. 4, no. 4, pp. 315–327, 2008.
- [28] Y. Y. Cao Shuya, "Chang Xiaolin, Lightweight secure authentication scheme using blockchain for RFID system in smart factory," *Cyberspace Security*, vol. 11, no. 9, p. 10, 2020.
- [29] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic Searchable Symmetric Encryption," in *Proceedings of the ACM Transactions on Internet Technology*, p. 965, Raleigh North Carolina USA, October 2012.
- [30] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable Symmetric encryption," in *Proceedings of the International Conference on Financial Cryptograph & Data Security*, pp. 258–274, Okinawa, Japan, April 2013.
- [31] D. Cash, J. Jaeger, S. Jarecki et al., "Dynamic searchable encryption in very-large databases: data structures and implementation," *Network & Distributed System Security Symposium*, 2014.
- [32] M. Naveed, M. Prabhakaran, and C. A. Gunter, "Dynamic searchable encryption via blind storage," in *Proceedings of the IEEE Symposium on Security & Privacy*, pp. 639–654, Berkeley, CA, USA, May 2014.
- [33] F. Hahn and F. Kerschbaum, "Searchable Encryption with Secure and Efficient Updates," in *Proceedings of the ACM Transactions on Internet Technology*, pp. 310–320, Raleigh North Carolina USA, October 2014.

Research Article

Healthcare Big Data Privacy Protection Model Based on Risk-Adaptive Access Control

Rong Jiang,^{1,2,3} Shanshan Han,^{1,2,3,4} Mingyue Shi,^{1,2,3,4} Tilei Gao ,⁴ and Xusheng Zhao^{1,2,3,4}

¹Institute of Intelligence Applications, Yunnan University of Finance and Economics, Kunming, China

²Key Laboratory of Service Computing and Safety Management of Yunnan Provincial Universities, Kunming, China

³Kunming Key Laboratory of Information Economy & Information Management, Kunming, China

⁴School of Information, Yunnan University of Finance and Economics, Kunming, China

Correspondence should be addressed to Tilei Gao; gtlei@ynufe.edu.cn

Received 20 December 2021; Revised 18 February 2022; Accepted 19 February 2022; Published 15 March 2022

Academic Editor: Honghao Gao

Copyright © 2022 Rong 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.

Edge computing is playing an increasingly important role in the field of health care. Edge computing provides high-quality personalized services to patients based on user and device data information. However, edge nodes will collect a large amount of sensitive patient information, and patients will also bear the risk of privacy disclosure while enjoying personalized services. How to reduce the risk of privacy disclosure while ensuring that patients enjoy personalized services brought by edge computing is the research content of this paper. In this paper, the work flow and management mode of Hospital Information System (HIS) are investigated on the spot, and the risk-adaptive access control model based on entropy is established. First, we use *International Classification of Diseases, Tenth Revision* (ICD-10) to mark the information resources accessed by users and use information entropy to measure the correlation “ α ” between medical information accessed by users and work tasks. Finally, we analyze the relationship between correlation “ α ” and risk through an example. The results show that users with high correlation α have low risk of access behavior, and users with low risk have high correlation α of access information resources and work goals. This discovery can help managers predict users’ access behavior in the Big Data environment, so as to dynamically formulate access control policies according to the actual access situation of users and then realize the privacy protection of medical big health data.

1. Introduction

Edge computing is used to extend cloud computing to the edge of the Web. Specifically, edge computing is a new distributed computing mode, in which multiple edge nodes located between cloud servers and local users cooperate to complete outsourced storage and computing tasks [1]. Edge computing is increasingly used in various areas of people’s life, including smart home, healthcare, industrial production, and media entertainment [2]. Especially in healthcare, medical informatization based on edge computing technology can greatly improve medical efficiency. At present, the research of edge computing combined with medical scenarios mainly focuses on the design of network communication protocol and routing algorithm but neglects the research of information security and privacy protection in

medical scenarios. As a result, the development of current medical application scenarios based on edge computing technology is blocked. As medical Big Data contains a wealth of patient-sensitive information, the collection, transmission, use, and sharing of data bring great security risks to people.

Medical Big Data is the core asset of the medical field. However, most hospitals lack special privacy protection measures, and the medical industry has become one of the most serious areas of privacy leakage [3]. In 2016, 10 industries with serious data leakage were released in the Internet Security Threat Report. The medical industry ranked first, with 116 data leakage incidents, and the incident incidence rate was 37.2%. The proportion of data leakage is much higher than the second-ranked retail industry. In 2017, 47 GB of medical information was leaked by Amazon server

and the private information of 150,000 patients was exposed, which brought great negative impact to both the society and individuals. Therefore, it is very necessary to study the security and privacy issues in the medical industry.

At present, the research on data security and privacy protection technology mainly includes access control, data anonymization, data encryption, differential privacy protection, digital watermarking, and so on. Among them, access control technology has become a hotspot of current research, but it mainly targets at the field of operating system, and there are not many researches in the information field, especially the research on the security and privacy protection of medical Big Data. Inspired by previous studies [4–6], this paper proposes a medical Big Data privacy protection model based on risk-adaptive access control. The main contributions are as follows:

- (i) We build a set of diagnostic codes that users can access under specific work goals. Based on the ICD-10 diagnostic codes, we cluster the set of diagnostic codes that allow users to access under the target disease.
- (ii) We design a method to evaluate user access behavior. According to the user's historical access data, we use information entropy to evaluate the risk of users' current request access behavior.
- (iii) We propose a new method for calculating risk benchmarks. Based on the user's information entropy, we use *K*-means clustering to calculate the baseline value of risk assessment.

The rest of the paper is organized as follows. Section 2 introduces the related work about medical data privacy protection. Section 3 specifically introduces the construction of the medical Big Data privacy protection model. Section 4 is the experimental simulation. Section 5 summarizes the paper and discusses directions of future work.

2. Related Work

Although edge computing improves medical efficiency, medical data may leak and cause serious damage to patients in the process of transmission and access. Therefore, the security and privacy protection of mobile medical information are particularly important. It is urgent to establish privacy security guarantee mechanism and monitoring mechanism to ensure the safe reading and access of medical data. The current research on Big Data security and privacy protection mainly adopts technologies based on cryptography, differential privacy, anonymization, identity authentication, and so on. Gao et al. [7] proposed the Sensitive Data Timed I/O Automata (SDTIOA) model, which was an automatic transformation method for modeling the timed privacy requirements of IoT service compositions. Gao et al. [7] used the SDTIOA model to verify whether the service combination meets user privacy requirements, which can effectively prevent the leakage of user privacy information. In literature [8–19], scholars used differential privacy technology to establish some privacy protection models for

medical Big Data security issues. Zhang et al. [20] used encryption technology to study the security of medical data according to the sequence of events; He et al. [21] protected medical information through anonymization and identity authentication. In order to protect the privacy of medical data, Li and Zhang [22] chose to desensitize and anonymize their EMR data before authorizing a third party to use it. Chen et al. [23] proposed an electronic medical record system based on blockchain joint proxy re-encryption, which ensured the security of medical data access and realized fine-grained access to data through attribute-based access control. Xanthidis and Xanthidou [24] designed an error-correction code hash function and constructed a privacy-preserving anonymization algorithm, which to some extent controlled users' access rights and ensured the safe sharing of data between doctors and patients. Some scholars used VPN, SSL and other technologies to control access to medical data, so as to protect the security of medical data. Malasri and Wang [25] proposed SNAP (sensor network for assessment of patients) scheme to solve the safety problems of wireless sensor monitoring network. In Sun et al.'s study [26], patients' physiological signals (such as blood pressure and heart rate) were used to generate symmetric keys with patient characteristics, so as to protect the data security of patients. However, these schemes are time-consuming and not practical for medical scenarios requiring high delay.

In recent years, scholars at home and abroad have also carried out research on risk-based access control technology. In Jason et al.'s [27], the author first put forward the concept of risk and gave the primary colors and suggestions related to risk quantification. Dankar and Badji [28] proposed a risk-aware information disclosure model for biomedical data. Model evaluated the risk posed by a data request using all contextual information surrounding the request and feed it into an access control decision module. Ni et al. [29] and Cheng et al. [30] presented specific risk quantification methods according to the safety marks and sensitivity of the subject and object. In addition, a role-based access control (RBAC) model based on risk perception was proposed, which mainly evaluated the trust of users, the relationship between users and roles, and the relationship between roles and permissions. Diep et al. [31] and Sharma et al. [32] mainly conducted risk assessment on the user's access behavior, and the evaluation basis was whether the user's access behavior will cause loss of the integrity, availability, and confidentiality of the information. Ding et al. [33] proposed a privacy-preserving multiparticipant risk-adaptive access control model. This model proposed a privacy quantification method for dynamically accessing data. Furthermore, a multiparticipant access control evolutionary game model was constructed based on evolutionary game. Yang et al. [34] designed a flexible access control mechanism based on keyword matching, which enabled data to be shared in a fine-grained access control mode, preventing privacy disclosure while not affecting data usage. Line et al. [35] summarized a variety of access control strategies and analyzed risk assessment criteria according to the actual situation of hospitals, and suggested that future work should

focus on expanding access control strategies based on location and situation; Wang and Jin [36] evaluated users' access behaviors based on their historical access information. The more chaotic the distribution of users' access behaviors, the greater the risks that users may cause. Shaikh et al. [37] proposed a risk-based decision access control system, which took into account not only the historical access behavior of users but also the recent access behavior of users, and the system was suitable for dynamic and complex environments like the medical industry. Choi et al. [38] constructed a context-aware medical information risk access control framework, which mainly judged whether to grant users access permissions based on permission files, user access logs, context information, etc.; Hui et al. [39] improved on the basis of literature [36] to prevent doctors from stealing patients' private information by forging work goals. Zhang [40] and Jiang et al. [41] mainly studied the privacy disclosure of medical Big Data in the cloud environment but focused on the analysis of the risk indicator system that may affect privacy disclosure, without involving specific risk quantification model. Few previous studies [42–44] established a risk assessment model for medical Big Data with the help of fuzzy theory.

A comprehensive analysis of relevant research shows that some scholars are currently doing research on the intersection of information and medicine and have made good achievements. The methods mainly focus on cryptography, anonymity, differential privacy, and so on, and some are analyzed from the perspective of management. Although there are also studies from the perspective of risk and access control, they are still in the initial stage of exploration and have not formed a relatively mature system model framework, especially for the research on the privacy protection of medical Big Data based on risk access control is extremely scarce.

3. Medical Big Data Privacy Protection Model

Workflow refers to the automation of part or whole of a business process in the computer application environment. It is an abstract and general description of the business rules between the workflow and each operation step [45]. Before studying the privacy protection of medical Big Data, we should be clear about the user's workflow, authorization management mode and information use process in HIS, otherwise it will be meaningless to discuss privacy protection apart from the actual situation. Therefore, Section 3.1 first investigates and sorts out the workflow and authorization management mode in HIS, and then establishes the access control model according to the actual situation.

3.1. Workflow and Authority Management Mode in HIS. Through the field investigation of HIS in some hospitals in Kunming, we found that the system generally includes four main modules: outpatient workflow, inpatient workflow, permission allocation, and drug storehouse, while the first three modules are mainly involved in the study of medical Big Data privacy issues. In the outpatient workflow, the outpatient

cashier is responsible for logging in the system to fill in the patient's registration information, outpatient fees, and refund processing; the outpatient doctor selects the department responsible for issuing medical advice. In the inpatient workflow, the inpatient nurse is responsible for the patient's admission registration, prepayment entry, patient admission, filling in the admission diagnosis information, and patient's basic health information; the resident is responsible for prescribing short-term or long-term medical advice to the corresponding patient, which is reviewed and implemented by the resident nurse.

In terms of authority allocation, most hospitals adopt role-based authorization management mode. The system administrator first adds the staff's basic information in the basic information bar of the personnel management module. The hospital mainly includes outpatient department, inpatient department, drug system, clinical department, medical technology department, hospital leader, and so on. The departments are divided into different offices and wards. When adding the staff's basic information, the system will automatically generate the doctor's code or the employee number, and the code is needed in the permission allocation. Then the administrator fills in the employee's department, section, position, title, and other relevant information in the personnel management column, and assigns the account number and password of the system to the employee. The account type includes financial personnel, outpatient financial account, outpatient doctor, system user, medical technology department, hospital office, inpatient care, resident doctor, and so on. User can view the login records of each account type. Finally, the administrator assigns roles to each user. The role management interface includes Administrators, Guests, Public, office staff, financial staff, decision analysis, developer, outpatient registration, outpatient charge, outpatient pharmacy, outpatient doctor, outpatient doctor station, personnel management, data center, resident nurse, resident doctor, medical technology department, and so on. The administrator grants different access modules to different roles. Therefore, the whole process realizes the assignment relationship between user-role-permission in HIS.

From the aforementioned analysis, it can be seen that doctors in different jobs and roles have different work tasks and access authority sets. In general, after a patient is discharged from hospital, the patient's paper medical record and medical information will be sealed by the medical record room, and junior professional title doctors can only use their own employee number and password to query the patient's recent medical information. However, in order not to affect the normal work of doctors, some highly qualified doctors or experts will be granted extremely high authority, they can access patient information not only for the whole group, but even for the entire district. In addition, the amount of information that doctors need to complete their respective tasks will vary depending on the patient's medical history, the number of patients, and other factors. For example, when a patient is diagnosed with cancer, the doctor has access to a lot of sensitive cancer-related information. It is difficult to adapt to the actual situation of the medical environment to evaluate the doctor's access risk by the amount

of doctor's access information or the sensitivity of doctor's access data. This paper is interested in whether the risks caused by users' access behavior are worth it, that is, whether to grant access to users is determined by measuring the relationship between risks and benefits.

3.2. Entropy-Based Risk-Adaptive Access Control Model. Entropy characterizes the chaos degree of random variable distribution. The more chaotic the distribution is, the greater the entropy is. The essence of entropy is to measure the amount of information. Information entropy, also known as Shannon entropy, is usually used to describe the average amount of information brought by the whole random distribution, and has more statistical characteristics. Since entropy is calculated based on sample data, it is also called empirical entropy. The relevant formula is defined as follows.

Definition 1. Assuming that X is a random variable and the random distribution of X is $P(X)$, the self-information $I(x)$ of the random variable x ($x \in X$) and the information entropy $H(X)$ of X are

$$\begin{aligned} I(x) &= -\log P(x), \\ H(X) &= \sum_{x \in X} P(x) \times I(x). \end{aligned} \quad (1)$$

According to Definition 1, entropy represents the chaos degree of random variable distribution, which can be used to formally represent the instability of user access behavior. Therefore, the entropy-based risk-adaptive access control model aims to quantify users' access behaviors by means of entropy. In HIS, each user will have a corresponding work task, and access the patient's information resources according to the work task. We believe that if the information resources accessed by the user are not relevant to the work task, or the correlation is very low, the user will have the risk and possibility of snooping the patient information. A user's access behavior is set to a six-tuple:

$$(U, R, T, P, M, \alpha), \quad (2)$$

where U is the set of all users, R represents the set of roles, T represents the set of tasks, P represents the set of permissions, M is the set of medical records, and α is the correlation between medical records and work tasks. The relationship between factors is as follows: the same user can be granted different roles, and the same role can also be assigned to different users. Users and roles are in a many-to-many relationship. In Figure 1, User1 can be granted Role1, Role2, and Role4; Role1 can be assigned to both User1 and User2. Tasks are assigned to users according to roles, and roles map users to corresponding tasks. A role can be assigned multiple tasks, and a task can also be assigned to multiple roles, tasks, and roles are also in a many-to-many relationship. In Figure 1, Role3 can access the medical information resources required by Task2 and Task4, and the medical information resources provided for Task2 can be accessed by Role2 and Role3. Tasks are assigned to users through roles to perform their permissions. The specific structure and relationship are shown in Figure 1.

The following will analyze in detail how to evaluate the user's access behavior. As we can be seen from the previous analysis, the correlation between the user's work task and the medical records accessed by the user is an important basis for evaluating the user's access behavior. Therefore, we should first clarify two questions before evaluating users' access behavior: (a) How to mark the medical information accessed by users and (b) How to quantify the risk value of known users' historical access behavior. The rest of Section 3.2 will focus on the aforementioned two aspects to analyze the user's access behavior.

3.2.1. Marking Medical Information. Most hospitals use the ICD-10 code to classify and label the diagnosis results of patients. ICD-10 is the 10th revision of the International Statistical Classification of Diseases and Health-related Problems. The disease name corresponds to a single code, and in turn, the disease name can be found through the disease classification code, and then the medical staff can extract the required medical record data. Generally, it is "one disease one code," which can provide a unified classification standard for medical record management, health statistics, medical information utilization, and scientific research.

Although there is a one-to-one relationship between disease name and coding, in practical problems, in order to fully understand the disease, it is normal for users to access some medical record information related to the disease. Therefore, according to the characteristics of ICD-10 diagnostic code, the paper reasonably summarizes the medical records of similar diseases through clustering. The 6-digit ICD-10 is used in China's medical system. For example, B18.202, the first three digits are the mixed codes of letters and numbers, which are the category codes with practical significance. The fourth digit or letter code is the subclassification of the first three digits, and the more similar diseases are, the more similar their ICD-10 codes are. Therefore, when the first letter is the same, the second and third digits of the ICD-10 diagnostic code are taken out, and when the second and third digits of the ICD-10 code are the same, they are grouped into one category.

Assume that the diagnostic code of a target disease is B18.902, and the set of diagnostic codes after clustering is as follows: $S = \{B18.000, B18.001, B18.002, B18.003, B18.103 + N08.0^*, B18.202, B18.204, B18.902, B18.904 + N08.0^*\}$. When the medical information records accessed by a user under a specific work task belong to set S , it indicates that the user's access behavior is within the scope of the work target. However, when the medical information records accessed by users under a specific work task do not belong to set S , we need to evaluate the instability of their access behavior and specifically quantify the correlation α . Therefore, it is theoretically feasible to mark medical information accessed by users through diagnostic codes.

3.2.2. Risk Quantification. We define the deviation degree between users' access to medical information and their work tasks as risks. The greater the deviation degree is, the greater

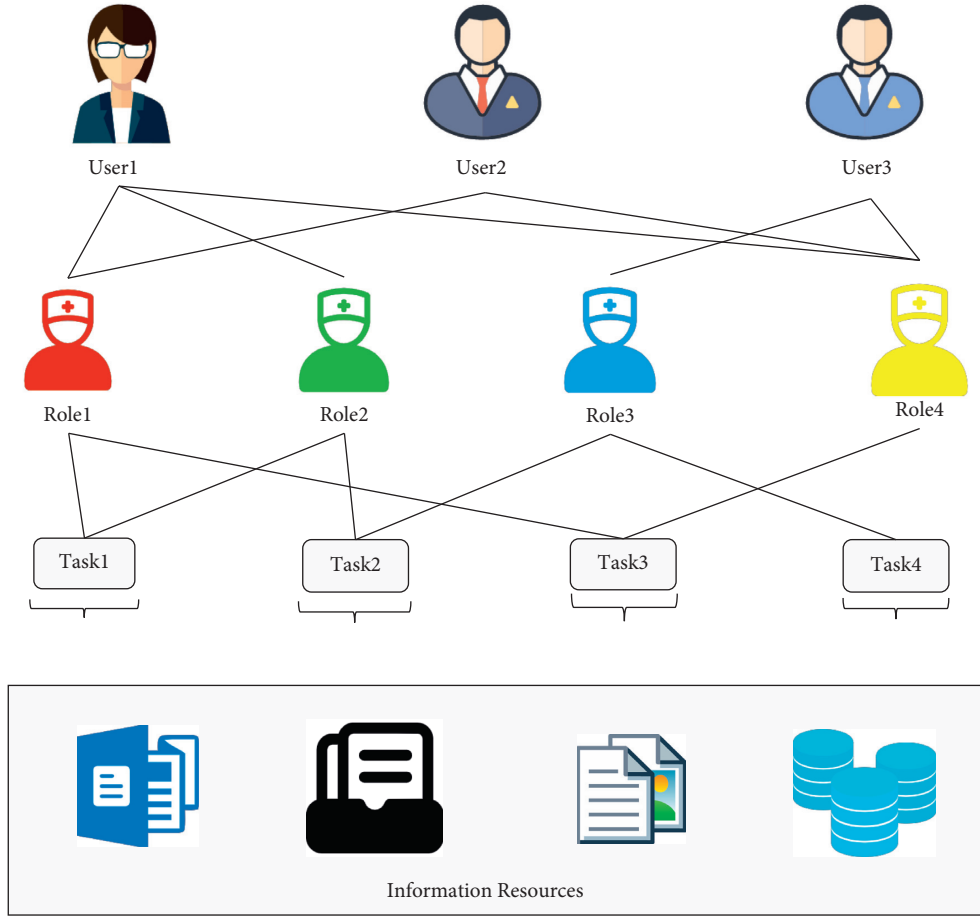


FIGURE 1: Diagrams of relationships among users, roles, tasks, and information resources.

the possibility of privacy snooping. When the risk reaches a certain level, users' access behavior should be controlled. We use entropy to quantify the user's access behavior. Before calculating the user's access behavior entropy, we need to define the probability P of the user's access to the medical information record set m_k .

Let the patient set $D = \{d_1, d_2, \dots, d_{I_d}\}$ received by user u_i within a period of time, and the medical record set accessed by use u_i for patient d_j is $M = \{m_1, m_2, \dots, m_{I_m}\}$, then the probability of user accessing medical record set m_k is as follows:

$$P(m_k|u_i, d_j) = \frac{\|f(m_k)\|}{\sum_{m_k \in M} \|f(m_k)\|}, \quad (3)$$

where I_d represents the number of patients, I_m represents the number of elements in the set M , $d_j \in D$, $m_k \subseteq M$ is a set of diagnostic codes for a certain disease in the medical system, and each element in M represents a set of diagnostic codes, $\|f(m_k)\|$ represents the number of users access to the set m_k . Therefore, the information entropy of the medical information accessed by the user u_i for the patient d_j under a specific task within a period of time is

$$H(u_i, d_j) = - \sum_{k=1}^{I_m} P(m_k|u_i, d_j) \times \log P(m_k|u_i, d_j). \quad (4)$$

Let $\{H(u_i, d_1), H(u_i, d_2), \dots, H(u_i, d_{I_d})\}$ is the entropy of user u_i access to medical information resources when user u_i treats all patients for a specific task within a certain period of time. By calculating the mean value of $\{H(u_i, d_1), H(u_i, d_2), \dots, H(u_i, d_{I_d})\}$, we can get the entropy $H(u_i)$ of user u_i accessing medical information resources for specific work tasks in a certain period of time.

$$H(u_i) = \frac{\sum_{j=1}^{I_d} H(u_i, d_j)}{I_d}. \quad (5)$$

The higher the entropy $H(u_i)$ of the user's access to medical information, the more unstable the user's access behavior, the greater the deviation degree between the medical records accessed by the user and their work tasks, the smaller the correlation, and the greater the possibility of disclosing privacy information. Therefore, the entropy $H(u_i)$ of user access to medical information is inversely proportional to the correlation parameter α , which can be expressed as follows:

$$\alpha = 1 - H(u_i). \quad (6)$$

To sum up, we can get the entropy $H(u_1), H(u_2), \dots, H(u_{I_u})$ of all users accessing medical information in the HIS within the same time period, where I_u represents the number of users in the HIS. Then, we take the entropy of all users' access to medical information as the input of K -means clustering, and finally obtained two clustering centers (x_1, y_1) and (x_2, y_2) [46]. We averaged the ordinate of the two clustering centers and used them as the benchmark π for risk assessment. Therefore, the access behavior risk of each user u_i is defined as

$$\text{Risk} = \max\{0, H(u_i) - \pi\}. \quad (7)$$

4. Case Analysis

We take the inpatient department as an example to analyze the effectiveness of the model in practical applications. That is, whether the model can evaluate the user's access behavior risk based on the actual situation of the hospital and the existing data resources. According to the previous analysis, when the information resources accessed by users are not related to the work objectives or the correlation α is low, the user will have the risk of disclosing the patient's privacy information. Therefore, the validity of the model can be tested by studying correlation α and risk. When users with high correlation α have low risk of access behavior, and users with low risk have high correlation α between access information resources and work objectives, the model in the paper can be considered to be effective.

According to the requirements of this paper, some medical data have been obtained from the Oracle database of a third-class hospital in Kunming, including doctor code table `Dmb_ysdm`, hospital department code table `Dmb_ksdm`, patient basic information table `Zy_hzjbxx`, doctor's order table `Zy_yz`, and patient inpatient information table `Zy_hzzyxx`. It is worth noting that each table in the hospital has more than 200 fields at most. The table shown in this paper is a regenerated table after extracting fields from multiple tables according to the needs of the model. When a doctor access electronic medical records, an access log will be generated, including the Doctor code, Patient's identification number, Medical record no., and access time. When users view the log content, they need to retrieve `Dmb_ysdm` and `Dmb_ksdm`. Under a specific work task, the doctor needs to obtain the basic information of the patient (Patient's condition, Clinic diagnosis, Admission diagnosis, ICD-10 code, medical record no., etc.) according to the patient's medical record number, and then needs to search `Zy_hzjbxx`, `Zy_yz`, and `Zy_hzzyxx`. The relevant information is shown in Tables 1 to 5.

As medical institutions prohibit public access to data, this paper presents only a part of patients' data in the basic patient information table `Zy_hzjbxx`, as shown in Figure 2.

According to Section 3.1, each user in HIS has a corresponding role and access module, and the user's access record can be viewed under the corresponding role,

including doctor code, access content, access time and access frequency. In addition, by retrieving the doctor code, you can also query the user's role, department, job title, and other information. We combine `Dmb_ysdm`, `Dmb_ksdm`, `Zy_hzjbxx`, `Zy_yz`, and `Zy_hzzyxx` to get a user's work goals and access information resources within a period of time. In the experiment, we randomly selected 30 users from the inpatient department of HIS, and tracked and marked their access within half a year. The marking content mainly includes the patient information received by the user in the past half a year, especially the patient's ICD-10 diagnostic code and the medical information record set accessed by the user for the patient. Table 6 shows the medical information accessed by the resident u_1 when treating the patient with ID 4151097:

Combining equations (3) and (4), we can calculate that the information entropy of the user accessing medical information for the patient's condition within half a year is 0.86. In the same way, according to equation (5), we can get the entropy $H(u_1)$ of the user accessing medical information for a specific task (patient's diagnostic code is A19.900) within half a year, and the entropy $\{H(u_2), H(u_3), \dots, H(u_{30})\}$ of all users accessing medical information within the same period. The specific value of entropy of user access to medical information resources is shown in Figure 3. The entropy in Figure 3 is prepared for us to calculate the risk benchmark and assess the risk of user access behavior. We take the entropy of all users accessing medical information resources as the input data set for K -means clustering. Finally, we get two clustering centers (x_1, y_1) and (x_2, y_2) , and the results are shown in Figure 4.

As we can be seen from Figure 3, in the same time period (the time set is half a year in the paper), different users have different access behavior risks for specific work tasks. This experiment proves that it is feasible for us to use the information entropy method to evaluate user access behavior's risk. It can be seen from Figure 4 that the entropy of 30 users accessing medical information is divided into two categories. The cluster center y_1 of the first type is 0.45, and the cluster center y_2 of the second type is 0.60, which are marked with red dots in the figure. Therefore, the risk benchmark $\pi = 0.525$ is obtained according to y_1 and y_2 . The extent to which the user's access behavior deviates from the risk baseline is shown in Figure 5. Where we set the risk value of users whose access entropy is below the risk baseline to be 0 and default to legitimate users, while the risk value of the user whose access entropy is above the risk baseline can be calculated according to equation (7), as shown in Figure 6.

From Figure 6, it is easy to determine whether to grant access to the user. As we can be seen from Figure 6, users whose access entropy is lower than the risk baseline are considered to be risk-free, and the model grants the user access rights. If the risk value is not 0, that is, the user's current access request may cause privacy security problems, the user's access request is rejected. Finally, in order to verify the validity of the model in this paper, we analyzed the change relationship between correlation α and risk, as shown in Figure 7. The results show that users with high correlation α have low risk of access behavior, and users with low risk

TABLE 1: Dmb_ysdm.

Column	Name	Type	Remark
Ysdm	Doctor code	CHAR(3)	
Ysxm	Doctor name	CHAR(10)	Get the doctor's department from the ksdm field in mb_ksdm
Yszc	Doctor title	CHAR(12)	
Ksdm	Subordinate department	CHAR(2)	

TABLE 2: Dmb_ksdm.

Column	Name	Type	Remark
Ksdm	Department code	CHAR(3)	
Ksmc	Department name	CHAR(10)	"1" is the inpatient department
Zybz	Whether in the hospital	CHAR(12)	

TABLE 3: Zy_hzjbxx.

Column	Name	Type	Remark
Bah	Patient's identification number	CHAR(8)	
Hzxm	Patient name	CHAR(10)	
Blh	Medical record no.	CHAR(10)	
Xb	Gender	CHAR(2)	
Sfzh	ID	CHAR(21)	
Mzzd	Clinic diagnosis	CHAR(36)	If there is no special description, the default value is used
Rydz	Admitting diagnosis	CHAR(36)	
Kdys	Billing doctor	CHAR(3)	
Fzys	Responsibility doctor	CHAR(3)	
Bq	Patient's condition	CHAR(10)	
Hljb	Nursing degree	CHAR(10)	
Gcys	Tube bed doctor	CHAR(3)	

TABLE 4: Zy_yz.

Column	Name	Type	Remark
Brid	Patient Id	CHAR (10)	
Zdsj	Diagnosis time	CHAR(10)	
Zdm	ICD-10 code (diagnosis code)	CHAR(10)	"1" is the inpatient department
Zyh	Admission number	CHAR(3)	
Ksmc	Department name	CHAR(10)	
Zybz	Whether in the hospital	CHAR(12)	

TABLE 5: Zy_hzzyxx.

Column	Name	Type	Remark
Bah	Patient's identification number	CHAR (8)	
Hzxm	Patient name	CHAR(10)	
Blh	Medical record no.	CHAR(10)	
Ryks	Admission department	CHAR(2)	
Zzys	Attending doctor	CHAR(3)	If there is no special description, the default value is used
Gcys	Tube bed doctor	CHAR(3)	
Ksmc	Admission bed	CHAR(12)	
Zybz	Whether in the hospital	CHAR(12)	
Xzks	Current department	CHAR(2)	
Xzwc	Current bed number	CHAR(12)	

Bah	Hzxm	Xb	Blh	Sfzh	Mzzd	Kdys
10065799	Jan* Ma	1	2018030204	****	Cerebral Infarction	1475
10214405	Ming* Hua	2	2018031101	****	Malignant Tumor	1493
10223465	Jun* Yang	2	2018012406	53212419551101****	Heart Disease	6165
10223467	Xiang* Xie	2	2018091603	53010319450416****	Cerebrovascular Diseases	5910
10223468	Fa* Li	1	2018021402	53012219641014****	Gastroenteritis	1410
10223471	Zheng* Chen	1	2018072408	53038120070601****	Influenza and Pneumonia	1309
10223472	Chun* Pu	2	2018111607	53012219930907****	Severe Hepatitis	1058
10223477	Ye* Du	2	2018122303	53010319910101****	Emphysema	1205
10223478	Xiao* Ji	2	2018072504	****	Diabetes	1205
10224481	Fen* Wu	2	2018072107	53032819660318****	Cirrhosis	1073
10177001	Min* Huang	2	2018030206	33032619921002****	Fatty Liver	1205
10224485	Ben* Wang	1	2018040207	53012219710724****	Benign Brain Tumor	1345
10224486	Xue* Shen	1	2018061301	53020041120603****	Acute Myocardial Infarction	6165
10224487	Chuan* Wang	1	2018051802	53212319850308****	Encephalitis	6344
10224488	Qing* Huang	1	2018072106	53011119371108****	Parkinson	1399
10222228	Yan* Li	1	2018051705	53012269050920****	Stroke	1347
10222059	Pei* Kong	2	2018042302	53222419480515****	Mammary Cancer	6273
10222062	Yu* Duan	1	2018060806	53272519640910****	Mental Disease	5699
10222063	Sheng* Hou	1	2018090203	53011119570802****	Cerebral Infarction	1160
10222064	Xiu* Luo	2	2018082203	53011119450625****	Myocarditis	1160
10222065	Zheng* Cui	1	2018062104	53011119470426****	Diabetes	6359
10222066	Su* Zhang	2	2018052505	53011219401120****	Primary Pulmonary Hypertension	1464
10222067	Zhi* Ma	2	2018071906	53011260080905****	Systemic Lupus Erythematosus	1301
10222068	Chao* Li	1	2018071104	53012819560722****	Acute Myocardial Infarction	1473
10222069	Tai* Li	1	2018082302	53011119630509****	Cholecystitis	1247
10222080	Nan* Li	2	2018052701	****	Cerebral Infarction	1070
10222085	Xiu* Huang	2	2018032403	42010619290424****	Hypertension	1493
10222088	Ya* Liu	1	2018082701	53010219570115****	Hepatocellular Carcinoma	1345
10222089	Shu* Li	1	2018110206	53011119570313****	Tuberculosis	1522
10222090	Xiao* Li	2	20180042203	53252619690807****	Mammary Cancer	1270
10224008	Jun* Zhao	1	2018061406	51072220041031****	Uremia	1234

FIGURE 2: Patients' basic information in Zy_hzjbxx.

TABLE 6: User access information table.

Patient Id	Diagnostic code	Doctor code	Medical records within the scope of the user's work goals	Medical record information actually accessed by the user	Access frequency
4151097	A19.900	507	A19.000	A19.000	1
			A19.001	A19.100	1
			A19.100	A19.200	1
			A19.200	A19.800	1
			A19.800	A19.900	2
			A19.801	A19.902	1
			A19.802	B24.x00	2
			A19.803		
			A19.900	A20.900	3
			A19.901		
			A19.902		

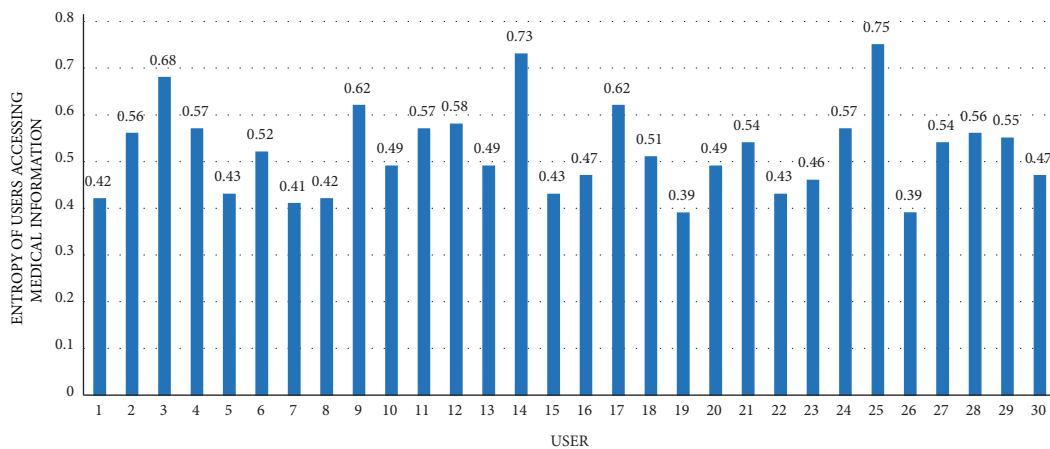


FIGURE 3: Entropy of user access to medical information resources.

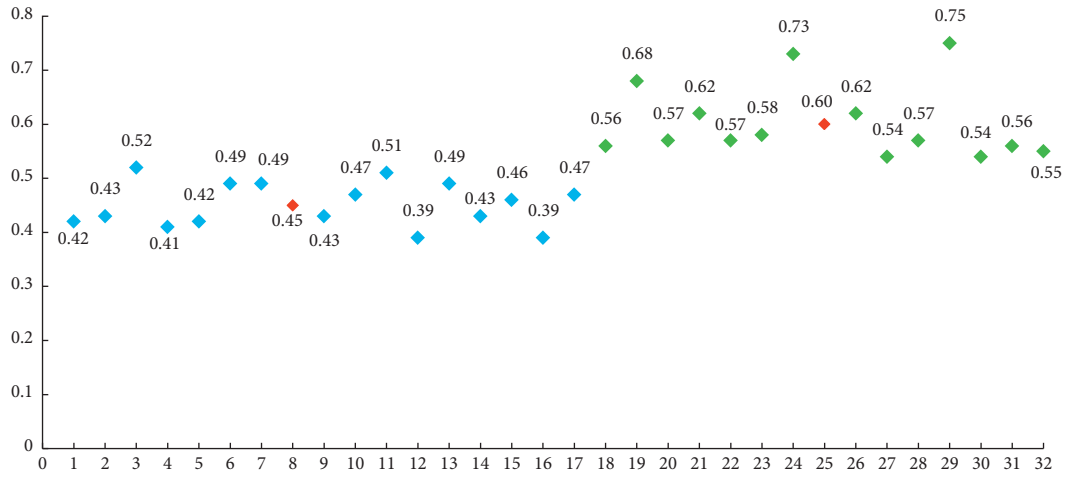


FIGURE 4: K-means clustering results.

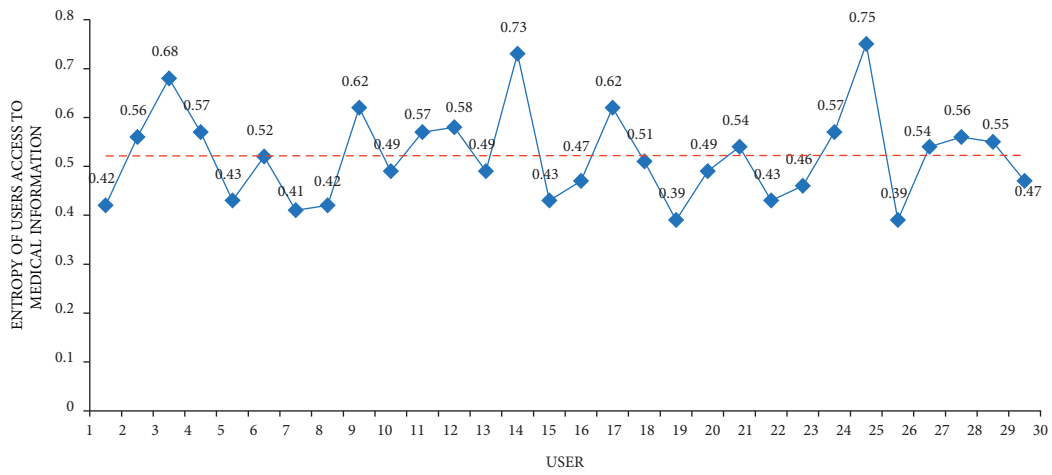


FIGURE 5: The degree to which users' access behavior deviates from the risk baseline.

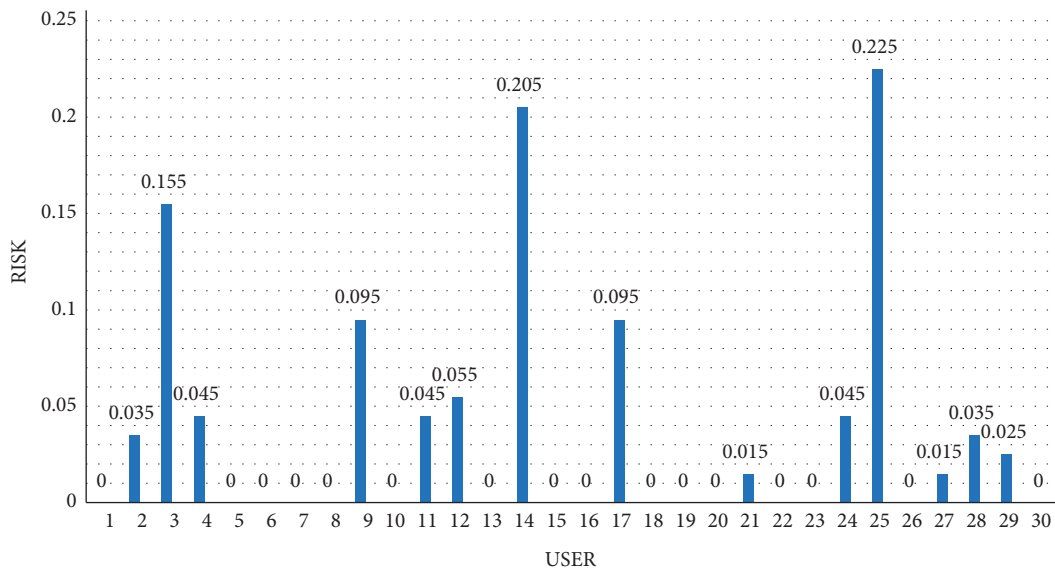


FIGURE 6: User access behavior risk.

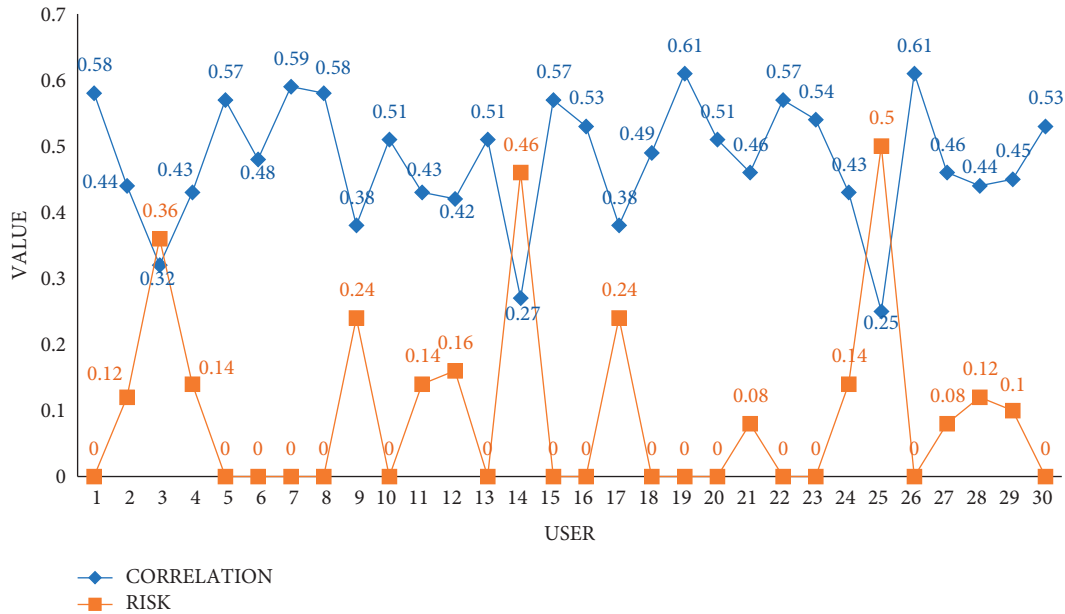


FIGURE 7: The relationship between correlation α and risk.

have high correlation α between access information resources and work goals. Therefore, managers can predict the risks of users' access behaviors based on the correlation between the information resources accessed by users and the work objectives. In this way, administrators can dynamically formulate access control policies based on users' access conditions.

5. Conclusion

In this paper, we sort out the current hospital workflow and management mode and establish an access control model based on risk adaptive. By analyzing the correlation between information resources accessed by users and work objectives, we assess the risk of patient information disclosure caused by users' access behavior. The experimental results show that hospital administrators can predict the risk of privacy disclosure caused by users' access behavior, this discovery helps them to formulate scientific access control strategies. However, since the HISs of most hospitals are different at present, the privacy-preserving model proposed in this paper cannot be fully adapted to all hospitals. In the future, we will study a more compatible access control privacy protection model, provide new ideas for the hospital's resource management model, and promote the overall progress of the hospital's comprehensive management capabilities.

Data Availability

The original data of this article have been signed in a confidentiality agreement with the hospital and are temporarily unavailable, but the processed data (data used to support the research in this article) can be partially shared publicly and submitted with the manuscript.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (grant nos. 71972165 and 61763048) and the Science and Technology Foundation of Yunnan Province (grant no. 202001AS070031).

References

- [1] Y. Yin, Z. Cao, Y. Xu, H. Gao, R. Li, and Z. Mai, "QoS prediction for service recommendation with features learning in mobile edge computing environment," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 4, pp. 1136–1145, 2020.
- [2] P. Zhang, Y. Zhang, H. Dong, and H. Jin, "Mobility and dependence-aware QoS monitoring in mobile edge computing," *IEEE Transactions on Cloud Computing*, vol. 9, 2021.
- [3] X. Jin, *Big Data in Health Care*, People's Medical Publishing House, USA, 2018.
- [4] R. Jiang, Y. Xin, Z. Chen, and Y. Zhang, "A medical big data access control model based on fuzzy trust prediction and regression analysis," *Applied Soft Computing*, vol. 117, Article ID 108423, 2022.
- [5] Y. Xu, Y. Wu, H. Gao, S. Song, Y. Yin, and X. Xiao, "Collaborative APIs recommendation for artificial intelligence of things with information fusion," *Future Generation Computer Systems*, vol. 125, pp. 471–479, 2021.
- [6] Y. Huang, H. Xu, H. Gao, X. Ma, and W. Hussain, "SSUR: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 670–681, 2021.
- [7] H. Gao, Y. Zhang, H. Miao, R. J. D. Barroso, and X. Yang, "SDTIOA: modeling the timed privacy requirements of iot

- service composition: a user interaction perspective for automatic transformation from BPEL to timed automata,” *Mobile Networks and Applications*, vol. 26, pp. 1–26, 2021.
- [8] C. Lin, Z. Song, H. Song, Y. Zhou, Y. Wang, and G. Wu, “Differential privacy preserving in big data analytics for connected health,” *Journal of Medical Systems*, vol. 40, no. 4, 2016.
 - [9] C. Lin, P. Wang, H. Song, Y. Zhou, Y. Wang, and G. Wu, “A differential privacy protection scheme for sensitive big data in body sensor networks,” *Annals of Telecommunications*, vol. 71, no. 9, pp. 465–475, 2016.
 - [10] J. L. Raisaro, G. Choi, S. Pradervand et al., “Protecting privacy and security of genomic data in i2b2 with Homomorphic Encryption and Differential Privacy,” *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 15, no. 5, pp. 1413–1426, 2017.
 - [11] X. Wu, *Privacy Protection and its Key Technologies in Big Data*, Nanjing University, Nanjing, China, 2017.
 - [12] Y. Bai, “Data Base Technique, Application of differential privacy protection in medical big data,” *Electronic Technology & Software Engineering*, vol. 24, pp. 196–197, 2017.
 - [13] M. Sung, D. Cha, and Y. Park, “Local differential privacy in the medical domain to protect sensitive information: algorithm development and real-world validation,” *JMIR Medical Informatics*, vol. 9, no. 11, Article ID e26914, 2021.
 - [14] L. Zhang, X. Zhu, J. Ma, Z. Ma, and D. Yuan, “Medical privacy-preserving service recommendation,” in *Proceedings of the ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, Dublin, Ireland, June 2020.
 - [15] D. R. Harris, “Leveraging differential privacy in geospatial analyses of standardized healthcare data,” in *Proceedings of the IEEE International Conference on Big Data (Big Data)*, pp. 3119–3122, Atlanta, GA, USA, December 2020.
 - [16] Y. Hu, L. Ge, G. Zhang, and D. Qin, “Research on differential privacy for medical health big data processing,” in *Proceedings of the 20th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, pp. 140–145, Gold Coast, QLD, Australia, December 2019.
 - [17] A. M. Olawoyin, C. K. Leung, and R. Choudhury, “Privacy-preserving spatio-temporal patient data publishing,” in *Proceedings of the Database and Expert Systems Applications*, pp. 407–416, Bratislava, Czech Republic, September 2020.
 - [18] J. W. Kim, B. Jang, and H. Yoo, “Privacy-preserving aggregation of personal health data streams,” *PLoS One*, vol. 13, no. 11, Article ID e0207639, 2018.
 - [19] Z. Lv and F. Piccialli, “The security of medical data on internet based on differential privacy technology,” *ACM Transactions on Internet Technology*, vol. 21, no. 3, pp. 1–18, 2021.
 - [20] J. Zhang, “Research on security system of healthcare big data based on cryptographic technique,” *Journal of Information Security Research*, vol. 3, no. 7, 2017.
 - [21] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, “Anonymous authentication for wireless body area networks with provable security,” *IEEE Systems Journal*, vol. 11, no. 4, pp. 2590–2601, 2016.
 - [22] Z. Li and L. Zhang, “An EMR sharing and privacy protection mechanism based on medical consortium blockchain,” in *Proceedings of the 6th International Conference on Computer and Technology Applications*, pp. 160–164, Antalya, Turkey, 2020.
 - [23] W. Chen, S. Zhu, J. Li, J. Wu, C.-L. Chen, and Y.-Y. Deng, “Authorized shared electronic medical record system with proxy Re-encryption and blockchain technology,” *Sensors*, vol. 21, no. 22, 2021.
 - [24] D. Xanthidis and O. K. Xanthidou, “A proposed framework for developing an electronic medical record system,” *Journal of Global Information Management*, vol. 29, no. 4, pp. 78–92, 2021.
 - [25] K. Malasri and L. Wang, “Design and implementation of a secure wireless mote-based medical sensor network,” *Sensors*, vol. 9, no. 8, pp. 6273–6297, 2009.
 - [26] Y. Sun, C. Wong, G.-Z. Yang, and B. Lo, “Secure key generation using gait features for body sensor networks,” in *Proceedings of the IEEE 14th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, pp. 206–210, Eindhoven, Netherlands, May 2017.
 - [27] Jason, “Broader access models for realizing information DomiCorporation,” Report JSR-04-132, MITRE Corporation, McLean, VA, USA, 2004.
 - [28] F. K. Dankar and R. Badji, “A risk-based framework for biomedical data sharing,” *Journal of Biomedical Informatics, Journal of Biomedical Informatics*, vol. 66, pp. 231–240, 2017.
 - [29] Q. Ni, E. Bertino, and J. Lobo, “Risk-based access control systems built on fuzzy inferences,” in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, pp. 250–260, Beijing, China,, 2010.
 - [30] P.-C. Cheng, P. Rohatgi, C. Keser, P. A. Karger, G. M. Wanger, and A. S. Reninger, “Fuzzy multi-level security: an experiment on quantified risk-adaptive access control,” in *Proceedings of the IEEE Symposium on Security and Privacy (SP’07)*, pp. 222–230, Berkeley, CA, USA, May 2007.
 - [31] N. N. Diep, L. X. Hung, Y. Zhung, and S. Lee, “Enforcing access control using risk assessment,” in *Proceedings of the Fourth European Conference on Universal Multiservice Networks (ECUMN’07)*, pp. 419–424, Toulouse, France, February 2007.
 - [32] M. Sharma, Y. Bai, S. Chung, and L. Dai, “Using risk in access control for cloud-assisted ehealth,” in *Proceedings of the IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems*, pp. 1047–1052, Liverpool, UK, June 2012.
 - [33] H. Ding, C. Peng, and Y. Tian, “Privacy risk adaptive access control model via evolutionary game,” *Journal on Communications*, vol. 40, no. 12, pp. 9–20, 2019.
 - [34] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Change, “Privacy-preserving fusion of IoT and big data for e-health,” *Future Generation Computer Systems*, vol. 86, pp. 1437–1455, 2018.
 - [35] M. B. Line, I. A. Tøndel, and E. A. Gjære, “A risk-based evaluation of group access control approaches in a healthcare setting,” *International Conference on Availability*, vol. 6908, pp. 26–37, 2011.
 - [36] Q. Wang and H. Jin, “Quantified risk-adaptive access control for patient privacy protection in health information systems,” in *Proceedings of the 6th ACM symposium on information, computer and communications security*, pp. 406–410, Hong Kong, China, March 2011.
 - [37] R. A. Shaikh, K. Adi, and L. Logrippo, “Dynamic risk-based decision methods for access control systems,” *Computers & Security*, vol. 31, no. 4, pp. 447–464, 2012.
 - [38] D. Choi, D. Kim, and S. Park, “A framework for context sensitive risk-based access control in medical information systems,” *Computational and Mathematical Methods in Medicine*, vol. 2015, Article ID 265132, 15 pages, 2015.
 - [39] Z. Hui, H. Li, M. Zhang, and D.-G. Feng, “Risk-adaptive access control model for big data in healthcare,” *Journal on Communications*, vol. 36, no. 12, pp. 190–199, 2015.

- [40] J. Zhang, *The Risk Assessment of Medical Big Data Privacy Security Cloud Environment*, Yunnan University of Finance and Economics, Yunnan, China, 2018.
- [41] R. Jiang, M. Shi, and W. Zhou, "A privacy security risk analysis method for medical big data in urban computing," *IEEE Access*, vol. 7, Article ID 143841, 2019.
- [42] J. Li, Y. Bai, and N. Zaman, "A fuzzy modeling approach for risk-based access control in eHealth cloud," in *Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 17–23, Melbourne, VIC, Australia, July 2013.
- [43] E. Smith and J. Eloff, "Cognitive fuzzy modeling for enhanced risk assessment in a health care institution," *IEEE Intelligent Systems and Their Applications*, vol. 15, no. 2, pp. 69–75, 2000.
- [44] M. Shi, R. Jiang, X. Hu, and J. Shang, "A privacy protection method for health care big data management based on risk access control," *Health Care Management Science*, vol. 23, no. 3, pp. 427–442, 2020.
- [45] X. Ma, H. Xu, H. Gao, and M. Bian, "Real-time multiple-workflow scheduling in cloud environments," *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4002–4018, 2021.
- [46] Y. Zhu, W. Zhang, Y. Chen, and H. Gao, "A novel approach to workload prediction using attention-based LSTM encoder-decoder network in cloud environment," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–18, 2019.

Research Article

A Method of the Active and Passive Event Service Based on the Sensor Web

Lan Liu ¹, Jingjing Fan,² Chengfan Li ³ and Xuefeng Liu ²

¹School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China

²School of Communication and Information Engineering, Shanghai University, Shanghai 200444, China

³School of Computer Engineering and Science, Shanghai University, Shanghai 200444, China

Correspondence should be addressed to Xuefeng Liu; lx02@shu.edu.cn

Received 7 December 2021; Accepted 10 January 2022; Published 31 January 2022

Academic Editor: Yuyu Yin

Copyright © 2022 Lan 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.

The intelligent information system constructed by the sensor web can monitor all kinds of sudden abnormal events, improve the ability of event discovery and rapid disposal, and promote the development of smart city and the construction of the Internet of Things (IoT). In this paper, we consider the problem of complex integration and poor expansibility in the large-scale full-network operation and maintenance system construction and propose an active and passive event service (APES) method based on the sensor web. In the APES, a system framework with the perception layer, data service layer, event service layer, and user layer is firstly defined and constructed. Secondly, a middleware with the ability to active and passive event service (APES) is designed and implemented based on the system framework. Finally, taking abnormal weather and fire warning as examples, the performance of the proposed event service middleware is tested, respectively. Experimental results show that the proposed APES model in this paper has the advantages of high precision, stable operation, and strong practicability and solves “Information Island” and low reusability in the whole network operation and maintenance system. This is an attempt at the structural design of a similar intelligent information system.

1. Introduction

With the commercially developing industrial Internet of Things (IIOT), the original scattered industrial network is rapidly evolving into a large-scale industrial interconnection network via the integration of information and communications technology (ICT) and operational technology (OT) [1–3]. How to ensure the stable and efficient operation of information communication and digital applications and build a network management system with distributed monitoring and intensive management has become a difficulty in related research and application. Meanwhile, more and more enterprises and industries are paying attention to the economic benefits brought by remote operation and predictive maintenance of network infrastructure.

At present, the combination of the sensor network and event service has become an important content of smart city construction [4, 5]. In 2005, the open geospatial consortium

(OGC) proposed a novel sensor web enablement (SWE) framework, and the corresponding sensor web standards and protocols have also been presented. In view of the standard-based discovery, access, subscription, and other operations within the sensor web, the structural differences in communication protocols, data acquisition, processing, and storage in different sensor networks can be eliminated, and then the island effect of sensor networks can be decreased too. Sensor observation server (SOS) mainly focuses on data services. As one of the data sources of event services, SOS manages and stores the data collected by front-end sensors in a unified manner and returns the qualified data to users facing requests.

The event service dedicated to the discovering and alerting of events is usually composed of event providers and event consumers [6, 7]. There are two ways to communicate between the event provider and the event consumer, for example, request-response mode and

subscription-publishing mode [8–10]. Based on the active and passive relationship between the event provider and consumer, the event service is correspondingly divided into active service and passive service [11]. Traditionally, event services are active or passive with respect to service providers. In the event service binary structure composed of event providers and consumers, providers actively “push” services to consumers as active services, and consumers actively “pull” services as passive services. In fact, it is difficult to determine whether these two modes are active or passive under the above definition because the act does not clearly define the “push” or “pull.”

To address the above problems and simplify and clarify the definition of the active and passive relationship of event service, in this paper, the definitions of the active and passive service can be preset as follows: whether the active service or the passive service still takes the event service provider as the reference subject, which emphasizes the core of the event service initiator. If an event service is initiated by the consumer of the service, that is, the service consumer first requests or subscribes to the service from the service provider, the service is regarded as a passive service regardless of the way the service provider provides the service to the service consumer. On the contrary, if the initiator of the service is the provider of the service, the consumer only passively accepts the service, and this mode should be regarded as an active service relative to the reference subject of the service provider. For example, both request-response and subscription-publication event service modes are passive services, and push daily weather forecast, air quality status, and other public service behaviours to the public are the active service. Our proposed active and passive event service (APES) model based on the sensor web has the advantages of high precision, stable operation, and strong practicability and effectively solves the island effect and low reusability in the whole network operation and maintenance system.

The major contributions are concluded as follows:

- (1) Based on the sensor web framework, the APES scheme is presented from the aspects of service architecture, service mode, and event discovery, which is composed of the perception layer, data service layer, event service layer, and user layer.
- (2) An event service middleware (ESM) in the APES method is designed and implemented based on the sensor web. It manages multisource sensor observation data and simplifies the interaction between middleware, data service layer, and users.

The rest of this paper is structured as follows. Section 2 discusses the related work of the APES method based on the sensor web. Section 3 presents details of the event service model including overall architecture and detailed design of the event service layer. Section 4 describes the implementation of the ESM, and Section 5 presents our experimental results. Our conclusions and future work are presented in Section 6.

2. Related Work

The object management group (OGM) first formulated the common object request broker architecture (CORBA) specification and event service specification [12–14]. CORBA event service architecture is mainly composed of the event provider, event channel, and event consumer. Due to the intermediary (event channel) between providers and consumers of the CORBA architecture, the providers and consumers do not interact directly. The CORBA event service model has no clear relationship between the active and passive services.

With the development of the Internet of Things (IoT), the event service model still faces the unprecedented challenges. In the CORBA’s trinity event service model, the discovery of events is at the forefront, and the event channel middleware only plays the role of event delivery. The front-end sensors are mainly responsible for the observation and collection of data and are not directly responsible for the discovery (decision) of events. It not only serves as a delivery event but also can discover and filter events. Therefore, the CORBA event service model cannot meet the above requirements for event services on the IoT. OGC complies with the demands of the development of the IoT and proposes a new type of SWE, which satisfies the intelligent requirements for event services in the IoT era to some extent [15]. As an important part of the SWE, the sensor event service (SES) combines the sensor web with event services to deliver perceptible information that meets filter conditions to consumers [16]. The SES specification adopts a subscription-notification pattern of real-time event services and, in essence, is a passive service. As a member of the SWE, SOS is a data service component, which has no event service capability and can only save sensor observation data for a long period of time to facilitate data backtracking [17, 18]. It provides data support for the construction of such event filters when historical observations are required as a reference for the occurrence of an event.

Based on the standard CORBA specification, an active service system framework is proposed, and the active service is defined as the service provider providing the service to the user without the user giving the order [19]. In this framework, the active service corresponds to the “push” pattern in the CORBA specification, the passive service corresponds to the “pull” pattern, the subscription pattern is classified as the active service, and the request-response pattern is classified as the passive service. To some extent, it extends the service mode of traditional event service. A new notification service based on the traditional event service was first presented in 2000. It is compatible with event services, except that notification services add filtering capabilities. Real-time event service is to extend the standard event service to meet the requirements of real-time applications. And it realizes the real-time scheduling strategy, and the information can be allocated and processed in time.

Then, a real-time event detection service with data service middleware (DSWare) was developed [20]. The middleware can handle unreliable individual reports in

real-time event services, sensor observations with different correlations, and real-time events with special attributes. It can support data semantics information including the relative importance and historical patterns of events. However, the accuracy is low, and the practicability is poor.

The SES specification in the overall sensor web framework has been applied to Zanzibar Island in northeast Tanzania, Africa, and successfully realized the monitoring and notification service of water resources [21]. It avoids wasting a lot of time on polluting water sources, indirectly contributing to the region's workforce and economic development. By integrating multiple object-oriented architecture standards and the real-time event-driven architecture (EDA) package, it sends the data to a central communication middleware, namely, enterprise service bus (ESB), and finally diffuses the data into SES components. By extending the basic CORBA event service specification, a middleware that can complete a real-time event service is designed when consumers can firstly receive notification when an event occurs. It can improve the timeliness and continuity of event service and use efficiency. Since events occur continuously and dynamically in the IoT environment, a hybrid complex event service model based on the IoT resource model is presented, and it has great flexibility and wide application range in the actual applications.

In this paper, we design and implement ESM in APES and use for event discovery and event service. The sensor observation information from the SOS is converted into events so that hot events of public concern can be actively pushed to registered users, while the specific events can be monitored according to the user's personalized subscription requirements after passively accepting the user's subscription request. When an event occurs, an alert notification is sent to the user. This scheme not only makes up for the shortage of the CORBA but also solves the defects that SES cannot provide pure active event service.

3. Event Service Model

3.1. Overall Architecture. The APES model consists of four parts, i.e., perception layer, data service layer, event service layer, and application layer. And the overall architecture of the APES model is shown in Figure 1.

The sensor layer consists of a series of sensors that send the collected data to the data service layer. The core of the data service layer is SOS. The event service layer is the core of this model. The ESM is composed of the data request and parsing module, active service module, and passive service module. The main body of the application layer is the user (consumer), which requests service, receives, and displays alarm information by the consumer's intelligent mobile device.

For the event M , the metamodel can be defined as

$$\text{Event } M = (I d, A, E, L, T), \quad (1)$$

where $I d$ is the number of sensors, and each Event M can be defined by a unique $I d$; A is the attribute of Event M , $A = (\text{attr}1, \dots, \text{attr}n)$, $n \geq 0$; R is the EventSet that contains

the sets of all the operations OPRSet that caused the Event M , $R = (\text{EventSet}, \text{OPRSet})$; L is the location of Event M and can be expressed by the function boundingbox; and T is the occurrence time of Event M , real-time or interval events. In event monitoring, the attribute A contains at least the sensor $I d$ and observation results.

The data samples collected by sensor nodes in the network have both autocorrection and cross-correlation. In return, for a measurement data series of the same physical quantity X_1, X_2, \dots, X_N , the sampling time is T_1, T_2, \dots, T_N , and then the correlation of sensor data can be written as follows:

$$R_x(k) = \sum_{i=1}^{N-k} X_i \cdot X_{i+k}, \quad (2)$$

where k is the sequence step. Although the time variable T does not appear in formula (2), the assumption of the formula is that the continuous data samples are sampled at equal intervals.

Similarly, for the two measurement data series with different physical quantities X_1, X_2, \dots, X_N and Y_1, Y_2, \dots, Y_N , the sampling time is T_1, T_2, \dots, T_N , and then the cross-correlation of sensor data can be written as follows:

$$R_{xy}(k) = \sum_{i=1}^{N-k} X_i \cdot X_{i+k}, \quad (3)$$

where k is the sequence step. Cross-correlation reflects the situation where two random numerical variables change simultaneously.

3.2. Detailed Design of the Event Service Layer. The event service layer is the core component of the APES model. It is an intermediary between the data service layer and the application layer (consumer) and a bridge between the data service layer and the application layer, which distinguishes between the active and passive services. In this paper, we implement the function of the event service layer by constructing an ESM composed of three modules. The composition of the event service layer is shown in Figure 2.

3.2.1. Data Request and Parsing Module. The main functions of the module are as follows:

- (1) When the active service module or the passive service module is called, the request parameters transmitted by the active service module and the passive service module are encapsulated into an XML format request document conforming to the SOS specification and sent to the SOS
- (2) Parsing the key data in the XML format response document returned by SOS and returning the parsed data to the corresponding event service module

3.2.2. Active Service Module. The active service does not require the consumer to subscribe or send a request. After the consumer registers the personal information to the event

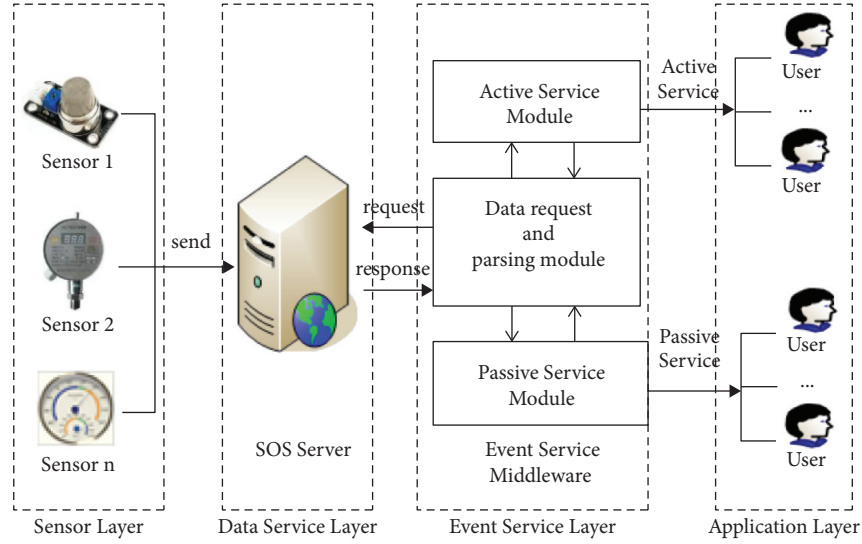


FIGURE 1: Overall architecture of the APES model.

service layer and applies for membership of the event provider, the event service layer will default the consumer to accept the active event service initiated by the event service middleware. The event filtering component in the active service module performs event filtering according to a preset event judgment expression based on the data returned by the data request and parsing module. If the event was established, the event notification component is invoked to send the alarm information. After the event notification component receives the request that the alarm information needs to be sent, the corresponding alarm information is dynamically generated according to the specific event in the request, and the event alarm information is pushed to the consumer through a short message or an e-mail.

3.2.3. Passive Service Module. The passive service is initiated by the consumer, i.e., the consumer is required to subscribe to the event of interest to the event service layer after the registration is completed. The passive service module consists of the event generation component, event filtering component, and event notification component. The event generation component dynamically generates an event discrimination expression according to the subscription condition of the consumer and transmits the logical expression to the event filtering component. The event filtering component filters the event according to the event discrimination expression based on the data returned by the data request and analysis module, and if the event is established, the event notifying component is called to send alarm information. The event notification component publishes the event alarm information to the user who subscribed to the event.

4. Implementation of ESM

4.1. ESM Design. ESM is a component between the data service layer and the application layer, which is the bridge between the above two parts. ESM is in the event service layer, which is the core component of this model. ESM is

composed of three parts, parsing module, active service module, and passive service module, which cooperate to complete all the functions of the event service layer. The composition of the ESM is shown in Figure 3.

4.1.1. Parsing Module. As shown in Figure 3, all functions of the parsing module are implemented by the parser. The parser is the bridge of information exchange between the data service layer and event service layer. The information exchange between active (passive) modules and the data service layer needs to be completed by the parser, and the parser is responsible for interacting with the SOS.

4.1.2. Active Service Module. The event service controller, event filter, and timer logic jointly realize data processing and event filtering of active service. The composition of the active service module is shown in Figure 4.

The event service controller controls the on or off specific event monitoring in the active service. That is to say, it mainly reflects the initiative of the event service by the event service controller and is not restricted to the received active service.

The timer logic is used to control the frequency at which event alert messages are sent. If the active service cycle T_s (data requests, document parsing, event filtering, and judgment after every T_s time) is short and events continue to occur for a period, middleware will push the same alert message to consumers every T_s time without timer logic components, which can result in wasted resources and poor user experience. This module in the timer logic component presets an alarm period T_0 ; when an alarm is issued, the next alarm interval should not be less than the time.

The event filter is responsible for the discovery of the event. It constructs an event filter expression based on the observed attributes of one or more sensors and uses the sensor observations parsed by the parser as the input to the

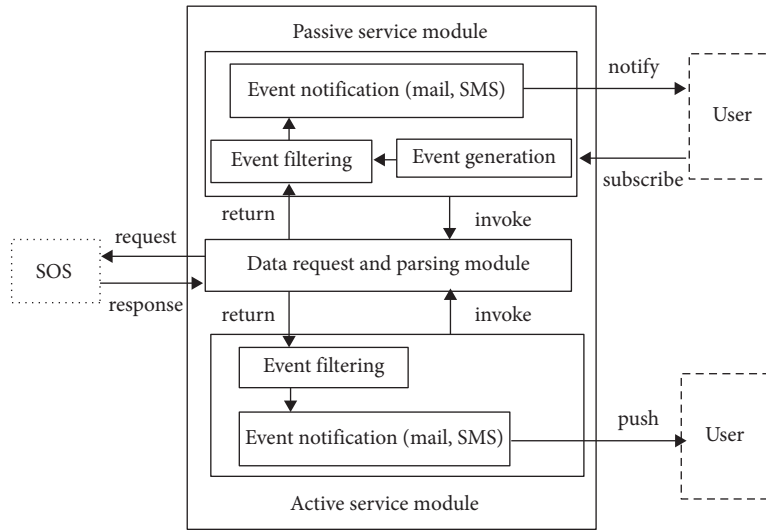


FIGURE 2: The composition of the event service layer.

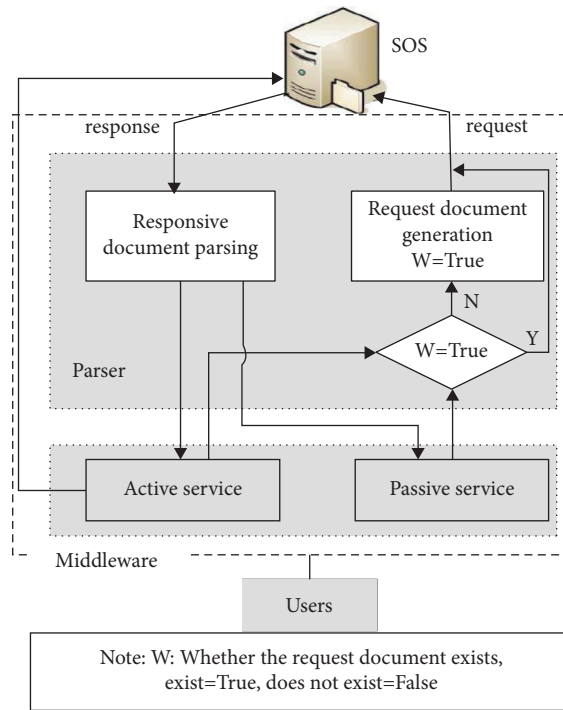


FIGURE 3: The composition of the ESM.

expression. When the expression is established, the event which satisfies the condition will be generated, and the event alarm program will be triggered.

The initiator of the active service is the ESM, and the consumers passively accept the services from the ESM. When starting an active event service, the initial state of the event service controller will be turned on, and the event service controller sends a data request to the parser. After receiving the request, the parser first judges whether the parsed document corresponding to the request exists.

4.1.3. Passive Service Module. The passive service module consists of two parts: a user service controller deployed on the user’s smart phone and an event filter deployed on the server. The composition of the passive service module is shown in Figure 5.

The user service controller is arranged on the smart phone of the user and is responsible for subscribing events to the event service layer to initiate an event service process. Once the event service subscription is successful, the filter of the event service layer starts a passive event service process

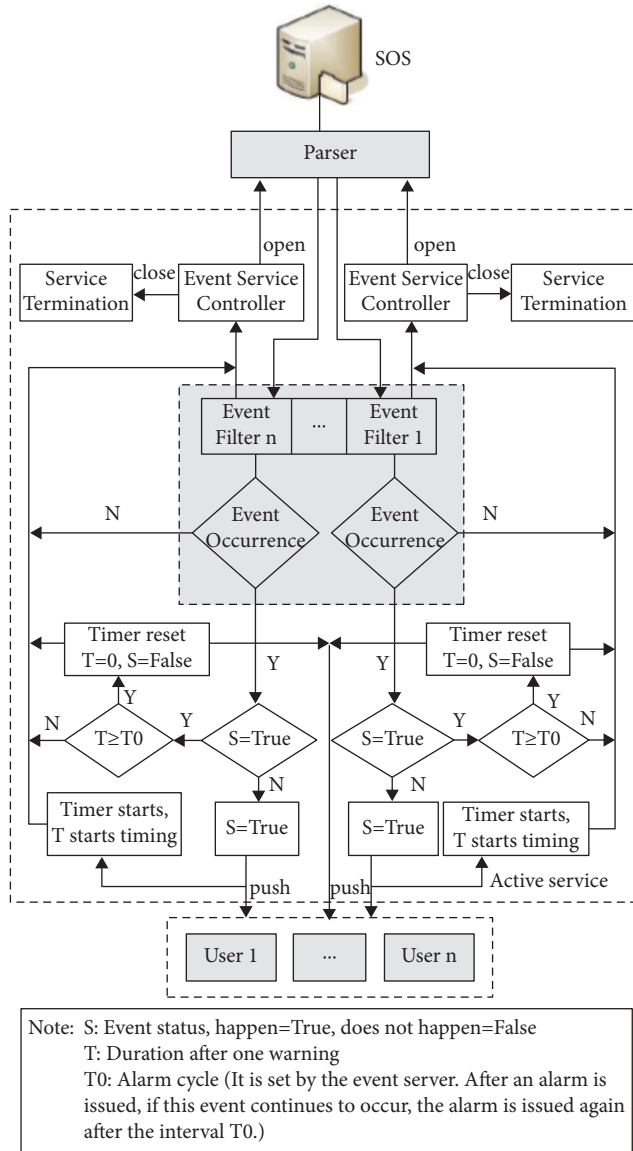


FIGURE 4: The composition of the active service module.

until the event is established, and an alarm notification is sent to the user. Visible, passive service is initiated by consumers, service enabled or not controlled by the user.

Event filter is the core of the passive event service, which is responsible for receiving user's event subscription, constructing event filter expression in real time, sending data service request to the parser, receiving the parsing result returned by the parser, and judging whether the expression is established according to these results. Once the expression is established, the event to which the user subscribes occurs, and an alert notification is immediately sent to the user.

When a consumer subscribes to the ESM service, the consumer's registration information is verified first. If the consumer has not previously registered personal information with the SOS service, there is no right to subscribe to the service because middleware only provides services for registered users. If the user has already registered, the service subscribed by the user will be sent to the middleware.

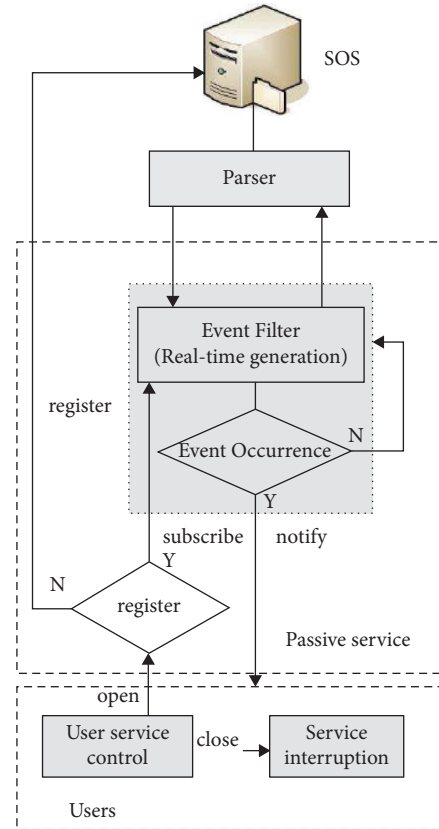


FIGURE 5: The composition of the passive service module.

4.2. Middleware Implementation

4.2.1. Data Request and Parsing Module Implementation.

A class named parser is created to implement the functions of the data request and parsing module, and Table 1 illustrates a detailed structure diagram of the class.

It can be seen from Table 1 that the class contains two member variables and two member methods. The access permission of the GetData method is public, which is mainly used by the outside world to obtain the data of the corresponding sensor. Invoking this method needs to pass in two parameters, namely, the ID number of the sensor and the observation attribute (offering) that needs to be obtained. Then, the method will generate an XML request document conforming to the SOS standard and send a request to the SOS. The SOS returns an XML-formatted document in response to the request. This method returns the document name as a string and stores it in the XMLDoc member variable. The XMLDoc variable access permission is private to prevent the external modification of the document to ensure the authenticity of the data and event judgment results. The access permission of the AnalyseData method is also public, which can be invoked by the outside class. The main function of this method is to parse the content of the returned XML document. The XMLDoc member property is passed to the method as an argument. The AnalyseData method uses the SAX parsing technique to return the parsing results in the string format and store them in the

TABLE 1: The structure of the parser class.

Member variables and member methods	Function
+ Result: string	Storing parsed data
- XMLDoc: string	Storing the document name of the return document by the SOS
+ AnalyseData(string doc): string	Parsing the documents returned by the SOS
+ GetData(string ID, string offering): string	Sending data request to SOS service

Class member access rights: + public; - private.

Result member variable. The access permission of the Result member variable is public which can be obtained by the outside world for filtering events. By the above four members of the class, the parser class implements the functions of request document generation, sending, and response document parsing.

4.2.2. Active Service Module Implementation. A class named *ActiveEventService* is created to implement the function of the active service module of the ESM, and Table 2 illustrates a detailed structure diagram of the class.

It can be seen from Table 2 that there are two member variables and two member methods in this class. The *CycleControl* method is used to control the thread loop process. If T_s is passed as a parameter to the method, all the methods in the *ActiveEventService* class will execute the cycle in T_s period. The *EventJudgement* method mainly filters events. When this method runs, it first calls the *GetData* method of the *Parser* class to request data and then calls the *AnalyseData* method to perform data parsing. Finally, a series of logical combinations are judged based on the data stored in the *Result* variable.

4.2.3. Passive Service Module Implementation. A class named *PassiveEventService* is created to implement the functionality of the passive service module for the ESM, and Table 3 illustrates a detailed structure diagram of the class.

It can be seen from Table 3 that the class has three member methods and two member variables. The *CycleControl* method is used to control the thread loops of this class. If you enter a time parameter of T_s , the methods in that class cycle through T_s . The *DynamicJudgement* method is triggered when a user subscribes to a passive service module for an event. The user's subscription conditions are passed in as arguments to the method, which parses the subscription and dynamically generates an event filter. Finally, the filter's logical discriminate expression is returned in the string format and passed to the *EventJudgement* method.

4.2.4. Alarm Notification Implementation. ESM provides two ways to send alerts, i.e., SMS and e-mail. Create *SMSSend* class and *EmailSend* class to realize the function of SMS notification and e-mail notification, respectively. There is only one implementation method in both classes. In this work, in the implementation of mail function by the JDK e-mail functions, the ESM just needs to send the message subject and content to the method in this class, and then mail

will be automatically generated and sent out through the SMTP protocol. The realization of SMS alarm function uses the third-party platform. By encapsulating the implementation interface given by the third-party platform, the ESM only needs to transmit the user number and the content of the received EMS to the method in the *SMSSend* class, and if the transmission is successful, the server receives the returned status code 200 in the background.

5. Experimental Results

Figure 6 demonstrates the system architecture diagram of the simulation experiment. It shows that there are sensor, server, and mobile smart device in the experiment.

As shown in Figure 6, PC1, PC2, and PC3 use the TCP protocol to transmit data, and PC4 and PC5 use the UDP protocol for data transmission. PC1 simulates a temperature sensor, PC2 simulates a humidity sensor, PC3 simulates a wind speed sensor, PC4 simulates a temperature sensor, and PC5 simulates a CO₂ concentration sensor. Both the SOS and the ESM are deployed on PC6. The client uses the Android-based mobile smart device to receive and display alarm information.

5.1. Active Service Simulation and Testing. The performance of the active service module is tested by abnormal weather warning. In the test, there are two conditions which can be defined as follows:

- (1) High temperature event: the temperature is higher than 35°C, which is a simple event involving real-time observations of only one sensor
- (2) Cold wave event: the temperature drops more than 8°C, and the current temperature is less than 4°C within 24 hours, which is a complex event, involving not only the real-time observation data of the sensor but also the historical data of the sensor

PC1 is used to simulate the temperature sensor with ID number *temp_S-1-1*, and a 96-size array is designed to store a set of temperature data representing the 48-hour real-time observations of the sensor, and then PC1 sequentially extracts one temperature data from the array at 30-minute intervals and sends it to the SOS. SOS receives this data and saves it to the database table. Table 4 demonstrates the part of the simulated temperature data. The first 24 hours will trigger a high temperature anomaly, and the second 24 hours will trigger a cold wave anomaly as the temperature drops.

TABLE 2: The structure of the ActiveEventService class.

Member variables and member methods	Function
- TimeFlag: Boolean	Identifying whether this method is executed
+ ServiceFlag: Boolean	Identification whether the time difference is greater than T_0
+ EventJudgement(): void	Event filtering
+ CycleControl (int time): void	Controlling the thread loop of the class

Class member access rights: + public; - private.

TABLE 3: The structure of the PassiveEventService class.

Member variables and member methods	Function
+ ServiceFlag: Boolean	Identifying whether this method is executed
+ ServiceTerminate: Boolean	Identifying whether the event service ends
+ EventJudgement (string judge): void	Event filtering
+ CycleControl (int time): void	Controlling the thread loop of the class
+ DynamicJudgement (string request): string	Dynamically generating the event filter condition

Class member access rights: + public; - private.

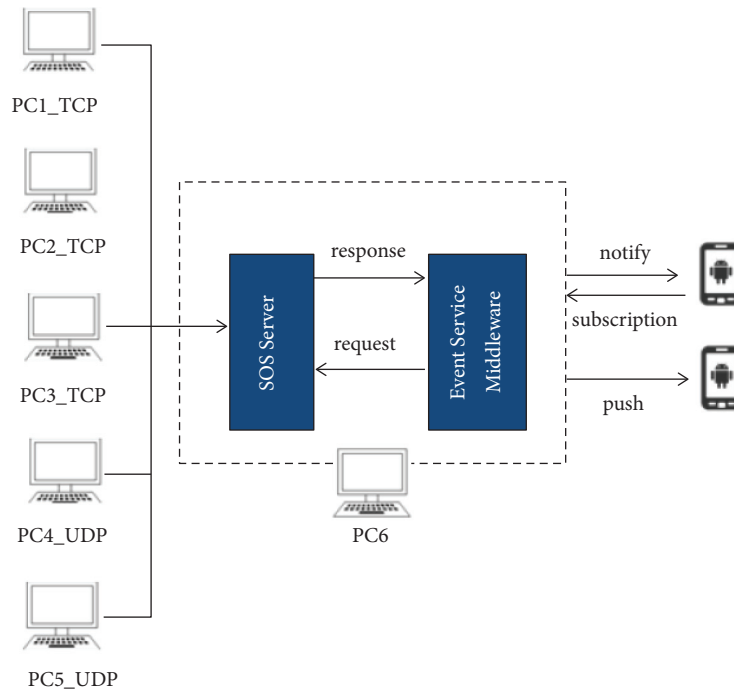


FIGURE 6: The system architecture diagram of the simulation experiment.

After the active service starts, the middleware sends a request to the SOS to obtain the latest observation data, the SOS returns the first real-time temperature (15°C) (serial number: 7801) to the middleware, and the middleware performs event filtering; no high temperature event occurs because the temperature is lower than 35°C. Thereafter, the middleware performs data request and event filtering in a 30-minute cycle. The temperature rises gradually as time goes on. When the temperature reaches 36°C (serial number: 7822), a high-temperature abnormal event is triggered, and the active event service module successfully sends the alarm information to the consumer by SMS and e-mail, respectively, as shown in Figure 7.

After 24 hours, the simulated temperature gradually drops. When the temperature obtained by the sensor is 8°C

(serial number: 7855), the condition of “temperature drop over 8°C in 24 hours” has been met. However, the current temperature has not reached below 4°C, and the cold wave weather alarm is not triggered by the system. With the passage of time, when the temperature obtained by middleware is 3°C (serial number: 7895), the second condition of cold wave weather is met, and the cold wave weather alarm is triggered at this time. The active event service module successfully sends the alarm information to the consumer by SMS and e-mail, as shown in Figure 8.

5.2. *Passive Service Simulation and Testing.* In the test, the condition of the fire event can be defined as follows:

- (1) The temperature rises rapidly above 80°C ($t > 80$)

TABLE 4: Simulated partial temperature data.

Sensor ID	Observation value (°C)	Observation serial number
Temp_S-1-1	15	7801
Temp_S-1-1	16	7802
Temp_S-1-1	19	7803
...
Temp_S-1-1	30	7820
Temp_S-1-1	32	7821
Temp_S-1-1	36	7822
Temp_S-1-1	34	7823
...
Temp_S-1-1	10	7854
Temp_S-1-1	8	7855
Temp_S-1-1	6	7856
...
Temp_S-1-1	3	7895
Temp_S-1-1	1	7896

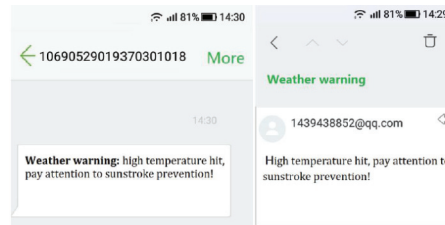


FIGURE 7: The alarm information of high temperature weather by SMS and e-mail.

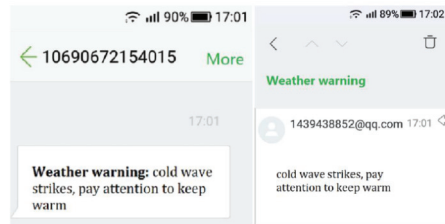


FIGURE 8: The alarm information of the cold weather event by SMS and e-mail.

TABLE 5: Simulated partial temperature and carbon dioxide concentration data.

Sensor ID	Observation value (°C)	Observation serial number	Sensor ID	Observation value (°C)	Observation serial number
Temp_S-1-2	20	8801	Carb_S-1-1	400	8801
Temp_S-1-2	20	8802	Carb_S-1-1	389	8802
...
Temp_S-1-2	48	8840	Carb_S-1-1	760	8840
Temp_S-1-2	57	8841	Carb_S-1-1	840	8841
...
Temp_S-1-2	116	8884	Carb_S-1-1	1480	8884
Temp_S-1-2	134	8885	Carb_S-1-1	1920	8885
...
Temp_S-1-2	186	8895	Carb_S-1-1	2140	8895
Temp_S-1-2	192	8896	Carb_S-1-1	2420	8896

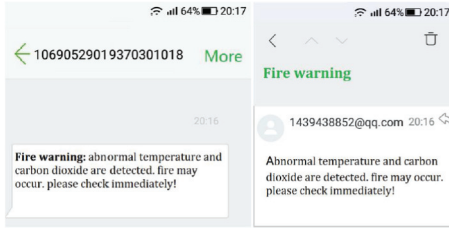


FIGURE 9: The alarm information of the fire event by SMS and e-mail.

- (2) The CO₂ concentration exceeds 2000 ppm ($c > 2000$) in five minutes

The temperature sensor with ID number temp_S-1-2 and the carbon dioxide sensor with ID number Carb_S-1-1 installed in a user's home are simulated by PC4 and PC5, respectively. The user first registers the two sensors in the SOS and subscribes the fire event service to the ESM according to the fire event subscription conditions. As shown in Table 5, two arrays of size 120 were designed to store a simulated set of temperature and carbon dioxide concentration data (5 s/time data acquisition cycle) monitored over 5 minutes, respectively, and the two sets of data were synchronously sent to the SOS at the same cycle in an associated database.

After the service begins, the middleware requests the SOS for the latest observation data at a frequency substantially synchronized with the SOS acceptance data and constructs an event filter according to the user subscription conditions for event filtering. Initial temperature is 20°C, carbon dioxide concentration is about 400 ppm (serial number: 8801), belonging to the normal range, and no alarm occurs. When there are objects burning in the room, the indoor temperature and carbon dioxide concentration increase significantly. When the monitored temperature reaches 116°C, the first condition of the fire event (temperature difference $t > 80^\circ\text{C}$ in 5 minutes) is met, but the carbon dioxide concentration has not reached the warning condition (serial number: 8884), and then there is no event alarm which is triggered. When the monitored temperature and the carbon dioxide concentration reach 186°C and 2140 ppm, respectively, two conditions of a fire event are met, an alarm is successfully triggered, and the passive service module sends alarm information to a consumer by SMS and e-mail, as shown in Figure 9.

6. Conclusions and Future Work

In this paper, we propose a novel event service framework named APES based on the sensor web for the elimination of "Information Island" and low reusability in the whole network operation and maintenance system. In the model, there are perception layer, data service layer, event service layer, and application layer, and the core part is the ESM module. Finally, taking abnormal weather and fire warning as an example, the performance of the ESM module is tested, and the experimental results verify the effectiveness of the proposed method and the practicality of the ESM.

Meanwhile, the SOS information is used as the data source of event service; that is, the front-end sensor does not interact directly with the ESM module to realize event monitoring but sends the collected data to the SOS and stores in the database. To some extent, it results in the delay of event alarm and affects the real-time performance of event discovery. In addition, the performance of the proposed method is tested in the experimental environment instead of real sensor data. In the future, we will exploit APES for a wider range of tests, such as the interactive mode of data and the real sensor web data environment.

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

The authors appreciate the China Vision Cloud platform of Shanghai University and Shanghai Engineering Research Centre of Intelligent Computing System. This work was partially supported by the Science and Technology Commission of Shanghai Municipality (nos. 21142202400 and 19142201600) in China and Graduate Innovation and Entrepreneurship Program in Shanghai University in China (no. 2019GY04).

References

- [1] L. Lan, B. Wang, L. Zhang, R. Shi, and F. Li, "An event-driven service-oriented architecture for internet of things service execution," *International Journal of Online Engineering*, vol. 11, no. 2, pp. 68–73, 2015.
- [2] Y. Huang, H. Xu, H. Gao, X. Ma, and W. Hussain, "SSUR: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 670–681, 2021.
- [3] X. Zhou, X. Xu, W. Liang, Z. Zeng, and Z. Yan, "Deep-learning-enhanced m detection for end-edge-cloud surveillance in smart IoT," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12588–12596, 2021.
- [4] M. Sorrentino, V. Cirillo, D. Panagrosso, A. Trifirò, and F. Bedogni, "Development of free-cooling detection procedures to support energy intelligence actions within telecommunication environments," *Applied Thermal Engineering*, vol. 144, no. 1, pp. 1037–1048, 2018.
- [5] C. Rodríguezdomínguez, K. Benghazi, M. Noguera, J. Garrido, M. Rodríguez, and T. RuizLópez, "A communication model to integrate the request-response and the publish-subscribe paradigms into ubiquitous systems," *Sensors*, vol. 12, no. 6, pp. 7648–7668, 2012.
- [6] M. Fan, H. Fan, N. Chen, Z. Chen, and W. Du, "Active on-demand service method based on event-driven architecture for geospatial data retrieval," *Computers & Geosciences*, vol. 56, no. C, pp. 1–11, 2013.

- [7] C. Guo, J. Liu, and P. Zou, "The study and implementation of active service based on CORBA event service," *Journal of National University of Defense Technology*, vol. 21, no. 4, pp. 83–86, 1999.
- [8] X. Liu, F. Ye, Y. Liu, X. Xie, and J. Fan, "Real-time forecasting method of urban air quality based on observation sites and Thiessen polygons," *International Journal on Smart Sensing and Intelligent Systems*, vol. 8, no. 4, pp. 2065–2082, 2015.
- [9] X. Ma, H. Xu, H. Gao, and M. Bian, "Real-time multiple-workflow scheduling in cloud environments," *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4002–4018, 2021.
- [10] X. Zhou, X. Xu, W. Liang et al., "Intelligent small object detection for digital twin in smart manufacturing with industrial cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 2, pp. 1377–1386, 2022.
- [11] Y. Sun, T. Zhao, E. Li et al., "Radiometer calibration of airborne L-band active and passive microwave detector," *National Remote Sensing Bulletin*, vol. 25, no. 4, pp. 918–928, 2021.
- [12] R. Liu, N. Li, G. Wang et al., "Structure design and analysis of airborne active and passive microwave sounder," *Electro-Mechanical Engineering*, vol. 36, no. 1, pp. 14–21, 2020.
- [13] X. Y. Qian, Q. W. He, D. Y. Li, and C. Huang, "Research on the design and test of a novel hybrid vibration isolator," *Ship Electronic Engineering*, vol. 39, no. 6, pp. 176–187, 2019.
- [14] Y. Xu, Y. Wu, H. Gao, S. Song, Y. Yin, and X. Xiao, "Collaborative APIs recommendation for artificial intelligence of things with information fusion," *Future Generation Computer Systems*, vol. 125, no. 1, pp. 471–479, 2021.
- [15] X. Zhou, X. Yang, J. Ma, and K. I. K. Wang, "Energy efficient smart routing based on link correlation mining for wireless edge computing in IoT," *IEEE Internet of Things Journal*, vol. 8, p. 1, 2021.
- [16] B. Arne, E. Johannes, J. Simon et al., "New generation sensor web enablement," *Sensors*, vol. 11, no. 3, pp. 2652–2699, 2011.
- [17] N. Chen, L. Di, G. Yu, and M. Min, "A flexible geospatial sensor observation service for diverse sensor data based on web service," *ISPRS Journal of Photogrammetry and Remote Sensing*, vol. 64, no. 2, pp. 234–242, 2009.
- [18] H. Gao, Y. Zhang, H. Miao, R. J. D. Barroso, and X. Yang, "SDTIOA: modeling the timed privacy requirements of IoT service composition: a user interaction perspective for automatic transformation from BPEL to timed automata," *Mobile Networks and Applications*, vol. 26, 2021.
- [19] J. B. Liang, F. S. Tian, C. Jiang, and T. S. Wang, "Survey on task offloading techniques for mobile edge computing with multi-devices and multi-servers in internet of things," *Computer Science*, vol. 19, no. 1, pp. 17–24, 2020.
- [20] S. Jirka, A. Bröring, P. Kjeld, J. Maidens, and A. Wytzisk, "A lightweight approach for the sensor observation service to share environmental data across Europe," *Transactions in GIS*, vol. 16, no. 3, pp. 293–312, 2012.
- [21] J. Pradilla, M. Esteve, and C. Palau, "SOSFul: sensor observation service (SOS) for internet of things (IoT)," *IEEE Latin America Transactions*, vol. 16, no. 4, pp. 1276–1283, 2018.

Research Article

PACAM: A Pairwise-Allocated Strategy and Capability Average Matrix-Based Task Scheduling Approach for Edge Computing

Feng Hong, Tianming Zhang , Bin Cao, and Jing Fan

College of Computer and Science College of Software, Zhejiang University of Technology, Hangzhou, China

Correspondence should be addressed to Tianming Zhang; tmzhang@zjut.edu.cn

Received 22 September 2021; Revised 25 November 2021; Accepted 8 December 2021; Published 11 January 2022

Academic Editor: Yuyu Yin

Copyright © 2022 Feng Hong 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 development of the smart Internet of Things (IoT), an increasing number of tasks are deployed on the edge of the network. Considering the substantially limited processing capability of IoT devices, task scheduling as an effective solution offers low latency and flexible computation to improve the system performance and increase the quality of services. However, limited computing resources make it challenging to assign the right tasks to the right devices at the edge of the network. To this end, we propose a polynomial-time solution, which consists of three steps, i.e., identifying available devices, estimating device quantity, and searching for feasible schedules. In order to shrink the number of potential schedules, we present a pairwise-allocated strategy (PA). Based on these, a capability average matrix (CAM)-based index is designed to further boost efficiency. In addition, we evaluate the schedules by the technique for order preference by similarity to an ideal solution (TOPSIS). Extensive experimental evaluation using both real and synthetic datasets demonstrates the efficiency and effectiveness of our proposed approach.

1. Introduction

As an essential function, task scheduling of edge computing has widespread applications in various domains such as the Internet of vehicle [1], transportation [2], health emergency [3], and smart homes [4]. With the development of the smart Internet of Things (IoT) [5–7], an increasing number of tasks deployed on the edge of the network and the IoT devices require to process the heavy tasks with finite response time. Considering the substantially limited processing capability, how to assign tasks to these devices is a significant issue to improve the performance of the system and increase the quality of services. In the following, we give a representative example.

1.1. Motivation Example. (Internet of vehicle) Unmanned aerial vehicles (UAVs) are one type of new IoT devices that are usually used for surveying and mapping services. The number of tasks containing surveying and mapping is large, and if most tasks are assigned to a small part of UAVs, this causes these UAVs to require much time to process tasks and other UAVs do a few tasks, even none. The time cost of services

depends on the time point of finishing the last task, and such assignment making not full use of devices results in a longer response time of finishing a service. In addition, considering limited capability, UAVs are unable to execute the heavy tasks, which results in low quality of services since a few tasks are not finished. Given these limitations, an effective and efficient task scheduling helps to assign the right tasks to the right UAVs and reduce the time cost of finishing services on the premise of guaranteeing the quality of services.

In past years, important research focused on the mathematically strict scheduling models and effective techniques for task scheduling problems of edge computing [8–10]. Few works consider the optimization goals in aspects of fairness; that is, most works consider the global result of each optimization goal in the whole schedule while ignoring its changing local results [11]. Besides, it is well known that task scheduling is an NP-hard problem [12]. Some existing works adopted mathematical programming, such as mixed-Integer programming (MIP [13–17]). Each of them ordinarily adopts the solvers to generate the feasible schedules, and this process requires prohibitive computations to be supported.

In addition, there are many similar studies on task scheduling problems of edge computing [17–18], and they may suffer from one or more of the following drawbacks:

- (1) Most of the studies model their problems and adopt a series of pruning techniques to shrink the number of potential schedules, such as substituting the precise solutions with approximate ones. Although this way can reduce a part of the computation burden, it remains to be time-consuming.
- (2) The task scheduling problems usually involve more than one optimization goal, and the potential conflicts between objectives may exist; i.e., the improvement of one goal may lead to the performance degradation of another. Many studies convert multiple goals to one single objective by empirically using different weights over different goals. However, too much domain knowledge is needed in this way and the generated schedule may fail if the weights are changed.

In our defined task scheduling problem, two categories of constraints are defined. (1) Hard constraint: we consider two hard constraints; i.e., *each device is assigned to at most one task per service* and *each device works at most k consecutive services*. Any one of them is broken will lead to the invalidity of the schedule. (2) Soft constraint: that is, *the total capabilities of the assigned devices for each type of task are equal to its workload*, which should be maximally satisfied. To effectively evaluate the quality of a schedule, we define two optimization goals, i.e., the average coverage *Ave_Coverage* and the fairness of coverage *Coverage_Fairness*, where *Ave_Coverage* computes the coverage ratio of the whole schedule and *Coverage_Fairness* is utilized to measure that all the coverage ratios in the schedule get close to 1. The closer *Ave_Coverage* is to 1 and the smaller *Coverage_Fairness* is, the higher the quality of the schedule will be.

Based on these, we propose a pairwise-allocated strategy and capability average matrix-based approach (PACAM), which is a polynomial solution. To be more specific, PACAM consists of three steps, i.e., identifying available devices, estimating device quantity, and searching for a feasible schedule. In the first step, for each device, PACAM checks whether it is available for tasks according to hard constraints. If one device broke any one of the hard constraints on one service, it will be identified to be unavailable and cannot be assigned to tasks on this service. Next, we need to assign them to tasks. When assigning available devices to tasks directly, we will face a large number of potential different device combinations, which contain plenty of obviously unfeasible device combinations; e.g., all the devices are assigned to the same type of tasks. Hence, in the second step, PACAM preestimates the number of devices for each type of task by the workload for each type of task and the average capability of devices. Then, in the third step, PACAM assigns the corresponding estimated number of devices to each type of task, which effectively reduces the potential device combinations by pruning obviously unfeasible device combinations in advance.

However, evaluating each device combination for searching for the feasible schedule after the pruning technique still requires a great amount of computational consumption; thus, PACAM proposes the pairwise-allocated strategy (PA) to solve this problem. PA treats two devices as a device group and assigns device groups to the corresponding task according to their average capability. Note that the number of devices in these device groups for each task is equal to its estimated number. The reason is that the estimated number of devices for each task is computed by the workload of each task and average capability of devices, the closer the average capability of these device groups is to that of all the devices, the smaller the difference between the total capabilities of these device groups and the workload of the corresponding tasks is. To boost its efficiency, PACAM proposes the capability average matrix (CAM). Besides, PACAM introduces the technique for order preference by similarity to an ideal solution (TOPSIS, [19]) as the evaluation metric. The reason why we use TOPSIS is that it is a multicriteria decision analysis method [20] and is widely used in evaluating a solution with different dimensions. TOPSIS provides enough information for PACAM to generate a wise feasible schedule.

We experimentally evaluate PACAM using a variety of real and synthetic datasets coming from China Telecom company. The real part of datasets contains daily call arrivals for six months of 2020, and the synthetic part is the devices and their capabilities in the corresponding months. We demonstrate the effectiveness and efficiency of PACAM on these datasets. It only takes a few minutes to search for a feasible schedule. In general, the contributions in this article are summarized as follows:

- (1) We propose a polynomial-time solution to efficiently handle task scheduling problems.
- (2) We present PACAM, where a pairwise-allocated (PA) strategy is proposed to shrink the number of potential device combinations and a CAM index is designed to boost efficiency further.
- (3) We first introduce the TOPSIS to effectively evaluate the potential schedules and decide the final feasible schedule.
- (4) Using real-life data (daily call arrivals in 6 months of 2020) and synthetic data (capabilities of devices), we experimentally verify the effectiveness and efficiency of our proposed method. Compared with five state-of-the-art methods for task scheduling, i.e., linear programming (LP [21]), integer programming (IP [22]), MIP [16]), improved particle swarm optimization (IPSO [23]), and multiobjective evolutionary algorithm-based decomposition (MOEAD [24]), we find that PACAM is at least two orders of magnitude faster than the above methods.

The rest of this article is organized as follows. Section 2 introduces several concepts and optimization goals and defines the problem formally. Section 3 elaborates a polynomial-time solution for task scheduling. Experimental

results and our findings are reported in Section 4. Section 5 reviews related work. Finally, Section 6 concludes the article with some directions for future work.

2. Preliminaries

In this section, first, we present a series of basic concepts, i.e., scheduling horizon, devices, and scheduling constraints. Then, we introduce two optimization goals. Finally, we define the task scheduling problem. For ease of reference, Table 1 summarizes the notations used frequently in this article.

2.1. Basic Concepts. We start with notations of each basic concept.

2.1.1. Scheduling Horizon. A scheduling horizon is defined as $S = \{s_1, s_2, \dots, s_n\}$, where $s_i \in S$ represents a service. Each service s_i has two types of tasks, i.e., day task and night task, denoted as DT_i and NT_i , respectively. In addition, each type of task for s_i has a corresponding workload. Specifically, the workloads of the day task DT_i and night task NT_i are represented as WD_i and WN_i , respectively.

2.1.2. Devices. Devices are defined as $D = \{d_1, d_2, \dots, d_m\}$, where each device $d_j \in D$ has a capability c_j . After devices are assigned to tasks, the total capabilities of the devices assigned to the day task DT_i and the night task NT_i are denoted as $\text{totalc_}DT_i$ and $\text{totalc_}NT_i$, respectively.

It is worth noting that the workload corresponds to the device's capabilities. For example, a device whose capability is 2 is assigned to the day task, which means that the workload of this task this device finishes is 2.

2.1.3. Scheduling Constraints. When assigning devices to tasks, constraints such as devices' maintenance, business rules, and regulations are considered. They are divided into two types, i.e., hard constraints that can not be violated and soft constraint that should be maximally satisfied.

In this article, we mainly consider two hard constraints and one soft constraint. Specifically, hard constraints include the following:

- (1) Hard_1 , each device is assigned to at most one type of tasks per service.
- (2) Hard_2 , each device works at most k consecutive services.

The soft constraint is as follows:

- (1) Soft_1 , the total capabilities of the assigned devices for each type of task are equal to its workload.

2.2. Optimization Goals. Following the principle that soft constraints should be maximally satisfied, we proposed two optimization goals: *average workload coverage* and *coverage fairness*.

2.2.1. Average Workload Coverage. A feasible assignment should follow that the total capabilities of the assigned devices maximally satisfy the workloads of tasks. Hence, we define *Ave_Coverage* to compute the coverage ratio of the whole schedule.

Given a scheduling horizon $S = \{s_1, s_2, \dots, s_n\}$ and a set of devices $D = \{d_1, d_2, \dots, d_m\}$, devices are assigned to the day and night tasks, the *Ave_Coverage* is computed by

$$\text{Ave_Coverage} = \frac{1}{2n} \times \sum_{i=1}^n \left(\frac{\text{ac_}DT_i}{WD_i} + \frac{\text{ac_}NT_i}{WN_i} \right). \quad (1)$$

Example 1. The workload of the three services is listed in Table 2 and the total capabilities for each type of task of each service are shown in Table 3. To compute *Ave_Coverage*, thus, according to equation (1), $\text{Ave_Coverage} = (1/6) \times ((2.2/2.2) + (1.1/1.0) + (1.2/0.8) + (2.3/4.6) + (2.3/2.3) + (2.3/2.3)) = 1.02$.

Note that *Ave_Coverage* is used to compute the total average coverage ratio of the whole schedule, but the coverage ratios of some types of tasks are not close to 1; e.g., the coverage ratios of DT_2 and NT_2 are 1.5 and 0.5, which violate Soft_1 . Hence, we adopt *Coverage_Fairness* to ensure that the coverage ratio gets close to 1.

2.2.2. Coverage Fairness. Given a scheduling horizon $S = \{s_1, s_2, \dots, s_n\}$ and a set of devices $D = \{d_1, d_2, \dots, d_m\}$, the *Coverage_Fairness* is defined as follows:

$$\text{Coverage_Fairness} = \left\{ \frac{1}{2n} \times \sum_{i=1}^n \left[\left(\frac{\text{ac_}DT_i}{WD_i} - \text{Ave_Coverage} \right)^2 + \left(\frac{\text{ac_}NT_i}{WN_i} - \text{Ave_Coverage} \right)^2 \right] \right\}^{1/2}. \quad (2)$$

Consider Example 1, according to equation (2), $\text{Coverage_Fairness} = \left\{ (1/6) \times [(1 - 1.02)^2 + (1.1 - 1.02)^2 + (1.5 - 1.02)^2 + (0.5 - 1.02)^2 + (1 - 1.02)^2 + (1 - 1.02)^2] \right\}^{1/2} = 0.289$.

2.3. Problem Definition. Based on the above concepts, we define the problem formally.

2.3.1. Task Scheduling Problem. Given a scheduling horizon $S = \{s_1, s_2, \dots, s_n\}$ and a set of devices $D = \{d_1, d_2, \dots, d_m\}$, the task scheduling aims to assign the devices in D to the tasks of services in S , such that

- (1) hard constrains Hard_1 and Hard_2 must be satisfied
- (2) $|1 - \text{Ave_Coverage}|$ is minimized

TABLE 1: Symbols and description.

Annotation	Description
$S = \{s_1, s_2, \dots, s_n\}$	A scheduling horizon of n services
DT_i or NT_i	The day or night tasks of the service s_i
WD_i or WN_i	The workload of the day task DT_i or the night task NT_i
$D = \{d_1, d_2, \dots, d_m\}$	A set of m devices
$C = \{c_1, c_2, \dots, c_m\}$	The capabilities set of m devices
$Hard_1, Hard_2$	The hard constraints
$Soft_1$	The soft constraint
ac_DT_i / ac_NT_i	The total capabilities of devices assigned to the day task DT_i or the night task NT_i
$total_AC$	The total number of capabilities of available devices
k	The maximal number of consecutive services
$available_D$	The set of devices that can be assigned to tasks
$(task_s_{i-k+1}, \dots, task_s_i)$	The previous k tasks of s_i
$number_DT_i/number_NT_i$	The estimated number of devices for the day/night task of s_i
$totalac_s_i$	The total quantity of capabilities that can be assigned to tasks of s_i
DC_DT_i/DC_NT_i	The device combinations for the day and night tasks of s_i

TABLE 2: The workload for each type of task of each service.

Horizon	WD_i	WN_i
s_1	2.2	1.0
s_2	0.8	4.6
s_3	2.3	2.3

TABLE 3: The assigned capability of each type of task.

Horizon	Total assigned capability	
	ac_DT_i	ac_NT_i
s_1	2.2	1.1
s_2	1.2	2.3
s_3	2.3	2.3

(3) the value of $Coverage_Fairness$ is minimized

3. Algorithm

A naive way to find the optimal schedule is to first enumerate all the possible device combinations and then choose the best one that minimizes the values of $|1 - Ave_Coverage|$ and $Coverage_Fairness$. However, it is computationally intractable because the number of possible device combinations is exponential (i.e., $|S| \times 2^{|D|}$), where $|S|$ and $|D|$ are cardinalities of the scheduling horizon S and the set D of device. To reduce the asymptotic complexity of device scheduling, we design a PA strategy that dramatically shrinks the number of potential device combinations and defines a CAM index to boost efficiency. Based on these, a polynomial-time solution is proposed. The pseudocode is shown in Algorithm 1.

Specifically, we arrange the tasks by services (line 1); each service is composed of three procedures, namely, identifying available devices $identify_device()$ (line 2), estimating device quantity $estimate_quantity$ (lines 3-4), and searching for feasible schedule $search_schedule$ (line 5). Device (D) will be input into $identify_device()$ to generate a set of available devices ($available_D$). Then, $available_E$ and the workload of each type of task will be computed by $estimate_quantity()$

to estimate the number of devices for each type of task of the service s_i (the estimated quantity of devices for day/night tasks $number_DT_i / number_NT_i$). Next, $search_schedule$ generates the feasible schedule according to the workload for each type of task of the service s_i (the workload of day/night task WD_i / WN_i) and the estimated quantity of devices for each type of task. In the following, we detail these three key procedures.

3.1. Identifying Available Device. For the service s_i ($k \leq i < n$), not all the devices can be assigned to the tasks of s_i , since the hard constraint $Hard_2$ rules that the maximal number of consecutive services cannot exceed k services for a device. Hence, for each device, the procedure $identify_device()$ checks whether there is a Rest-status in its tasks of the previous k services (i.e., $s_{i-k+1}, s_{i-k+2}, \dots, s_i$). If the answer is yes, the device is identified to be available for s_i . As for the service s_i ($0 < i < k$), all devices are identified to be available, since even if the device d_j is assigned to tasks during the previous i services, the maximal consecutive services of d_j for s_i cannot be exceed k services.

Next, we give an example to show how we identify available devices, combined with the procedure of $identify_device()$, which is presented in Algorithm 2.

Example 2. Consider a scheduling example as shown in Table 4, where there are 7 devices and all of them have been assigned to tasks of s_1 and s_2 , suppose that the maximal number of consecutive services k is set to 2; now we need to identify the availability of devices for the service s_3 . From Table 4, since the service s_3 ($k < 3 < n$, $k = 2$), we get tasks of the previous 2 services for each device (line 3), then we traverse the tasks of each device to check for whether they contain a Rest-status (line 4). In this example, the tasks of the devices d_1, d_2, d_3, d_4, d_5 contain a Rest-status and the others are not. The device with the tasks containing a Rest-status will be identified to be available and be stored in the set of available devices $available_D$ (line 5). Thus, the devices d_1, d_2, d_3, d_4, d_5 will be put into $available_D$, and the devices d_6, d_7 are

Input: The set of devices D ; the workload WD_i and WN_i ; the maximal consecutive services k
Output: The feasible schedule fs

- (1) **for** each service s_i in S **do**
- (2) $available_D \leftarrow$ **identify_device** (D, k, s_i)
- (3) $number_DT_i \leftarrow$ **estimate_quantity** ($WD_i, available_D$)
- (4) $number_NT_i \leftarrow$ **estimate_quantity** ($WN_i, available_D$)
- (5) $fs \leftarrow$ **search_schedule** ($WD_i, WN_i, number_DT_i, number_NT_i$)
- (6) **Return** fs

ALGORITHM 1: The overview of PACAM.

Input: The set of device D ; the maximal consecutive services k ; the i^{th} service s_i
Output: The set of available devices **available_D** (s_i)

- (1) **for** each service s_i ($k < i < n$) **do**
- (2) **for** each device d_j in D **do**
- (3) $(task_{s_{i-k+1}}, task_{s_{i-k+2}}, \dots, task_{s_k}) \leftarrow$ get tasks of the previous k services for d_j ;
- (4) **if** $(task_{s_{i-k+1}}, task_{s_{i-k+2}}, \dots, task_{s_k})$ contains a Rest-status **then**
- (5) put d_j into $available_D$;
- (6) **for** each service s_i ($0 < i \leq k$) **do**
- (7) **for** each device d_j **do**
- (8) put d_j into $available_D$;
- (9) **Return** $available_D$

ALGORITHM 2: identify_device (D, k, s_i).

TABLE 4: The assigned capability of each type of task.

Device	Service s_1	Service s_2	Service s_3
d_1	Day task	Rest-status	Available
d_2	Night task	Rest-status	Available
d_3	Rest-status	Day task	Available
d_4	Rest-status	Day task	Available
d_5	Rest-status	Rest-status	Available
d_6	Day task	Night task	Unavailable
d_7	Night task	Day task	Unavailable

identified to be unavailable for the service s_3 . As for the service s_i ($0 < i \leq k, k = 2$), each device is available and will be stored in $available_D$ (lines 6–8).

3.2. Estimating Device Quantity. After the available device of s_i is identified, we need to assign them to the tasks of s_i . To avoid enumerating the exponential device combinations, we invoke the procedure *estimate_quantity*() (as Algorithm 3 shows) to estimate the number of devices required for each type of task in advance. Specifically, Algorithm 3 takes the set of available devices and the workload of each type of task of s_i as inputs, and the output is the estimated quantity of available devices required for each type of task of s_i .

First, according to the available device set, we compute their total capability $total_AC$ and average capability *average_AC* (lines 1-2). Based on this, we estimate the number of devices required for each type of task. To avoid the understaffing/overstaffing problem, we need to confirm the

total quantity of available capability $totalac_s_i$ by the following equation:

$$totalac_s_i = \begin{cases} total_AC, & total_AC < WD_i + WN_i, \\ WD_i + WN_i, & total_AC \geq WD_i + WN_i, \end{cases} \quad (3)$$

where $totalac_s_i$ is the total quantity of capabilities that can be assigned to tasks of s_i , $total_AC$ denotes the total number of capabilities of all available devices of s_i , and WD_i/WN_i represents the workload of the day/night task of s_i . If $total_AC < WD_i + WN_i$, we assign all available devices to tasks and $totalac_s_i = total_AC$ (lines 3 and 4). Otherwise, part of available devices will be assigned to tasks and $totalac_s_i = WD_i + WN_i$ (lines 5 and 6).

Then based on the ratio of the workload of each task to that of all tasks, we compute the estimated quantity of each type of task, shown in the following equation (lines 7-8):

$$\begin{cases} ac_DT_i = totalac_s_i \times \frac{WD_i}{WD_i + WN_i}, \\ ac_NT_i = totalac_s_i \times \frac{WN_i}{WD_i + WN_i}, \end{cases} \quad (4)$$

where ac_DT_i and ac_NT_i are the number of capabilities that can be assigned to the day and night tasks of s_i , $totalac_s_i$ is the total quantity of capabilities that can be assigned to tasks of s_i , and WD_i/WN_i represents the workload of the day/night task of s_i .

Next, according to equation (5), we estimate the number of devices required for each task of s_i (lines 9-10):

Input: The set of available devices **available_D**; the workload of day and night tasks WD_i and WN_i
Output: The estimated number of devices for each task number DT_i and number NT_i

- (1) $total_AC \leftarrow$ compute the total capabilities of all available devices;
- (2) $average_AC \leftarrow$ compute the average capability of all available devices
- (3) **if** $total_AC < WD_i + WN_i$ **then**
- (4) $totalac_s_i = total_AC$
- (5) **else**
- (6) $totalac_s_i = WD_i + WN_i$
- (7) $ac_DT_i = total_AC \times (WD_i / (WD_i + WN_i))$;
- (8) $ac_NT_i = total_AC \times (WN_i / (WD_i + WN_i))$;
- (9) $number_DT_i = round_off(ac_DT_i / average_AP)$;
- (10) $number_NT_i = round_off(ac_NT_i / average_AP)$;
- (11) **Return** [$number_DT_i, number_NT_i$];

ALGORITHM 3: estimate_number (*available_D*, WD_i , WN_i).

$$\begin{cases} number_DT_i = round_off\left(\frac{ac_DT_i}{average_AC}\right), \\ number_NT_i = round_off\left(\frac{ac_NT_i}{average_AC}\right), \end{cases} \quad (5)$$

where $number_DT_i / number_NT_i$ is the estimated quantity of available devices required for the day and night tasks, $average_AC$ is the average capability of all available devices, and $round_off$ is the function that rounds off the estimated quantity of devices. For example, $round_off(4.5) = 5$ and $round_off(4.4) = 4$.

Subsequently, we use an example to illustrate how *estimate_quantity()* estimates the number of devices for each type of task of service.

Example 4. Combined with Example 2, the capability of available devices, from d_1 to d_5 , is 1.1, 1.21, 1.35, 1.25, and 1.26, respectively. Supposing that the workload for the day and night tasks of s_i is 5 and 3, we compute the total capability of all available devices. That is, $total_AC = 1.1 + 1.21 + 1.35 + 1.25 + 1.26 = 6.17$. Then, the average capability of these available $average_AC = 6.17 / 5 = 1.234$. According to equation (3), $totalac_s_i = 6.17$, since $total_AC < WD_i + WN_i$ ($6.17 < 5 + 3$). Thus, we compute $ac_DT_i = 6.17 \times 5 / (5 + 3) = 3.86$ and $ac_NT_i = 6.17 \times 3 / (5 + 3) = 2.31$ as equation (4). Then, according to equation (5), we round off the estimated quantity of devices for each type of task of s_i , the estimated quantity of DT_i and NT_i is $number_DT_i = round_off(3.86 / 1.234) = 3$ and $number_NT_i = round_off(2.31 / 1.234) = 2$.

3.3. Searching for a Feasible Schedule. Since the quantity of devices is estimated by the average capability $average_AC$ of all available devices, procedure *search_schedule()* should ensure that the average capability of the actual assigned devices is as close to $average_AC$ as possible. The more closer to $average_AC$ the average capability of the actual assigned device is, the smaller the values of $|1 - Ave_Coverage|$ and $Coverage_Fairness$ are. To achieve this goal, we propose a PA

strategy to search for a feasible schedule. Besides, we define a *CAM* as an index to further its efficiency. Next, we specify the main idea of PA and *CAM* with the following example, combined with the procedure *search_schedule()*, as shown in Algorithm 4.

First, the capabilities of available device are sorted in ascending order (line 1). Then, as Figure 1 shows, it is divided into two subsets (i.e., AC_1 and AC_2) by the value of $average_AC$ (line 2). Thus, $AC_1 = \{1.1, 1.21\}$, $AC_2 = \{1.25, 1.26, 1.25\}$. Next, we adopt PA strategy. Specifically, we take the first capability in AC_1 and AC_2 (lines 4-5), denoted by $\{L1, R1\} = \{1.1, 1.25\}$ (line 6). Thus, the corresponding device group $dp_1 = \{d_1, d_4\}$ (line 7). The average capability of dp_1 $average_dp_1 = (1.1 + 1.25 / 2) = 1.175$ is treated as a trigger to find the next device group cp_2 . To enable the average capability of dp_1 and dp_2 to maximally close to $average_AC$, the expected average capability of dp_2 $Ep_2 = 2 \times average_AC - average_dp_1 = 2 \times 1.234 - 1.175 = 1.293$ (line 8). To quickly pick up such dp_2 , we precompute the *CAM* index as Figure 2 shows (line 3), which is defined as a square matrix of *available_D*. The PA strategy looks up the value that is closest to $Ep_2 (=1.293)$ in this *CAM* index. Note that, to follow the hard constraint $Hard_1$ (i.e., each device is assigned to at most one task per service), dp_2 is selected from at the available device except d_1 and d_4 (lines 9, 11) as Figure 3 shows. Hence, $dp_2 = \{d_3, d_5\}$, because the average capability of d_3 and d_5 is 1.305, which is closest to 1.293 (line 10). Subsequently, the PA strategy computes the expected average capability of dp_i ($i \geq 3$) and locates dp_i in the same way until the total quantity of devices in the selected groups equals the estimated quantity (line 12). It is worth noting that if the estimated quantity of devices is odd, the last device is regarded as a group. Selecting the last device also follows the principle that the average capability of the group (i.e., the capability of the last device) is maximally close to the expected average capability. Thus, we generate a candidate assignment of device combinations (DC_DT_i and DC_NT_i), where the devices d_1, d_4, d_5 are assigned to DT_i and d_2, d_3 are assigned to NT_i (lines 13–16). Subsequently, we select the first capability in AC_1 and the second one in AC_2 , denoted by $\{L1, R2\} = \{1.1, 1.26\}$, and the corresponding device group

Input: The capabilities of available devices AC ; The estimated device quantity for each task number DT_i , number NT_i ;

Output: The feasible schedule $Schedule$

- (1) $AC \leftarrow$ sort AC in ascending order;
- (2) $AC_1, AC_2 \leftarrow$ average AC ;
- (3) $CAM \leftarrow$ compute the average value of any two capabilities in AC
- (4) **for** $c_j \in AC_1$ **do**
- (5) **for** $c_k \in AC_2$ **do**
- (6) $\{L1, R1\} \leftarrow (c_j, c_k)$;
- (7) dp_1 find the corresponding devices of c_j, c_k in AC
- (8) $Ep_2 \times average_AP - average_dp_1$;
- (9) **Remove** $dp_1 \in CAM, AC_1$ and AC_2 ;
- (10) $dp_2 \leftarrow$ search in CAM ;
- (11) **Remove** $dp_2 \in CAM, AC_1$ and AC_2 ;
- (12) search dp_i until device quantity of $\{dp_1, dp_2, \dots, dp_{i-1}\}$ equals to number DT_i
- (13) $DC_DT_i \leftarrow \{dp_1, dp_2, \dots, dp_{i-1}\}$;
- (14) **Replace** number DT_i with number NT_i ;
- (15) DC_NT_i repeat the search operations of DT_i
- (16) **add** (DC_DT_i, DC_NT_i) into assignment
- (17) the feasible schedule $fs \leftarrow$ TOPSIS(assignment)
- (18) **Return** fs

ALGORITHM 4: search_schedule (available_D, totalc_DT_i, totalc_NT_i, number_DT_i, number_NT_i).

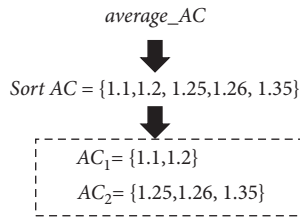


FIGURE 1: Dividing the capabilities set into two subsets.

	d_1	d_2	d_3	d_4	d_5
ac_1	1.1	1.155	1.225	1.175	1.18
ac_2	1.155	1.21	1.28	1.23	1.235
ac_3	1.225	1.28	1.25	1.3	1.305
ac_4	1.175	1.23	1.3	1.25	1.255
ac_5	1.18	1.235	1.305	1.255	1.26

FIGURE 2: The example of establishing capability average matrix.

	d_1	d_2	d_3	d_4	d_5
ac_1	1.1	1.155	1.225	1.175	1.18
ac_2	1.155	1.21	1.28	1.23	1.235
ac_3	1.225	1.28	1.25	1.3	1.305
ac_4	1.175	1.23	1.3	1.25	1.255
ac_5	1.18	1.235	1.305	1.255	1.26

FIGURE 3: The example of searching dp_2 .

$dp_1 = \{d_1, d_5\}$ is utilized to generate the next candidate assignment until all combinations of capability between AC_1 and AC_2 are listed.

These candidate assignments will be evaluated by TOPSIS [19] to select the feasible schedule (line 17). The reason why we use TOPSIS is that it is a multicriteria decision analysis method [20] and is widely used in evaluating a result with different dimensions. TOPSIS orthogonalizes optimization goals; that is, all optimization goals have the same direction of optimization. Next, TOPSIS standardizes all optimization goals since the optimization goals have different magnitudes. Finally, TOPSIS evaluates all candidate assignments and generates their scores; the higher the score is, the higher the quality of this assignment is. The detailed steps of TOPSIS will be described in the experiment section.

4. Discussion

We discuss the space and time complexities below.

4.1. Space Complexity Comparison. In the worst case, the space of our approach is $O(n \cdot (m^2/2))$, where n denotes the number of services in the scheduling horizon S and m represents the number of devices. As for the method of enumerating all possible schedules, its space is $O(n \cdot (\sum_{t=0,1,\dots,m} 2^t \cdot C_m^t))$, where n denotes the number of services in the scheduling horizon S , t is the number of devices whose capabilities maximally minimize $|1 - Ave_Coverage|$ and $Fairness_Coverage$, and C_m^t represents the number of combinations of selecting t devices from the devices set whose size is m . Hence, the space of our approach is square, and that of traversing is exponential.

$$\begin{aligned}
& \lim_{n \rightarrow \infty} n \times \frac{m^2}{2} / n \times \left(\sum_{t=0,1,\dots,m} 2^t \cdot C_m^t \right) \\
& \leq \lim_{m \rightarrow \infty} \frac{m^2}{\sum_{t=0,1,\dots,m} C_m^t} \\
& = \lim_{m \rightarrow \infty} \frac{m^2}{2^m} = 0.
\end{aligned} \tag{6}$$

4.2. Time Complexity. Our approach generates a feasible assignment by the CAM index, which is composed of m^2 average capabilities. Hence, a feasible assignment requires $O(m^2)$ time and all feasible assignments of n services need $O(n \cdot m^4)$ time. As for enumerating all possible schedules, it requires $O(n \cdot (\sum_{t=0,1,\dots,m} 2^t \cdot C_m^t))$ time. This time complexity is more than $O(2^m)$, and $O(2^m) > r \text{ bin } O(m^4)$.

5. Experiments

In this section, we experimentally evaluate the efficiency and effectiveness of our proposed solution PACAM against the state-of-the-art methods. We implement our algorithm in Python and adopt the Python implementation of all competitors based on the following methods: (1) LP [21], (2) IP [22], (3) MIP [16], (4) IPSO [23], and (5) MOEAD [24]. The solver used in this article is Gurobi solver 9.1 [25]. It is worth noting that since all the above-mentioned approaches are universal methods, they can not be used directly; we make minor modifications to adapt them to our studied problem. In addition, to compare the performance of PACAM with the other five methods, we (1) report the response time of each method generating the same feasible schedule results and (2) report the TOPSIS score of each method under the same response time, in order to have a fairer and more accurate comparison.

Besides, all evaluations in this section are based on a mixture of real and synthetic datasets, which are presented in Table 5. The real part comes from the China Telecom company, containing the tasks of six months from July 2020 to December 2020. In Table 5, the number of services of each dataset is listed; it is worth noting that the tasks of each service s_i in each dataset are divided into two parts, treated as the workloads WD_i and WN_i for the day and night tasks of s_i , respectively. The synthetic part is the devices, which are synthesized from the real devices of China Telecom company, as shown in Table 5. Specifically, each month contains five synthetic device sets, whose quantities are 20, 40, 60, 80, and 100. Each device in these device sets has a capability. Note that each experiment will randomly choose the corresponding quantity of devices for ten times to be executed, and the average measurement is reported. All the experiments are conducted on a server machine with an Intel(R) Xeon(R) CPU E5-2637 3.50 GHz processor and 8 GB RAM, running Windows 10 with Python 3.8.

5.1. Metrics. Each potential schedule will be evaluated for facilitating generating the feasible schedule, and we adopt

TOPSIS [19] to achieve this step. The main step of TOPSIS is presented as follows.

First, the optimization goals need to be transformed into such an indicator, whose value is larger, resulting in a feasible with better quality, as TOPSIS asks. Hence, we transform *Ave_Coverage* according to the following equation:

$$\bar{x}_i = 1 - \frac{|x_i - x_{\text{best}}|}{M}, \tag{7}$$

$$\text{s.t. } M = \max\{|x_i - x_{\text{best}}|\},$$

where x_i denotes the value of *Ave_Coverage* for the i^{th} schedule and x_{best} is the best value of *Ave_Coverage* for all schedules.

Coverage_Fairness is transformed based on the following equation:

$$\bar{y}_i = \frac{1}{y_i}, \tag{8}$$

where y_i denotes the value of *Coverage_Fairness* for i^{th} schedule.

Next, we normalize these transformed optimization goals as follows:

$$\text{normalized_value}_{ij} = \frac{\text{value}_{ij}}{\sqrt{\sum_{i=1}^n \text{value}_{ij}^2}}, \tag{9}$$

where value_{ij} is the value of i^{th} optimization goal for j^{th} potential schedule and n denotes the number of potential schedules.

Then, we compute the distance between the optimal/worst schedule and each potential schedule, according to the following:

$$\begin{cases} \text{distance_opt} = \sqrt{\sum_{j=1}^2 (\text{opt} - \text{normalized_value}_{ij})^2}, \\ \text{distance_wor} = \sqrt{\sum_{j=1}^2 (\text{wor} - \text{normalized_value}_{ij})^2}, \end{cases} \tag{10}$$

where *opt/wor* denotes the values of optimization goals for the optimal/worst schedule among all potential schedules.

Finally, we score each potential schedule according to the following equation and select the feasible schedule:

$$\text{score}_i = \frac{\text{distance_wor}}{\text{distance_opt} + \text{distance_wor}}. \tag{11}$$

5.2. Experiment Setting. We perform nine sets of experiments to evaluate the performance of PACAM, where EXP1 to EXP6 are used to evaluate the overall performance among PACAM and five alternatives and EXP7 to EXP9 present the

TABLE 5: The datasets used in experiments.

Datasets	Services	Tasks	Device quantity
July 2020	30	37,691	81
Aug. 2020	31	38,037	60
Sept. 2020	31	35,991	76
Oct. 2020	30	37,110	70
Nov. 2020	31	38,133	86
Dec. 2020	30	36,510	79

internal performance of PACAM. The parameters in each experiment are illustrated in Table 6.

EXP1 and EXP2 evaluate the impact of varying the datasets; we fix the number of devices to 100 and set the maximal consecutive services k to 4 services. Note that EXP1 generates the schedule with the same quality on all six datasets to report the response time, and EXP2 runs the same response time on all six datasets to report the quality of the generated schedule. EXP3 and EXP4 evaluate the impact of varying k ; we fix the number of devices to 100 and run EXP3 on November to report the response time for generating the schedule with the same quality and run EXP4 on November to report the quality of generated schedule with the same running time. EXP5 and EXP6 evaluate the impact of varying the number of devices; we set the maximal consecutive services k to 4 and run EXP5 on November to report the response time for generating the schedule with the same quality and run EXP6 to report the quality of generated schedule with the same running time.

All internal experiments (i.e., from EXP7 to EXP9) are performed, considering generating the schedule with the same quality as the end signal. Besides, EXP7 evaluates the internal impact of varying the datasets for PACAM; we fix the number of devices to 100, set the maximal consecutive services to 4, and report the response time. EXP8 evaluates the internal impact of varying k ; we fix the number of devices to 100 and run it on November to report response time. EXP9 evaluates the internal impact of varying the number of devices; we set the maximal consecutive services to 4 and run it on November to report the response time.

5.3. Overall Performance

5.3.1. EXP 1: Search Efficiency. The first set of experiments verifies the performance of PACAM by varying datasets compared with the other five alternative methods. The result is illustrated in Figure 4(a). The first observation is that PACAM is the best in all cases, with IP, LP, and MIP in the second place, they are comparable, and then IPSO and MOEAD are the worst. Particularly, on all six datasets, PACAM outperforms IP, LP, and MIP by two orders of magnitude, and it is faster than IPSO and MOEAD by 316.23 and 2511.89 times at least, respectively. This is because that IP, LP, and MIP need to consider all the potential schedules and MOEAD and IPSO need a large number of iterations to generate a feasible schedule due to the random nature of searching strategies, while PACAM preestimates the number of devices required for each type of task, which effectively shrinks the number of potential schedules. The second

TABLE 6: The parameters used in experiments.

EXPs	Data sets	Number of devices	k	Same run time	Same quality
EXP1	—	100	4		✓
EXP2	—	100	4	✓	
EXP3	Nov.	100	—		✓
EXP4	Nov.	100	—	✓	
EXP5	Nov.	—	4		✓
EXP6	Nov.	—	4	✓	
EXP7	—	100	4		✓
EXP8	Nov.	100	—		✓
EXP9	Nov.	—	4		✓

observation is that PACAM is more stable than MOEAD because PACAM searches for the feasible schedule within a small search range, owing to its preestimating strategy. While MOEAD generates the optimal schedule by mutation and crossover operations, these operations contain a random mechanism, which results in the instability of newly generated solutions.

5.3.2. EXP 2: Search Effectiveness on Running the Same Time.

Compared with EXP 1, EXP 2 runs under the condition of running the same time and reports the TOPSIS score of each method as illustrated in Figure 4(b). It is seen that when varying datasets, the TOPSIS score of PACAM changes slightly, and it is the highest. The reason is that PACAM adopts the pairwise-allocated strategy, which assigns devices to the tasks following the principle that the total capabilities of devices assigned to one task should be maximally close to the workload of this task. This guarantees that the average coverage will be maximally close to 1 and the coverage fairness will be reduced to the minimum. Hence, the corresponding TOPSIS will perform best. Three mathematical methods consider a prohibitive number of potential schedules, and thus they need more time to generate the feasible schedule. IPSO searches for the feasible schedule according to one previous solution nearest to the fixed schedule, which easily leads to locally optimal solutions. As for MOEAD, the limited running time does not allow MOEAD to perform enough generation operations, which influences the quality of the generated schedule.

5.3.3. EXP 3: Effect of k on Search Efficiency.

The third set of experiments aims to explore the impact of varying maximal consecutive services k on search performance. The result is shown in Figure 5(a). The first observation is that the running time of all methods, except MOEAD, changes slightly with the growth of k . This is because PACAM uses the preestimating strategy so that varying the maximal consecutive services has nearly no effect on its efficiency. IP, LP, and MIP search for the feasible schedule in a huge range; the internal algorithms in solvers such as the branch and bound method help generate stable solutions. IPSO falls into a local optimum since its search strategy is based on the previous solution nearest to the fixed schedule. On the other hand, MOEAD generates a feasible schedule based on the

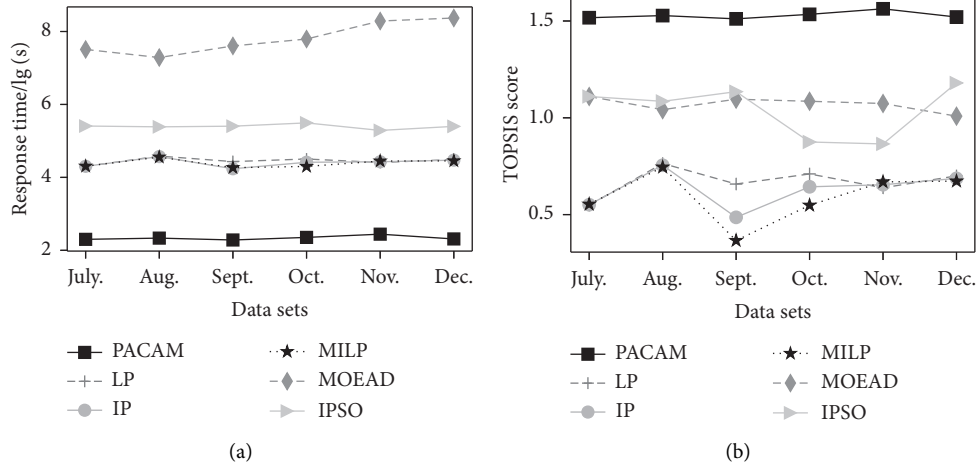


FIGURE 4: Overall effectiveness and efficiency with different datasets. (a) Fixing schedule quality. (b) Fixing response time.

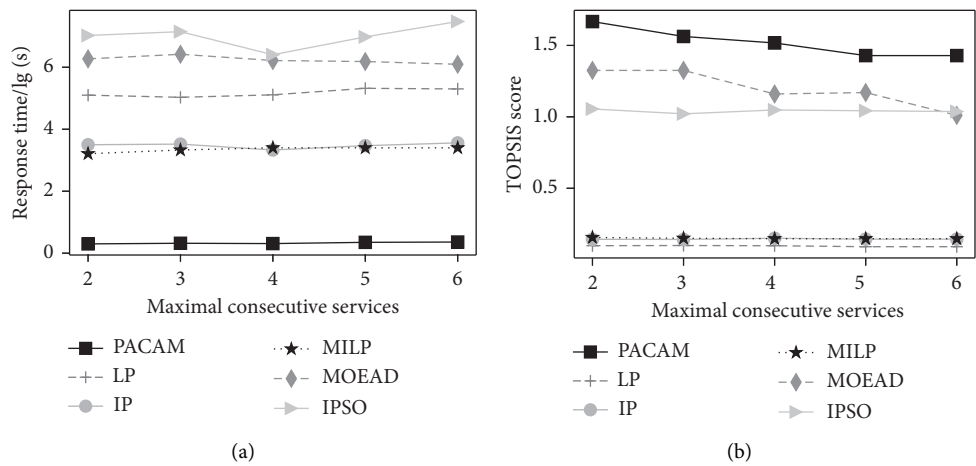


FIGURE 5: Overall effectiveness and efficiency with varying k . (a) Fixing schedule quality. (b) Fixing response time.

random nature of the search strategy, and its response time is dependent on this rather than k . Thus, the response time of MOEAD fluctuates greatly. The second observation is that PACAM has the lowest elapsed time. The reason lies in two aspects. First, while searching for the feasible schedule, PACAM prunes a large number of potential schedules and finds the feasible schedule based on pairwise-allocated strategy. Second, CAM is established to boost efficiency.

5.3.4. EXP 4: Effect of k on Search Effectiveness with Same Running Time. EXP 4 runs under the same condition as EXP3 and reports the TOPSIS score of each method. The result is plotted in Figure 5(b). The first observation is that the TOPSIS score of PACAM increases as k ascends. The reason is that a larger k means fewer rest services in a scheduling horizon and more available devices to be assigned in a day, leading to the total capabilities of devices assigned to one task being closer to its workload, and hence a higher TOPSIS score. The second observation is that the TOPSIS score of PACAM is still the highest under the

different k . It is because the pairwise-allocated strategy in PACAM follows the principle that the selected device group should be the one making the average capability of all selected device groups nearest to that of all devices. Thus, the total capabilities of all assigned devices are maximally equal to the workload of the corresponding tasks.

5.3.5. EXP 5: Effect of the Number of Devices on Search Efficiency. The fifth set of experiments evaluates the impact of the number of devices on search efficiency. The result is depicted in Figure 6(a). The first observation is that the response time of PACAM, IP, LP, and MIP increases as the number of devices grows. The reason is that, for PACAM, an increasing number of devices means more potential device groups, which requires PACAM to spend more time searching for the suitable device group. Three mathematical methods require more response time since the number of potential device group combinations increases with the number of devices grows. The second observation is that the running time of MOEAD and IPSO fluctuates with the

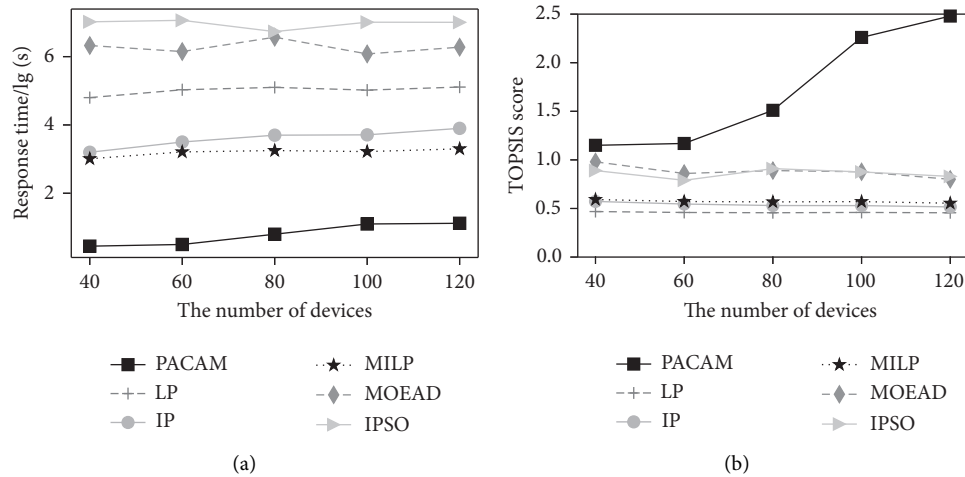


FIGURE 6: Overall effectiveness and efficiency with the number of devices. (a) Fixing schedule quality. (b) Fixing response time.

increase in the number of devices. The reason is that to search for the feasible schedule, MOEAD and IPSO need a large number of generation and iteration operations, where there is a great deal of randomness.

5.3.6. EXP 6: Effect of the Number of Devices on Search Effectiveness. Figure 6(b) shows the result of each method by varying the number of devices. It is observed that the TOPSIS score of PACAM increases as the number of devices grows. It is because that more device groups are available with an increasing number of devices, which means there is a higher possibility for PACAM selecting the device groups whose capability is nearest to the workload of tasks. As for the others, under limited running time, their mechanisms are time-consuming, and the generated feasible schedules are of low quality. Again, the TOPSIS score of PACAM is the highest in all cases.

5.4. Internal Performance

5.4.1. EXP 7: Internal Performance vs. Different Datasets. The seventh set of experiments evaluates the internal impact of the performance of the PA strategy and CAM by varying the datasets. We compare PACAM with two alternative methods, i.e., PACAM-NoCAM and *Traverse*, respectively. PACAM-NoCAM removes the CAM, and *Traverse* evaluates all potential schedules. The result is illustrated in Figure 7(a). It is observed that PACAM is faster than PACAM-NoCAM and *Traverse* on all datasets. In particular, PACAM is 380 times faster than PACAM-NoCAM and outperforms *Traverse* by two orders of magnitude on average, respectively. This is because, compared to *Traverse*, PACAM and PACAM-NoCAM contain PA, which greatly reduces the number of potential schedules. This indicates that PA effectively shrinks search range and improves efficiency. In addition, PACAM adopts CAM to boost efficiency, and based on CAM, PACAM outperforms PACAM-NoCAM by 4.47 times; this finding indicates that CAM further improves the efficiency of search.

5.4.2. EXP 8: Internal Performance vs. k . The eighth set of experiments verifies the internal performance for PACAM by varying k . The result is illustrated in Figure 7(b). The first observation is that the response time of all methods remains stable as the number of consecutive services grows. It is because both PACAM and PACAM-NoCAM adopt the pairwise-allocated strategy, shrink the number of potential schedules, and search for the feasible schedule in a small search range, which provides the stability of PACAM and PACAM-NoCAM. As for *Traverse*, once it finds the schedule, the response time is reported. Hence, the response time of *Traverse* remains stable. The second observation is that PACAM is the best in all cases, with PACAM-NoCAM in the second place, and then *Traverse* is the worst. The reason is that the number of potential schedules that are evaluated by *Traverse* is large; hence, *Traverse* requires a large amount of time consumption. PACAM-NoCAM adopts the PA strategy to reduce the number of potential schedules and searches for the feasible schedule in a small range, which effectively reduces the time cost. In addition, based on the PA strategy, PACAM utilizes the CAM to improve efficiency further.

5.4.3. EXP 9: Internal Performance vs. the Number of Devices. The ninth set of experiments explores the effect of the number of devices on the internal performance of PACAM. The result is plotted in Figure 7(c). The first observation is that the response time of traversing is exponential because the number of potential schedules grows exponentially as the number of devices increases. The second observation is that the response time of PACAM and PACAM-NoCAM keeps stable since estimating the number of devices prunes plenty of unfeasible schedules, leading to less time in selecting suitable device groups. The third observation is that compared with PACAM-NoCAM, the response time of PACAM is much shorter. The reason is that PACAM uses CAM for fast finding the suitable device groups.

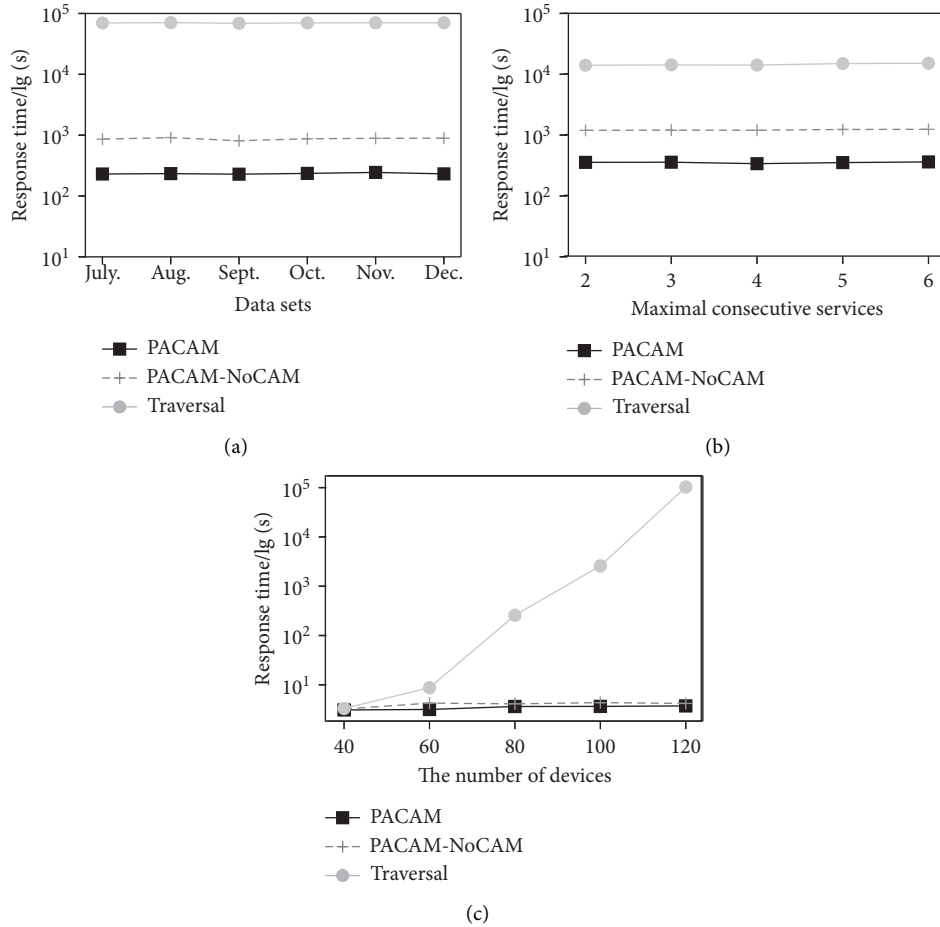


FIGURE 7: Internal performance of PACAM by varying parameters. (a) Response time vs. different data sets. (b) Response time vs. k . (c) Response time vs. the number of devices.

6. Related Work

Currently, algorithms to address task scheduling problems of edge computing are divided into three categories. The first category is to adopt the method of mathematical programming. Regularly, it models the task scheduling problem by complex mathematical models, then computes the feasible schedules by operating a series of solvers like MIP solver [13–17] on this problem model. Although this category of the method has high effectiveness, a large amount of computation leads to low efficiency and high response time. These methods do not provide the allocated strategy and search strategy as PACAM does and limit themselves to similar trips or other mathematical methods.

The second category is the approximate algorithm. Many studies are adopting approximate algorithms in such resource scheduling. Badri et al. [26] modeled the application placement of the MEC system and adopted the parallel sample averaging approximation (SAA) algorithm to solve it. Guo et al. [27] treated the edge-cloud placement problem as a multiobjective optimization problem and addressed it by k -means and hybrid quadratic programming. Fang [28] described a multiuser resource allocation problem in edge computing and proposed an approximate algorithm for local

search to solve this problem. The basic idea of these algorithms is to model their problem and adopt the existing approximate methods for generating feasible solutions. In addition, some works assigned tasks to devices with proper skill type by collaborative filtering mechanism [29], but it is out of our consideration. In summary, these methods have shortages, such that they are easy to fall into a local optimum and the performance of the solutions can not be guaranteed due to randomness. Moreover, in our work, we propose PACAM, which strategically assigns devices and defines a matrix-based index to speed up searching for the feasible schedule.

The third category is the heuristic algorithm. Nowadays, an increasing number of ways to solve task scheduling problems in edge computing is heuristic algorithms. Considering some phenomena in nature, heuristic algorithms abstracted this similarity into their methods to address the task scheduling problem [30]. Hong et al. [24] modeled their resource scheduling problem as a multiobjective problem and adopted the multiobjective evolutionary algorithm based on decomposition (MOEAD) to generate feasible solutions. In addition, some works [31, 32] used the non-dominated sorting genetic algorithm (NSGA) to deal with the task scheduling problem containing multiple objectives.

Besides, the authors in [23] proposed a PSO-based heuristic strategy to solve the joint problem of service placement and task provisioning. This algorithm solved the resource scheduling problem by greedy-based and genetic-based algorithms. However, they are easy to fall into a local optimal solution. Besides, most of them require too much domain knowledge to adjust the parameters, and it is impossible to get feasible parameters efficiently. In our work, PACAM preestimates the number of devices required for each type of task, which avoids wide-range search. PACAM adopts a series of strategies to shrink the number of potential schedules, such as the PA strategy and CAM and effectively assign devices to the corresponding tasks of each day.

7. Conclusion

This article proposes PACAM, a PA strategy and CAM-based approach, to solving the task scheduling problem. Devices are assigned to tasks of each service in the scheduling horizon; meanwhile, the hard constraints must be followed and the soft constraint should be maximally satisfied. Based on these, PACAM estimates the number of devices required for each type of task of each service in the scheduling horizon. Then, PACAM adopts the PA strategy to assign the corresponding number of devices to tasks. To facilitate finding the device groups we need, PACAM takes CAM as an index to speed up this process. Thus, we just spent a few computations to find the final feasible schedule. Extensive experimental evaluation demonstrates the effectiveness and efficiency of our proposed approach. In the future, we intend to explore how to assign large-scale devices to tasks with more optimization goals.

Data Availability

The data will be made available on reasonable request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National R&D Program of China, under Grant no. 2018YFB1402800, and the Fundamental Research Funds for the Provincial Universities of Zhejiang under Grant no. RF-A2020007.

References

- [1] Z. Ning, K. Zhang, X. Wang et al., "Intelligent edge computing in internet of vehicles: a joint computation offloading and caching solution," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 4, pp. 2212–2225, 2020.
- [2] J. Lin, W. Yu, X. Yang, P. Zhao, H. Zhang, and W. Zhao, "An edge computing based public vehicle system for smart transportation," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 12635–12651, 2020.
- [3] H. Wang, J. Gong, Y. Zhuang, H. Shen, and J. Lach, "Healthedge: task scheduling for edge computing with health emergency and human behavior consideration in smart homes," in *Proceedings of the 2017 IEEE International Conference on Big Data (Big Data)*, pp. 1213–1222, IEEE, Shenzhen, China, August 2017.
- [4] H. Liu, S. Li, and W. Sun, "Resource allocation for edge computing without using cloud center in smart home environment: a pricing approach," *Sensors*, vol. 20, no. 22, p. 6545, 2020.
- [5] H. Gao, X. Qin, R. J. D. Barroso, W. Hussain, Y. Xu, and Y. Yin, "Collaborative learning-based industrial iot api recommendation for software-defined devices: The implicit knowledge discovery perspective," *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2020.
- [6] H. Gao, K. Xu, M. Cao, J. Xiao, Q. Xu, and Y. Yin, "The deep features and attention mechanism-based method to dish healthcare under social iot systems: An empirical study with a hand-deep local-global net," *IEEE Transactions on Computational Social Systems*, 2021.
- [7] Y. Yin, Z. Cao, Y. Xu, H. Gao, R. Li, and Z. Mai, "Qos prediction for service recommendation with features learning in mobile edge computing environment," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 4, pp. 1136–1145, 2020.
- [8] Y. Li and S. Wang, "An energy-aware edge server placement algorithm in Mobile Edge Computing," in *Proceedings of the 2018 IEEE International Conference on Edge Computing (EDGE)*, San Francisco, CA, USA, July 2018.
- [9] J. Meng, C. Zeng, H. Tan, Z. Li, B. Li, and X. Y. Li, "Joint heterogeneous server placement and application configuration in edge computing," in *Proceedings of the 2019 IEEE 25th International Conference on Parallel and Distributed Systems*, Tianjin, China, January 2020.
- [10] K. Xiao, Z. Gao, W. Qian, and Y. Yang, "A Heuristic Algorithm Based on Resource Requirements Forecasting for Server Placement in Edge Computing," in *Proceedings of the 2018 IEEE/ACM Symposium on Edge Computing (SEC)*, Seattle, WA, USA, October 2018.
- [11] J. Zhou and X. Zhang, "Fairness-aware task offloading and resource allocation in cooperative mobile edge computing," *IEEE Internet of Things Journal*, 2021.
- [12] S. Pasteris, S. Wang, M. Herbster, and T. He, "Service placement with provable guarantees in heterogeneous edge computing systems," in *Proceedings of the 2019 IEEE International Conference on Computer Communications (IEEE INFOCOM 2019)*, Paris, France, May 2019.
- [13] S. Yang, F. Li, M. Shen, X. Chen, X. Fu, and Y. Wang, "Cloudlet placement and task allocation in mobile edge computing," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5853–5863, 2019.
- [14] M. Breitbach, D. Schäfer, J. Edinger, and C. Becker, "Context-aware data and task placement in edge computing environments," in *Proceedings of the 2019 IEEE International Conference On Pervasive Computing And Communications (PerCom. IEEE)*, pp. 1–10, Kyoto, Japan, March 2019.
- [15] R. Mahmud, S. N. Srirama, K. Ramamohanarao, and R. Buyya, "Quality of experience (qoe)-aware placement of applications in fog computing environments," *Journal of Parallel and Distributed Computing*, vol. 132, pp. 190–203, 2019.
- [16] R. Mahmuda, S. N. Sriramab, K. Ramamohanaraoa, and R. Buyya, "Profit-aware application placement for integrated fog-cloud computing environments," *Journal of Parallel and Distributed Computing*, vol. 135, pp. 177–190, 2020.
- [17] S. Hu and G. Li, "Dynamic request scheduling optimization in mobile edge computing for iot applications," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1426–1437, 2019.

- [18] K. Gao, Z. Cao, L. Zhang, Z. Chen, Y. Han, and Q. Pan, "A review on swarm intelligence and evolutionary algorithms for solving flexible job shop scheduling problems," *IEEE/CAA Journal of Automatica Sinica*, vol. 6, no. 4, pp. 904–916, 2019.
- [19] G.-H. Tzeng and J.-J. Huang, *Multiple Attribute Decision Making: Methods and Applications*, CRC Press, Boca Raton, FL, USA, 2011.
- [20] V. Balioti, C. Tzimopoulos, and C. Evangelides, "Multi-criteria decision making using TOPSIS method under fuzzy environment. Application in spillway selection," *Proceedings*, vol. 2, no. 11, 2018.
- [21] P. Strandmark, Y. Qu, and T. Curtois, "First-order linear programming in a column generation-based heuristic approach to the nurse rostering problem," *Computers & Operations Research*, vol. 120, Article ID 104945, 2020.
- [22] R. Bürgy, H. Michon-Lacaze, and G. Desaulniers, "Employee scheduling with short demand perturbations and extensible shifts," *Omega*, vol. 89, pp. 177–192, 2019.
- [23] A. Mseddi, W. Jaafar, H. Elbiaze, and W. Ajib, "Joint container placement and task provisioning in dynamic fog computing," *IEEE Internet of Things Journal*, vol. 6, no. (6), pp. 10028–10040, 2019.
- [24] F. Hong, H. Chen, B. Cao, and J. Fan, "A moead-based approach to solving the staff scheduling problem," in *Proceedings of the International Conference On Collaborative Computing: Networking, Applications And Worksharing*, pp. 112–131, Springer, Shanghai, China, October 2020.
- [25] I. Gurobi Optimization, *Gurobi Optimizer Reference Manual*, Gurobi Optimization LLC, Houston, TX, USA, 2018.
- [26] H. Badri, T. Bahreini, D. Grosu, and K. Yang, "Energy-aware application placement in mobile edge computing: A stochastic optimization approach," *IEEE Transactions on Parallel and Distributed Systems*, vol. 31, 2020.
- [27] Y. Guo, S. Wang, A. Zhou, J. Xu, J. Yuan, and C. H. Hsu, "User allocation-aware edge cloud placement in mobile edge computing," *Software: Practice and Experience*, vol. 50, no. 5, pp. 489–502, 2020.
- [28] S. L. Fang, "Cost-efficient resource provision for multiple mobile users in fog computing," in *Proceedings of the 2019 IEEE 25th International Conference on Parallel and Distributed Systems*, December 2019.
- [29] X. Yang, S. Zhou, and M. Cao, "An approach to alleviate the sparsity problem of hybrid collaborative filtering based recommendations: the product-attribute perspective from user reviews," *Mobile Networks and Applications*, vol. 25, no. 2, 2020.
- [30] Q. Luo, C. Li, T. H. Luan, and Y. Wen, "Optimal utility of vehicles in lte-v scenario: An immune clone-based spectrum allocation approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, pp. 1–12, 2018.
- [31] K. Peng, M. Zhu, Y. Zhang et al., "An energy-and cost-aware computation offloading method for workflow applications in mobile edge computing," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–15, 2019.
- [32] X. Xu, H. Cao, Q. Geng, X. Liu, and C. Wang, "Dynamic Resource Provisioning for Workflow Scheduling under Uncertainty in Edge Computing Environment," *Concurrency and Computation Practice and Experience*, 2020.

Research Article

GTF: An Adaptive Network Anomaly Detection Method at the Network Edge

Renjie Li ^{1,2,3} Zhou Zhou ^{1,2} Xuan Liu ^{4,5} Da Li ⁶ Wei Yang ^{1,2} Shu Li ^{1,2}
and Qingyun Liu ^{1,2,3}

¹Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

²National Engineering Laboratory for Information Security Technology, Beijing, China

³School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China

⁴College of Information Engineering (College of Artificial Intelligence), Yangzhou University, Yangzhou, China

⁵School of Computer Science and Engineering, Southeast University, Nanjing, China

⁶Department of Electrical and Computer Engineering, University of Missouri-Columbia, Columbia, USA

Correspondence should be addressed to Wei Yang; yangwei@iie.ac.cn

Received 22 September 2021; Accepted 17 November 2021; Published 20 December 2021

Academic Editor: Yuyu Yin

Copyright © 2021 Renjie Li 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 Anomaly Detection (NAD) has become the foundation for network management and security due to the rapid development and adoption of edge computing technologies. There are two main characteristics of NAD tasks: tabular input data and imbalanced classes. Tabular input data format means NAD tasks take both sparse categorical features and dense numerical features as input. In order to achieve good performance, the detection model needs to handle both types of features efficiently. Among all widely used models, Gradient Boosting Decision Tree (GBDT) and Neural Network (NN) are the two most popular ones. However, each method has its limitation: GBDT is inefficient when dealing with sparse categorical features, while NN cannot yield satisfactory performance for dense numerical features. Imbalanced classes may downgrade the classifier's performance and cause biased results towards the majority classes, often neglected by many existing NAD studies. Most of the existing solutions addressing imbalance suffer from poor performance, high computational consumption, or loss of vital information under such a scenario. In this paper, we propose an adaptive ensemble-based method, named GTF, which combines TabTransformer and GBDT to leverage categorical and numerical features effectively and introduces Focal Loss to mitigate the imbalance classification. Our comprehensive experiments on two public datasets demonstrate that GTF can outperform other well-known methods in both multiclass and binary cases. Our implementation also shows that GTF has limited complexity, making it be a good candidate for deployment at the network edge.

1. Introduction

In the past few decades, the Internet of Things (IoT) and cloud services have penetrated many aspects of our lives and served quantities of applications, for example, automated vehicles, medical applications, industrial IoT, and cloud data centers [1–4]. These emerging applications have shown considerable potential in improving the quality of life and network services. However, the proliferation of these new technologies also has led to an increasing trend of cyberspace attacks and other threats, making security concerns still hamper IoT adoption. Reportedly, the losses caused by cybercrime in the United

States exceeded \$4.2 billion in 2020 [5]. As a result, network security is a critical concern in our daily lives and business operations. There is an urgent need for efficient and reliable anomaly detection mechanisms to shield our network.

Traditional NAD methods, such as firewalls and rule-based Network Intrusion Detection Systems, are often insufficient to detect unknown attacks due to the inability to keep up with the most recent and sophisticated attacks. With the prevalent application of artificial intelligence, machine learning (ML), especially deep learning (DL), has attracted much attention in edge computing and cloud computing [6–10], due to its advantages in discovering

hidden patterns from vast amounts of data. ML/DL techniques are now widely used for the purpose of NAD, enhancing the security of the networking infrastructure and crucial data.

A typical ML/DL-based NAD method, which aims to detect anomalous network traffic by observing traffic data over time to distinguish potential attacks from normal traffic, usually takes the tabular data as the input and reads the data in CSV format. The tabular data consists of series of network traffic records, each of which is a network connection session (or a flow) and is labeled as either normal or a specific attack type. In particular, the tabular input means that the input features of a NAD method can have both categorical and numerical ones. For example, transaction protocol types and service types are usually regarded as categorical ones, while the duration and source/destination bytes are numerical values. Therefore, a classification model must be able to learn effectively with tabular input data. In general, among traditional ML methods, decision-tree-based ensemble methods (e.g., Gradient Boosting Decision Tree, GBDT [11]) dominate the use cases for tabular input data due to their superior performance. On the other hand, the deep learning methods are more preferred for unstructured input data (e.g., images, speech, and text) [12]. Because of its popularity and performance, this paper focuses on GBDT. While some recent researches confirm that GBDT is still the most accurate method on tabular data [13, 14], others claim to outperform GBDT [15, 16] or come within a hair's breadth of GBDT's performance [17]. In general, each of them holds its pros and cons dealing with tabular data.

On the one hand, GBDT has better effectiveness in handling dense numerical features than sparse categorical features. Like many other tree-based models, GBDT can automatically collect and combine the helpful numerical features to fit the training targets properly by picking the features with the most significant statistical information gain to build the trees [18]. Since categorical features are generally converted to high-dimensional and sparse one-hot encodings, GBDT will obtain small information gain on sparse features. As a result, GBDT cannot handle categorical features efficiently. In addition, GBDT and other tree-based methods are fast to train and have better interpretability. On the other hand, DL methods' advantage mainly lies in their capability in handling sparse categorical features by learning parametric embeddings to encode categorical features and their power in learning from large-scale data. The main limitation of DL methods, such as Fully Connected Neural Network, is their shortcoming in learning with dense numerical features directly, mainly because of complex optimization hyperplanes and the risk of falling into local optimums [19]. Therefore, DL methods cannot match the performance of GBDT in many tasks and datasets [15, 20].

Another challenge of the NAD task is the class imbalance of the real-world network traffic captured by edge devices [21], making it challenging for the classifier to make decisions on such skewed data distribution. In such cases, learning-based classification methods are always designed to achieve the highest overall accuracy, which may produce a bias towards the

majority class [22]. Similar scenarios also exist in other real-world applications, such as credit fraud detection [23] and medical diagnosis [24], but we focus on the NAD task at the network edge in this paper. Anomalies rarely occur, and normal data usually accounts for a large proportion. Furthermore, the minority class ordinarily carries the concepts with more significant interests than the majority class [25].

Accordingly, developing an adaptive method to address two major challenges of NAD tasks, that is, tabular inputting and imbalance problem, is desired. Inspired by some recent studies, we intend to combine Neural Networks and tree-based models to learn effectively from tabular data and introduce a well-designed loss function to deal with class imbalance. In this paper, we propose a novel method for the NAD task, called **GTF**, an ensemble of GBDT and TabTransformer enhanced with Focal Loss. We explored the GBDT2NN [26] and the TabTransformer-based classifier [17] to handle numerical features and categorical features, respectively, as shown in Figure 1. As for class imbalance, we utilize Focal Loss, which is proposed in the field of object detection for solving the extreme foreground-background class imbalance, which degrades the first-stage detector's performance [27], to deal with imbalanced traffic classification. Besides, all of these methods are first aimed at binary classification problems, and we extend them to the multiclass NAD task. In summary, the main contributions of our work are listed as follows:

- (i) We introduce a novel supervised NAD method with adaptive learning, named GTF, which improves the robustness and effectiveness for tabular data with class imbalance problems. Our method is applicable to various kinds of classification tasks but is particularly useful for NAD.
- (ii) We consider the tabular input data of NAD tasks and introduce two advanced models, that is, TabTransformer and GBDT2NN. Our proposal combines the advantages of GBDT and NN to handle both categorical and numerical features efficiently.
- (iii) By integrating Focal Loss, the proposed GTF can adapt to scenarios in which the performance suffers from class imbalance and compensate for the degradation of the classification model in such scenarios.
- (iv) We also propose an adaptive learning framework for GTF to automatically search for optimal parameters without the expert's experience. Experiments demonstrate that GTF could achieve superior results on two well-known NAD datasets, that is, KDD'99 and UNSW-NB15, and achieve robust performance in both multiclass and binary cases.
- (v) We evaluate the complexity of GTF in terms of computational requirements and runtime. Our analysis shows that GTF is really efficient and scalable. Thus, it is a good fit to deploy on constrained edge devices.

The rest of the paper is organized as follows. We summarize the related work in Section 2, followed by our proposed method in Section 3. In Section 4, we provide the

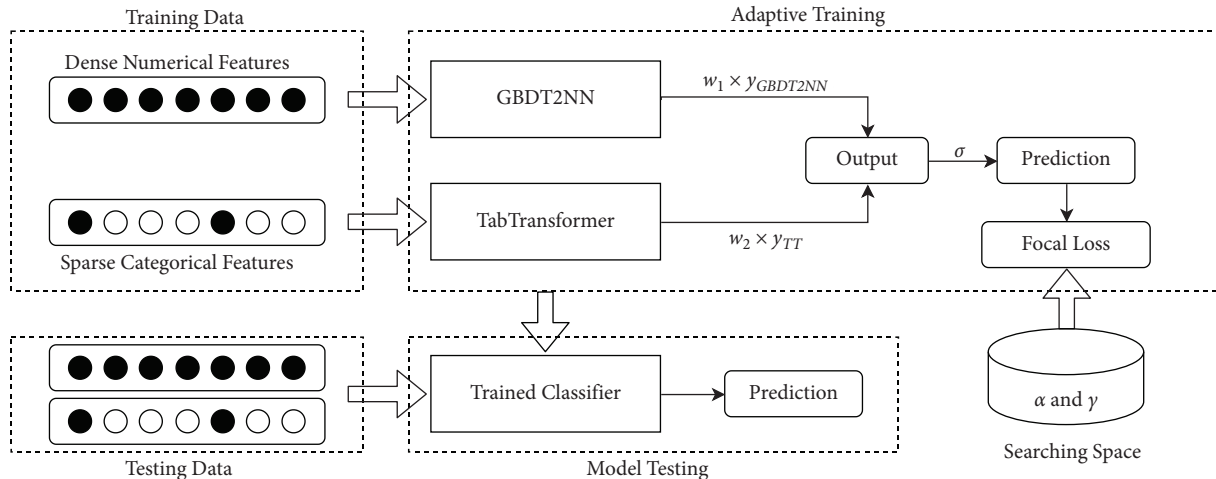


FIGURE 1: The framework overview of GTF. We use two modules to treat categorical and numerical features, respectively. The adaptive training module can learn optimal w_1 and w_2 through optimizer and find best α and γ used for Focal Loss from searching space automatically. For y_{TT} , TT represents Tab Transformer.

experimental details and results. Finally, we draw the conclusion in Section 5.

2. Related Work

As aforementioned, each of GBDT and Neural Network has its own weaknesses when facing the tabular data. Since sparse categorical features may impair the growth of trees in GBDT because of tiny statistical information gain, some methods require to encode categorical features into dense numerical values, which can be handled well by tree-based models. Some GBDT methods can directly take categorical features as their inputs, such as LightGBM [28] and CatBoost [29]. For example, CatBoost transforms categorical features to numerical before each split is selected in the tree by using various statistics on combinations of categorical features and combinations of categorical and numerical features. However, it may cause information loss. Binary coding [30] is another choice to encode features, which enumerates possible binary partitions of categorical features. But this method may cause overfitting and bring bias when there is not enough data in each category [28]. Neural Networks have been applied in many fields, but they are not well suited for tabular data. They mainly focus on the sparse categorical features and pay less attention to the dense numerical features. Although NN generally employs normalization [31] or regularization [12] for numerical features before the training phase, they usually cannot outperform GBDT and fail to find optimal solutions for tabular decision manifolds. For learning effectively with tabular data, some recent researches also try to combine the advantages of NN and GBDT. Although these methods are believed to have decision ability like trees to some extent, they mainly focused on computer vision or click prediction tasks rather than the NAD task with tabular inputting. Moreover, they may suffer from some disadvantages, like being inefficient and redundant.

Imbalance classification, also known as Imbalance Learning, has been one of the most challenging problems in

machine learning and deep learning. Many research works have been proposed to solve such problems and they can be summarized into three categories: data-level methods, algorithm-level methods, and cost-sensitive learning. To combat imbalance, typical algorithms adopt resampling techniques before training, such as SMOTE, ADASYN, NearMiss, and Tomek Link [32–35]. Most data-level methods have a distance-based design. On the one hand, resampling on large-scale data may lead to a high cost of computing the distance between samples. On the other hand, distance-based design may not be applicable for categorical features or missing values. Except for the time consumption of oversampling, undersampling may lose important information. Algorithm-level methods usually combine ensemble learning algorithms with advanced resampling techniques introduced to reduce the variance and they have achieved superior performance. But some of these ensemble methods are more time-consuming (e.g., SMOTEBagging and SMOTEBoost [36, 37]) and others have the risk of underfitting or overfitting (e.g., EasyEnsemble and BalanceCascade [38]). Cost-sensitive learning takes costs associated with the different classes into account. It mainly consists of two approaches: (1) assign the corresponding cost directly to each category and (2) employ metalearning during the training phase by preprocessing (usually data-level techniques) and postprocessing steps. However, some of them require a prerequisite of domain experts to set a cost matrix, and some have high computational complexity.

In summary, although there are increasing works that build more effective models and deal with skewed class distributions, most of them cannot completely solve the challenge of the NAD task (tabular input space and class imbalance). In this paper, we integrate NN and GBDT into a whole framework and adopt the advanced loss function to address the imbalance, which is suitable for real-world NAD datasets.

3. Methodology

In this section, we provide the formalized problem definition and our proposed method. Specifically, we focus on the imbalanced NAD task with tabular data as input. The whole framework, as the adaptive training module shows in Figure 1, consists of two components: TabTransformer for sparse categorical features and GBDT2NN for dense numerical features. We also introduce Focal Loss and adaptive tuning to guide the training phase. We will describe the details of each component in the following subsections.

3.1. Problem Definition. First of all, we only consider the input dataset in tabular format, which is very common in real-world applications at the network edge. Besides, we assume that there are n categories of network traffic, where $n \geq 2$ and at least one category is the normal network traffic class. Then, for the i -th category, we use N_i to denote its sample size. In this paper, we define the dataset as “an imbalanced dataset” when the sample sizes from different classes have wide ranges. In this paper, we use “majority classes” to refer to those with large sample sizes and “minority classes” to refer to other classes with much smaller sizes. Our ultimate goal is to improve the classification accuracy of minority classes without affecting the performance of overall classes.

3.2. TabTransformer for Categorical Features. Motivated by the initial success of Transformer [39] in NLP, Huang et al. adopted the idea to tabular data and proposed TabTransformer [17], which is an architecture that provides and exploits contextual embeddings of categorical features. Their study suggests that, for tabular data, TabTransformer can achieve comparable performance to tree-based ensemble approaches and outperform the state-of-the-art deep learning methods. As shown in Figure 1, we utilize TabTransformer’s advantage in handling categorical features, so we only use a part of its original structure. We remove the continuous features in the input, as well as the following normalization layer and concatenation layer related to these features. Figure 2 shows the architecture of TabTransformer used in this paper.

Generally speaking, TabTransformer comprises a column embedding layer, followed by a stack of N transformer layers, and a multilayer perceptron (MLP) before the loss function. Each transformer layer consists of a multihead self-attention layer followed by a position-wise feedforward layer. To learn categorical features more effectively, TabTransformer applies embedding technology on sparse vectors to get low-dimensional dense representation before stepping into transformer layers, denoted as

$$\mathbf{E}_\phi(\mathbf{x}_{\text{cat}}) = \{\mathbf{e}_{\phi_1}(x_1), \dots, \mathbf{e}_{\phi_m}(x_m)\}, \quad (1)$$

where \mathbf{x}_{cat} represents all the categorical features with x_i being i -th categorical feature. $\mathbf{e}_{\phi_i}(x_i)$ is corresponding embedding vector for x_i , which can be learned by back-propagation. Based on the above equation, the first transformer layer takes

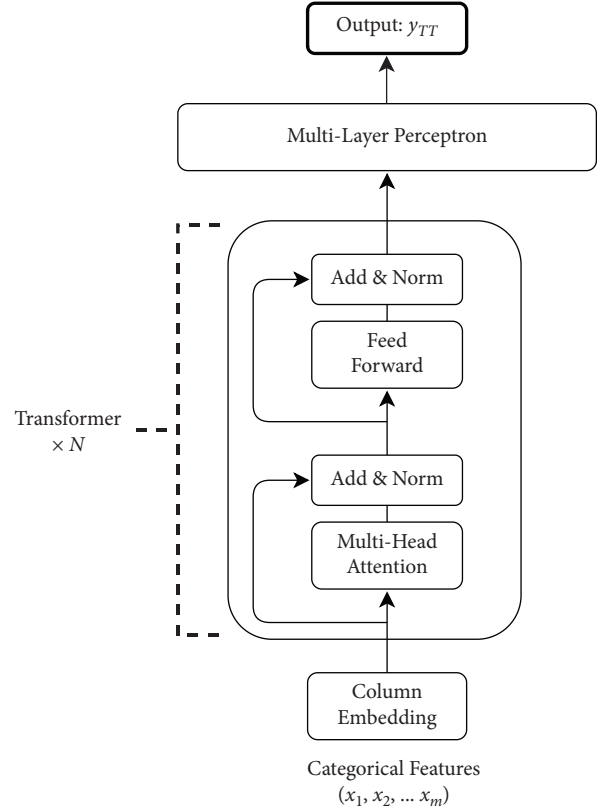


FIGURE 2: The architecture of TabTransformer.

$\mathbf{E}_\phi(\mathbf{x}_{\text{cat}})$ as its input, passes the output to the second transformer layer, and so forth. Unlike the original TabTransformer, we directly pass the output of the stack of transformer layers into an MLP to get the prediction. The prediction \mathbf{y}_{TT} can be formulated as follows:

$$\mathbf{y}_{TT}(\mathbf{x}_{\text{cat}}) = \mathcal{M}(f(\mathbf{E}_\phi(\mathbf{x}_{\text{cat}}); \boldsymbol{\theta}_1); \boldsymbol{\theta}_2), \quad (2)$$

where function f denotes N transformer layers, \mathcal{M} denotes the MLP, and θ_1 and θ_2 denote the parameters of two components.

3.3. GBDT2NN for Numerical Features. Gradient Boosting Decision Tree (GBDT) [11] is a widely used ensemble model of decision trees. In many application domains, it outperforms other machine learning algorithms such as Random Forest and Support Vector Machine. GBDT, as a tree-based gradient boosting algorithm, can build new trees by computing the information gain and fitting the residuals of previous trees. As mentioned in Section 2, GBDT’s strength lies in learning overdense numerical features but it fails to grow trees effectively using sparse categorical features. The path from the root node to the leaf node can build a decision rule, which can act as a vital cross feature. As a result, we choose GBDT to deal with numerical features.

While using GBDT alone is much easier, combining it with NN models is way more challenging. Most of the prior studies try to distill the trees of GBDT into an NN model but only transfer model knowledge in terms of the learned

function without considering other informational knowledges in the tree structure. In [26], Guolin et al. proposed a novel idea to efficiently distill the learned trees, called GBDT2NN, which could perfectly approximate the decision function and tree structure of GBDT with the help of the strong expressiveness ability of NN. For a single tree t , it can be distilled into an NN \mathcal{N} denoted as follows:

$$y^t(\mathbf{x}) = \mathcal{N}(\mathbf{x}[\mathbb{I}^t]; \boldsymbol{\theta}) \times \mathbf{q}^t, \quad (3)$$

where $\mathbf{x}[\mathbb{I}^t]$ is the input of \mathcal{N} , \mathbb{I}^t represents the used features given from GBDT, and θ is the parameter of \mathcal{N} . \mathbf{q}^t denotes the leaf values of tree and \mathbf{q}_i^t is the leaf value of i -th leaf. Since GBDT will get various trees after training, constructing an NN for each tree is very inefficient. In order to improve the efficiency, they proposed Leaf Embedding Distillation and Tree Grouping to downsize the scale of NNs. The Leaf Embedding Distillation adopts embedding technology and converts the one-hot representations of leaf indexes to dense vectors as the targets to be approximated in the learning process. The Tree Grouping divides the trees into k groups, and each group \mathbb{T} has $s = \lceil m/k \rceil$ trees, where there are m trees in total. Finally, the output of GBDT2NN can be denoted as

$$\mathbf{y}_{\text{GBDT2NN}}(\mathbf{x}) = \sum_{j=1}^k y_{\mathbb{T}_j}(\mathbf{x}), \quad (4)$$

where $y_{\mathbb{T}_j}(\mathbf{x}) = \mathcal{N}(\mathbf{x}[\mathbb{I}^{\mathbb{T}}]; \boldsymbol{\theta}^{\mathbb{T}})$, which represents the output of \mathcal{N}_j for j -th tree group.

3.4. Combination of TabTransformer and GBDT2NN. As described in previous subsections, we now own the output of TabTransformer and GBDT2NN. So, we are ready to combine them to perform end-to-end training. To get

prediction $\hat{\mathbf{y}}$ of the whole model, we assign different trainable weights that can be obtained from back-propagation, that is, w_1 and w_2 , for \mathbf{y}_{TT} and $\mathbf{y}_{\text{GBDT2NN}}$ as

$$\hat{\mathbf{y}}(\mathbf{x}) = \sigma(w_1 \times \mathbf{y}_{\text{GBDT2NN}}(\mathbf{x}) + w_2 \times \mathbf{y}_{TT}(\mathbf{x})), \quad (5)$$

where σ is the activation function for the last layer, for example, softmax for multiclass classification, and the loss value can be expressed as

$$\text{Loss} = \mathcal{L}(\hat{\mathbf{y}}(\mathbf{x}), \mathbf{y}), \quad (6)$$

where \mathbf{y} is the true label of sample \mathbf{x} and \mathcal{L} is the loss function.

3.5. Focal Loss. Focal Loss (FL) [27] is proposed to resolve the class imbalance in object detection tasks, and it is an improvement on the traditional cross-entropy (CE) loss. A proven ability of Focal Loss to solve the imbalance problem in the NAD task has been discussed in [40]. So, we also use FL as the loss function to focus on hard samples while avoiding the bias towards the easy samples. Hard samples are those in the training set which cannot be well predicted, and easy samples are the opposite. According to [27], for a binary classification task, FL is as follows:

$$FL = - \sum_{i=1}^m \alpha y_i (1 - \hat{y}_i)^\gamma \log(\hat{y}_i) + (1 - \alpha) (1 - y_i) \hat{y}_i^\gamma \log(1 - \hat{y}_i), \quad (7)$$

where \hat{y}_i represents the probabilistic predictions as defined in Section 3.4, y_i represents the labels of input samples, α is a balanced variant, $\gamma \geq 0$ is called *focusing parameter*, and m is the number of samples. When $\gamma = 0$, it turns into CE loss. For the multiclass classification task, we can use the concept of one-vs-all to extend FL as follows:

$$FL(\hat{y}_i, y) = -(\alpha y + (1 - \alpha)(1 - y)) \cdot (1 - (y \cdot \hat{y}_i + (1 - y) \cdot (1 - \hat{y}_i)))^\gamma \cdot (y \log(\hat{y}_i) + (1 - y) \log(1 - \hat{y}_i)), \quad (8)$$

where we assume that there are m samples and n classes, and then y is the one-hot encoding of the labels, and \hat{y}_i represents the probabilistic predictions with the size of (m, n) .

To obtain optimal α and γ , we also deploy adaptive training in the proposed framework by feeding different α and γ from the searching space into Focal Loss. According to [27], we set ranges of α and γ to be (0.25, 0.75) and (0.5, 5), respectively. In the training phase, we only need to choose a target metric, such as F1-score, and GTF can automatically search for the best parameters that yield the best performance. Such an adaptive training method enables GTF to be suitable for any scenarios and avoids the need for prior knowledge to set appropriate parameters.

4. Experiment

In this section, we will perform comprehensive evaluations of GTF on two public datasets and compare it with several

well-known methods. We will first describe the detailed experimental setup. Then, we will analyze the performance of GTF in both multiclass and binary cases to illustrate its effectiveness.

4.1. Experimental Setup. In this section, we will start with details about datasets and the evaluation criteria. Then, we will brief the comparison methods and ablation study and, finally, our implementation.

4.1.1. Dataset. To illustrate the effectiveness of our proposed method, we conduct experiments on two publicly available intrusion detection datasets, as listed in Table 1.

KDD Cup 1999 dataset [41], also known as KDD'99, is widely used by data mining techniques for the NAD task and includes a wide variety of intrusions simulated in a military network environment. It has been preprocessed into 41

features per network connection and consists of 5 categories of traffic. Besides the Normal traffic, there are 4 types of attacks: DoS (Denial of Service attacks), Probe (Scanning attacks), R2L (Remote to Local attacks), and U2R (User to Root attacks). Among the entire dataset, the majority class is DoS, which occupies 79.2% of the training set and 73.9% of the testing set. On the contrary, U2R only accounts for 0.1% of the training set and 0.2% of the testing set.

UNSW-NB15 dataset [42], published in 2015, is usually used as an alternative to KDD'99. Compared to KDD'99, it can better reflect modern low footprint attack scenarios and thus is more accurate to simulate the real-world traffic. Similar to KDD'99, the UNSW-NB15 dataset has 49 features (7 irrelevant features are removed and the reduced size of feature set is 42) and 9 types of attacks. The types of attacks are Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms.

Imbalance Ratio per Label (IRLbl) is a commonly used indicator to quantify the degree of class imbalance in a dataset. It calculates the ratio of the number of majority class i 's samples (N_{majority}) over the number of the class i 's samples (N_i) in the multiclass case, as shown as follows:

$$\text{IRLbl}_i = \frac{N_{\text{majority}}}{N_i}. \quad (9)$$

As for the binary case, we simply use *IR* because there only exists one minority class.

Both KDD'99 and UNSW-NB15 datasets are provided in CSV format and have different degrees of imbalanced class distributions. Tables 2 and 3 list the statistics of each dataset.

We consider both imbalanced binary and multiclass classification. In the binary case, we divide UNSW-NB15 into two categories: Normal and Attack. Then, we apply random sampling to the Attack class of the training set to construct datasets with different degrees of imbalance, where we set *IR* to 50, 100, 500, and 1000, respectively.

4.1.2. Implementation. We use scikit-learn (<https://scikit-learn.org/stable/index.html>), LightGBM (<https://lightgbm.readthedocs.io/en/latest/index.html>), imbalanced-ensemble (<https://github.com/ZhiningLiu1998/self-paced-ensemble>), CatBoost (<https://catboost.ai/>) and PyTorch (<https://pytorch.org/>) packages to implement these classifiers. We train these models with following parameters:

- (i) *Tree-Based Models.* We set the learning rate at 0.01, the number of trees at 128, and the max number of leaves at 10.
- (ii) *NN-Based Models.* We use AdamW optimizer with a learning rate of 0.001, a batch size of 1024, and the early stopping rounds of 20.
- (iii) *TabTransformer.* We set the embedding dimension at 32, the number of Transformer layers at 6, and the number of attention heads at 8.
- (iv) *GBDT2NN.* We decide to use 10 and 20 as fixed values for the number of tree groups and the leaf embedding dimension, respectively.

In order to simulate computationally constrained edge devices, we conduct all experiments on a laptop running Windows 10 with 8 GB RAM and a six-core Intel(R) Core(R) CPU. As in most papers, we perform 10-fold cross-validation for tree-based models and run all NN-based models five times with different random seeds.

4.1.3. Evaluation Criteria. Traditionally, accuracy metrics may have a bias towards the majority class and cannot reasonably reflect the model performance in our scenarios. As a result, we propose using the other evaluation criteria for both overall and individual metrics. All of these metrics are implemented in scikit-learn, a widely used Python library. In order to define our proposed criteria and their equations, let us use TP_i/FP_i to denote true/false positive and TN_i/FN_i to denote true/false negative for a given class i .

(1) *Individual Metrics.* To evaluate the performance on individual class, we consider Recall, Precision, and *F1*-score as individual metrics. They are defined in the equations below. Based on these equations, we can see that *F1*-score is a weighted average of the Recall and Precision and is usually considered as a trade-off between them.

$$\text{Recall}_i(R_i) = \frac{TP_i}{TP_i + FN_i},$$

$$\text{Precision}_i(P_i) = \frac{TP_i}{TP_i + FP_i}, \quad (10)$$

$$\text{F1-score}_i(F1_i) = 2 \cdot \frac{R_i \times P_i}{R_i + P_i}.$$

(2) *Overall Metrics.* To evaluate the overall performance in the multiclass case, we choose the Area Under the Receiver Operating Characteristic Curve (ROCAUC) and the Matthews Correlation Coefficient (MCC). ROCAUC shows the insensitivity of class imbalance (when *average* == 'macro' and *multi_class* == 'ovo' are set in scikit-learn). MCC is a correlation coefficient, whose value ranges from -1 to 1. A coefficient of 1 means a perfect prediction. Generally speaking, MCC is considered as an unbiased and more comprehensive metric for class-imbalanced tasks. In the binary case, we only use MCC as the overall metric.

$$\text{MCC} = \frac{TP \times TN - FP \times FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}. \quad (11)$$

4.1.4. Comparison Methods and Ablation Study. Since our goal is to address the imbalance issue in NAD tasks while learning effectively from tabular input data, we need to evaluate GTF based on these two scenarios. In order to conduct a comprehensive comparison and analysis, we use various models in the evaluation. First, we use LightGBM as our baseline due to its excellent performance and reliability. For NN-based models, we choose the original

TABLE 1: Details of the datasets used in experiments.

Dataset	Training	Testing	Numerical features	Categorical features
KDD'99	494 021	311 029	34	7
UNSW-NB15	175 341	82 332	37	5

TABLE 2: Class distribution and IRLbl of KDD'99.

	0		1		2		3		4	
	Num.	Num.	IRLbl ₁	Num.	IRLbl ₂	Num.	IRLbl ₃	Num.	IRLbl ₄	
Training	391 458	97 278	4.0	4107	95.3	1126	347.6	52	7528.0	
Testing	229 855	60 593	3.8	4166	55.2	16 345	14.1	70	3283.6	

*0: DoS, 1: Normal, 2: Probe, 3: R2L, and 4: U2R.

TabTransformer because it has been proven to be superior to recent deep Neural Networks for tabular data while matching the performance of tree-based ensemble models, like GBDT. For tree-based models, we include CatBoost, which could outperform other GBDT frameworks significantly and can handle categorical features very efficiently. Last but not least, we include two state-of-the-art methods for imbalance classification in NAD tasks. One is an algorithm-level method named Self-Paced-Ensemble (SPE [43]) and the other is a cost-sensitive method named FLAGB [40].

To prove the improvement brought by GTF, we also design two additional ablation experiments. In the first ablation experiment, we only use GBDT2NN without TabTransformer to evaluate the performance of GBDT2NN. As described in the preceding paragraph, TabTransformer has been tested separately, so we do not repeat it. In another ablation experiment, we weaken the GTF by removing Focal Loss to estimate its importance to GTF (represented by GT(F) in subsequent sections).

4.2. Results and Analysis. We first evaluate the performance of GTF in the multiclass case and show the results of both overall and individual comparisons on the two datasets in Tables 4 and 5, respectively. Note that the top-2 results are marked in bold. Due to the space limitation, we only present the most relevant metrics, that is, ROCAUC and MCC, for overall metrics and $F1$ for individual metrics. We also consider the binary case as described in Section 4.1.1 and show the experiment results in Figure 3. Lastly, we describe the results of the ablation study and give a computational complexity analysis of the proposed GTF.

4.2.1. Results on KDD'99. It can be seen that GTF outperforms other methods on both ROCAUC and MCC in the multiclass case, which explicitly indicates the advantage of our approach on imbalanced tabular data. Besides GTF, TabTransformer, GBDT2NN, and FLAGB also demonstrate enhancement on overall metrics. CatBoost and SPE achieve slightly better ROCAUC compared to baseline but worse performance on MCC. Compared to the baseline, GTF improves the ROCAUC (87.71% versus 76.79%) and MCC (82.46% versus 69.59%) simultaneously.

In terms of individual metrics, GTF/GT(F) improves the baseline significantly and beats other methods in three classes (0, 1, and 4). For class 3 and class 4, as shown in Table 2, all of their IRLbls in the training set are relatively large. Especially for class 4, $IRLbl = 7528$. Thus, the baseline cannot give a reliable prediction on minority classes and clearly demonstrates how the classifier's performance is negatively affected by the increased IRLbl. For instance, the $F1$ of baseline declines to 0 in class 4. The performances of TabTransformer and CatBoost also suffer from the large IRLbl. In class 3 and class 4, they both achieve 0 $F1$ -score. Interestingly, as far as class 3 and class 4 are concerned, SPE shows the opposite result compared to FLAGB and GTF. It performs best in class 3 but worst in class 4, while the other two perform better in class 4, mainly because of the ability of Focal Loss to focus on minority classes. Compared with FLAGB, GTF has an obvious improvement on $F1$ -score of all classes and boosts $F1_2/F1_3/F1_4$ by 2 to 3 times.

4.2.2. Results on UNSW-NB15. For the UNSW-NB15 dataset, although the numbers from GTF are not as eye-catching as those on KDD'99, it is still compelling enough as the metrics are either the best one or close to the best one. Regarding overall metrics, GTF achieves the best result on ROCAUC, which slightly improves the baseline (92.02% versus 91.11%), and the GTF's result on MCC is slightly worse than the baseline (69.87% versus 70.27%). Other methods, such as TabTransformer, do not yield any significant improvement on ROCAUC and achieve similar or worse performance on MCC. Such a situation also reflects on individual metrics. Overall, GTF is the most suitable method because it can boost ROCAUC the most without decreasing MCC. As far as individual metrics are concerned, GTF either performs better than the baseline or achieves very similar numbers. Its improvements on $F1_2$, $F1_8$, and $F1_9$ are maximum among all methods, which is the only one that can boost $F1$ on class 8 and class 9. Among all classes, GTF and SPE significantly outperform other methods in class 2, class 3, and class 5. These classes are relatively common in the training set, and their IRLbls are relatively low (all less than 50). It is counterintuitive to see the numbers, but it further confirms the supremacy of GTF.

TABLE 3: Class distribution and IRLbl of UNSW-NB15.

	0	1	2	3	4	5	6	7	8	9									
	Num.	IRLbl ₁	Num.	IRLbl ₂	Num.	IRLbl ₃	Num.	IRLbl ₄	Num.	IRLbl ₅	Num.	IRLbl ₆	Num.	IRLbl ₇	Num.	IRLbl ₈	Num.	IRLbl ₉	
Training	56 000	10 491	5.3	1746	32.1	12 264	4.6	33 393	1.7	2000	28.0	18 184	3.1	130	430.8	1133	49.4	40 000	1.4
Testing	37 000	3496	10.6	583	63.5	4089	9.0	11 132	3.3	677	54.7	6062	6.1	44	840.9	378	97.9	18 871	2.0

*0: Normal, 1: Reconnaissance, 2: Backdoor, 3: DoS, 4: Exploits, 5: Analysis, 6: Fuzzers, 7: Worms, 8: Shellcode, and 9: Generic.

TABLE 4: Comparison of metrics obtained by different methods for KDD'99. The results are expressed in %, and $F1_i$ means $F1$ -score in class i .

Model	Overall			Individual			
	ROCAUC	MCC	$F1_0$	$F1_1$	$F1_2$	$F1_3$	$F1_4$
Baseline	76.79	69.59	97.65	74.86	21.34	2.03	0
GTF	87.71	82.46	98.44	84.19	77.47	11.11	45.07
GT(F)	86.59	82.80	98.54	84.53	76.18	9.51	20.37
TabTransformer	79.58	82.33	98.39	84.45	81.31	0	0
GBDT2NN	80.19	82.04	98.41	83.70	76.53	9.60	20.90
CatBoost	82.23	61.86	91.29	71.84	76.50	0	0
FLAGB	85.31	69.98	95.96	78.64	39.87	3.40	21.13
SPE	81.04	64.92	97.70	66.67	19.34	14.22	1.36

Bold values represent top-2 results.

TABLE 5: Comparison of metrics obtained by different methods for UNSW-NB15. The results are expressed in %, and $F1_i$ means $F1$ -score in class i .

Model	Overall				Individual								
	ROCAUC	MCC	$F1_0$	$F1_1$	$F1_2$	$F1_3$	$F1_4$	$F1_5$	$F1_6$	$F1_7$	$F1_8$	$F1_9$	
Baseline	91.11	70.27	84.83	84.95	5.78	8.79	69.19	0	40.33	32.78	41.18	98.18	
GTF	92.02	69.87	82.44	84.13	11.57	24.91	69.42	3.14	38.37	36.36	47.78	98.35	
GT(F)	90.34	66.42	82.12	82.81	8.62	23.32	68.07	2.18	37.13	28.87	39.31	98.18	
TabTransformer	84.59	69.59	84.92	84.13	0	26.35	69.97	0	38.61	0	0	98.14	
GBDT2NN	70.36	55.42	77.87	25.93	3.25	22.30	58.38	5.50	26.47	0	0.67	92.63	
CatBoost	91.22	70.13	85.16	84.02	0.34	1.11	68.28	0	40.39	0	31.19	98.05	
FLAGB	91.04	70.17	84.87	85.01	5.24	8.61	68.93	0	40.14	43.75	39.44	98.15	
SPE	90.95	56.55	73.76	61.46	10.66	24.00	60.79	8.84	33.31	7.07	11.57	97.80	

Bold values represent top-2 results.

Based on the results, we can conclude that GTF can provide the best performance in the multiclass case with the comprehensive consideration of overall and individual metrics. It demonstrates that the proposed GTF can not only learn efficiently from tabular data but also mitigate the imbalance classification problem.

4.2.3. Overall Metric in the Binary Case among Different IRs.

Due to the limited space, we only show the overall metric of the binary case, that is, MCC, in Figure 3. The results indicate that the classifiers' performance generally shows a downward trend as the IR increases, and GTF outperforms other methods under all IRs. The performance of TabTransformer is the worst as it cannot distinguish Attack records from the Normal ones at all. The performance of CatBoost is very unstable, which is also lower than the baseline in most cases. FLAGB achieves good performance when $IR = 50$, but its performance drops dramatically when $IR \geq 100$. Both GTF and SPE outperform others regardless of the value of IR. From the figure, we also observe that GTF's performance is more stable (approximately within 20% range) for different IRs, compared to SPE. It is worth mentioning that SPE consumes about twice as much training time as GTF does in our experiments. Therefore, we can conclude that GTF can perform much better than other methods in the binary case while being fast enough.

4.2.4. Ablation Study. As shown in Tables 4 and 5 and Figure 3, neither TabTransformer nor GBDT2NN can achieve the best performance across all cases. What is worse is that, in some cases, these two models perform way worse than the baseline in terms of overall and individual metrics. On the contrary, in both multiclass and binary cases, GT(F) can beat TabTransformer and GBDT2NN on most metrics. For example, in Table 5, GT(F) can achieve good performance on $F1_7$ and $F1_8$, while both TabTransformer and GBDT2NN yield 0. Even though when GT(F) leads to worse performance compared to TabTransformer or GBDT2NN, such as $F1_4$ and $F1_5$ in Table 5, the achieved performance tends to be close to the best ones or above averages. This indicates that the combination of TabTransformer and GBDT2NN can improve the overall performance and prevent performance degradation in several cases.

Now we want to understand the impact of Focal Loss on the classification model by comparing GTF and GT(F). It is obvious to see that GTF outperforms GT(F) on almost all metrics, especially on the metrics to detect minority classes (e.g., $F1_3$ in Table 4 and $F1_7$ and $F1_8$ in Table 5). In some cases, such as $F1_4$ in Table 4, the Focal Loss leads to more than 100% improvement of the score. Another two interesting data points are $F1_2$ and $F1_3$ in Table 4. In these two cases, GT(F) is clearly underperforming compared to TabTransformer and GBDT2NN. But there is a big performance boost when the Focal Loss is added in GTF. For the overall

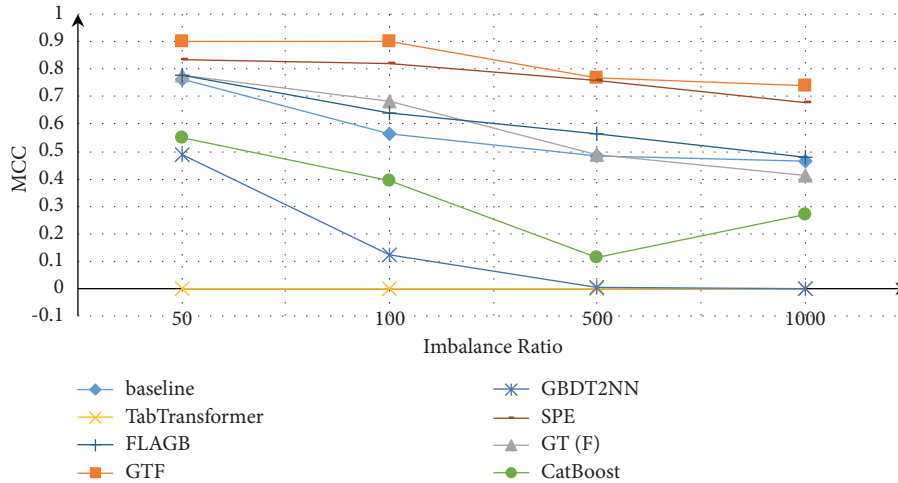


FIGURE 3: Overall metric in the binary case among different IRs.

TABLE 6: Computational complexity of GTF.

# of parameters	Batch size	MACs (M)	Inference time (milliseconds)
355,731	1	0.36	12.32
	1024	364.27	119.72

metrics in the binary case, we also observe more than 30% performance improvement on MCC when IR is 1000, as shown in Figure 3.

To summarize, all our results illustrate the effectiveness and performance improvement brought by GTF, which is a combination of TabTransformer, GBDT2NN, and Focal Loss to focus on minority classes.

4.3. Computational Complexity. Because edge devices usually have limited computation resources and memory, we also evaluate the complexity of GTF using (1) the number of multiply-accumulate operations (MACs, also known as MADDs) performed per inference, (2) the number of parameters, and (3) the inference time. We consider two batch sizes: 1 and 1024. The obtained results are displayed in Table 6. From these numbers, we can see that the number of parameters is less than one million, which is much less than some complex deep learning models. The MACs grow linearly with the batch size, but the inference time grows at a much slower rate. For instance, we notice that increasing the batch by 1000 times (from 1 to 1024) will only incur about a ten-time rise for inference time. When the batch size is 1 (single sample), the inference time can be as short as 12.32 ms. Thus, we can conclude that GTF is feasible to be deployed on constrained edge devices.

5. Conclusion

In this paper, we described the challenges of tabular input and class imbalance which exist in the nature of the NAD task. Based on the analysis of data characteristics, we propose a new method named GTF that combines the advanced

cost-sensitive algorithm and tabular learning strategy. Specifically, our proposal utilizes TabTransformer and GBDT2NN to handle categorical and numerical features, respectively. It also applies Focal Loss in the learning process to reduce the bias towards the majority classes. Powered by these components, GTF could gain powerful learning capability on tabular data while maintaining the ability to handle imbalance classification tasks. Compared to existing well-known models, our comprehensive experiments demonstrate that GTF can learn more effectively with tabular data and adapt to different imbalanced datasets in both multiclass and binary cases. Moreover, our implementation also shows that GTF is effective enough to deploy on constrained edge devices for NAD purposes.

Data Availability

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

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Acknowledgments

This work was supported by the Strategic Priority Research Program of the Chinese Academy of Sciences (no. XDC02030000), Jiangsu Planned Projects for Post-doctoral Research Funds (2021K402C), and Jiangsu Provincial Double-Innovation Doctor Program (JSSCBS20211035).

References

- [1] A. R. Javed, M. Usman, S. U. Rehman, M. U. Khan, and M. Sayad Haghighi, "Anomaly detection in automated vehicles using multistage attention-based convolutional neural network," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4291–4300, 2021.

- [2] A. Mohiyuddin, A. R. Javed, C. Chakraborty, M. Rizwan, M. Shabbir, and J. Nebhen, *Secure Cloud Storage for Medical Iot Data Using Adaptive Neuro-Fuzzy Inference System*, Springer, New York, NY, USA, 2021.
- [3] H. Gao, Xi Qin, R. J. D. Barroso, W. Hussian, Y. Xu, and Y. Yin, "Collaborative learning-based industrial iot api recommendation for software-defined devices: the implicit knowledge discovery perspective," *IEEE Transactions on Emerging Topics in Computational Intelligence*, pp. 1–11, 2020.
- [4] Y. Huang, H. Xu, H. Gao, X. Ma, and W. Hussian, "Ssur: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 670–681, 2021.
- [5] Federal Bureau of Investigation (Fbi), *Internet Crime Report 2020*, 2021, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.
- [6] Y. Zhu, W. Zhang, Y. Chen, and H. Gao, "A novel approach to workload prediction using attention-based lstm encoder-decoder network in cloud environment," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–18, 2019.
- [7] Y. Yin, Z. Cao, Y. Xu, H. Gao, R. Li, and Z. Mai, "Qos prediction for service recommendation with features learning in mobile edge computing environment," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 4, pp. 1136–1145, 2020.
- [8] H. Gao, K. Xu, M. Cao, J. Xiao, Q. Xu, and Y. Yin, "The deep features and attention mechanism-based method to dish healthcare under social iot systems: an empirical study with a hand-deep local-global net," *IEEE Transactions on Computational Social Systems*, pp. 1–12, 2021.
- [9] J. Xiao, H. Xu, H. Gao, M. Bian, and Y. Li, "A weakly supervised semantic segmentation network by aggregating seed cues: the multi-object proposal generation perspective," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 17, no. 1s, pp. 1–19, 2021.
- [10] Y. Xu, Y. Wu, H. Gao, S. Song, Y. Yin, and X. Xiao, "Collaborative apis recommendation for artificial intelligence of things with information fusion," *Future Generation Computer Systems*, vol. 125, pp. 471–479, 2021.
- [11] H. F. Jerome, "Greedy function approximation: a gradient boosting machine," *Annals of Statistics*, vol. 29, no. 5, 2001.
- [12] A. Kadra, M. Lindauer, F. Hutter, and J. Grabocka, "Regularization is all you need: simple neural nets can excel on tabular data," 2021, <https://arxiv.org/abs/2106.11189>.
- [13] L. Katzir, E. Gal, and R. El-Yaniv, "Net-dnf: effective deep modeling of tabular data," in *Proceedings of the International Conference on Learning Representations*, Addis Ababa, Ethiopia, May 2020.
- [14] L. Prokhorenkova, G. Gusev, A. Vorobev, A. V. Dorogush, and A. Gulin, "Catboost: unbiased boosting with categorical features," *Advances in Neural Information Processing Systems*, vol. 31, pp. 6638–6648, 2018.
- [15] S. Ö. Arik and T. Pfister, "Tabnet: attentive interpretable tabular learning," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 35, pp. 6679–6687, Vancouver, Canada, February 2021.
- [16] S. Popov, S. Morozov, and A. Babenko, "Neural oblivious decision ensembles for deep learning on tabular data," in *Proceedings of the International Conference on Learning Representations*, Jakarta, Indonesia, September 2019.
- [17] X. Huang, A. Khetan, M. Cvitkovic, and Z. S. Karnin, "Tabtransformer: tabular data modeling using contextual embeddings," 2020, <https://arxiv.org/abs/2012.06678>.
- [18] V. Sugumaran, V. Muralidharan, and K. I. Ramachandran, "Feature selection using decision tree and classification through proximal support vector machine for fault diagnostics of roller bearing," *Mechanical Systems and Signal Processing*, vol. 21, no. 2, pp. 930–942, 2007.
- [19] M. Fernández-Delgado, E. Cernadas, S. Barro, and D. Amorim, "Do we need hundreds of classifiers to solve real world classification problems?" *Journal of Machine Learning Research*, vol. 15, no. 1, pp. 3133–3181, 2014.
- [20] T. Chen and C. Guestrin, "XGBoost," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, August 2016.
- [21] S. S. Meriem Amina, B. Abdolkhalegh, N. Kim, and C. Mohamed, "Featuring real-time imbalanced network traffic classification," in *Proceedings of the 2018 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)*, IEEE, Halifax, Nova Scotia, Canada., July 2018.
- [22] H. Guo, Y. Li, J. Shang, G. Mingyun, H. Yuanyue, and G. Bing, "Learning from class-imbalanced data: review of methods and applications," *Expert Systems with Applications*, vol. 73, pp. 220–239, 2017.
- [23] A. Dal Pozzolo, G. Boracchi, C. Olivier, C. Alippi, and G. Bontempi, "Credit card fraud detection: a realistic modeling and a novel learning strategy," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 8, pp. 3784–3797, 2018.
- [24] D. Gamberger, N. Lavrac, and C. Groseelj, "Experiments with noise filtering in a medical domain," *ICML*, vol. 99, pp. 143–151, 1999.
- [25] H. He and Y. Ma, *Imbalanced Learning: Foundations, Algorithms, and Applications*, Wiley-IEEE Press, Hoboken, NJ, USA, 1st edition, 2013.
- [26] K. Guolin, Z. Xu, J. Zhang, B. Jiang, and T.-Y. Liu, "DeepGBM," in *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, ACM, Anchorage, AK, USA, July 2019.
- [27] T.-Yi Lin, P. Goyal, R. Girshick, K. He, and P. Dollár, "Focal loss for dense object detection," in *Proceedings of the 2017 IEEE International Conference on Computer Vision (ICCV)*, October 2017.
- [28] K. Guolin, M. Qi, and T. Finley, "Lightgbm: a highly efficient gradient boosting decision tree," *Advances in Neural Information Processing Systems*, vol. 30, pp. 3146–3154, 2017.
- [29] A. V. Dorogush, V. Ershov, and A. Gulin, "Catboost: gradient boosting with categorical features support," 2018, <https://arxiv.org/abs/1810.11363>.
- [30] J. Friedman, T. Hastie, and R. Tibshirani, *The elements of statistical learning*, Springer series in statistics, New York, NY, USA, 2001.
- [31] Sergey Ioffe and C. Szegedy, "Batch normalization: accelerating deep network training by reducing internal covariate shift," in *Proceedings of the International conference on machine learning*, pp. 448–456, PMLR, Lille, France, July 2015.
- [32] I. Mani and I. Zhang, "Knn approach to unbalanced data distributions: a case study involving information extraction," in *Proceedings of the workshop on learning from imbalanced datasets*, vol. 126, ICML United States, Washington, DC, USA, August 2003.

- [33] I. Tomek, "Two modifications of CNN," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. SMC-6, no. 11, pp. 769–772, 1976.
- [34] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: synthetic minority over-sampling technique," *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, 2002.
- [35] H. He, B. Yang, E. A. Garcia, and S. Li, "Adasyn: Adaptive synthetic sampling approach for imbalanced learning," in *Proceedings of the 2008 IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence)*, IEEE, Hong Kong, China, June 2008.
- [36] S. Wang and X. Yao, "Diversity analysis on imbalanced data sets by using ensemble models," in *Proceedings of the 2009 IEEE Symposium on Computational Intelligence and Data Mining*, March 2009.
- [37] N. V. Chawla, A. Lazarevic, L. O. Hall, and K. W. Bowyer, "SMOTEBoost: improving prediction of the minority class in boosting," in *Knowledge Discovery in Databases: PKDD 2003* vol. 107–119, Berlin, Germany, Springer, 2003.
- [38] Xu-Y. Liu, J. Wu, and Z.-H. Zhou, "Exploratory under-sampling for class-imbalance learning," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 39, no. 2, pp. 539–550, 2009.
- [39] A. Vaswani, N. Shazeer, N. Parmar et al., "Attention is all you need," in *Advances in Neural Information Processing Systems*, pp. 5998–6008, Springer, New York, NY, USA, 2017.
- [40] Yu Guo, Z. Li, Z. Li, G. Xiong, M. Jiang, and G. Guo, "FLAGB: Focal loss based adaptive gradient boosting for imbalanced traffic classification," in *Proceedings of the 2020 International Joint Conference on Neural Networks (IJCNN)*, July 2020.
- [41] KDD Cup 1999 Data, 2021, <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>.
- [42] N. Moustafa and Jill Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS)*, November 2015.
- [43] Z. Liu, W. Cao, Z. Gao et al., "Self-paced ensemble for highly imbalanced massive data classification," in *Proceedings of the 2020 IEEE 36th International Conference on Data Engineering (ICDE)*, April 2020.

Research Article

BEvote: Bitcoin-Enabled E-Voting Scheme with Anonymity and Robustness

Ning Lu,^{1,2} Xin Xu,¹ Chang Choi ,³ Tianlong Fei,¹ and Wenbo Shi¹

¹College of Computer Science and Engineering, Northeastern University, Shenyang, China

²School of Computer Science and Technology, Xidian University, Xi'an, China

³Department of Computer Engineering, Gachon University, Seongnam 13120, Republic of Korea

Correspondence should be addressed to Chang Choi; changchoi@gachon.ac.kr

Received 18 September 2021; Revised 8 November 2021; Accepted 24 November 2021; Published 15 December 2021

Academic Editor: Honghao Gao

Copyright © 2021 Ning 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.

When building the large-scale distributed decision control system based on mobile terminal devices (MTDs), electronic voting (E-voting) is a necessary technique to settle the dispute among parties. Due to the inherent insecurity of Internet, it is difficult for E-voting to attain complete fairness and robustness. In this study, we argue that Bitcoin blockchain offers better options for a more practical E-voting. We first present a coin mixing-based E-voting system model, which can cut off the relationship between the voter's real identity and its Bitcoin address to achieve strong anonymity. Moreover, we devise a secret sharing-based E-voting protocol, which can prevent voting number from being leaked ahead and further realize strong robustness. We establish the probable security theory to prove its security. In addition, we use the experimental evaluation to demonstrate its efficiency.

1. Introduction

1.1. Background and Motivation. Over the past two years, the rapid development of mobile edge computing (MEC) gives mobile terminal devices (MTDs) more computation and communication resource [1, 2], which produces the prospect of large-scale distributed decision control system based on MTD. For example, with the portable service of MTD, the medical intelligent diagnosis system allows multiple medical teams to carry out the consultation at any time and any place, which can effectively alleviate the burden of regional healthcare system caused by the emergent disaster (e.g., COVID-19); as MTD becomes more widespread, the intelligent property management system encourages more property owners to directly participate in community affairs, which facilitates the reduction in management costs, as well as the enhancement of management quality. It is widely known that in the distributed decision control system, settling the dispute among parties is an essential task. For example, in the multidisciplinary team (MDT)-based diagnosis treatment model, doctors usually have a disagreement in treatment plans for patients; in property

management, different owners usually have different preferences, and among them, it is difficult to reach an agreement. In this case, electronic voting (E-voting), as a common means of settling such dispute (i.e., collecting the wish of each individual to evaluate group overall preference), is a necessary technique when building the large-scale distributed decision control system.

To improve the decision quality, besides the correctness of ballot counts, E-voting still needs to ensure the secrecy of ballots and protect the identity privacy of voters. Yet, due to the inherent insecurity of the Internet, it is easy for attackers to undermine the fairness of E-voting and leak the voters' identity privacy. For example, at DEFCON 25, hackers can easily invade the voting system to tamper with the data [3]. This would pose a serious security risk to the whole distributed decision control system. The advent of blockchain, however, offers a new appealing option to support E-voting service over the Internet [4]. It provides an opportunity to design an E-voting system that satisfies the above requirements. For instance, the traceability of each transaction in blockchain increases the feasibility of the verifiability for voting results; with the transparency of transactions,

blockchain-based E-voting would be equipped with the open-audit ability; the tamper-resistant nature of blockchain can effectively improve the voter confidence of voting; the pay-per-use nature of blockchain service provides incentives to encourage organizers to deploy voting service [5, 6]. It is well known that Bitcoin, the most widely used electronic cryptocurrency, owes its success to the fact that its online trading platform is built on blockchain. In this, to help lower costs, migrating traditional voting solutions to the Bitcoin platform becomes more of a natural and practical choice.

There are, however, two challenges in the implementation of Bitcoin-enabled E-voting, particularly if we also take into consideration the openness of decision control system and the constantly evolving threat landscape.

- (i) *Anonymity*. To eavesdrop on the identity privacy of voters and further change their decisions to affect the fairness of the vote, the attackers may guess the true identities of transaction parties in blockchain. Bitcoin allows the input or output address that is not associated with user's real identity to conduct a transaction, but the sophisticated hackers can still infer their identities through clustering analysis of the transaction data. In this, Bitcoin is actually pseudo-anonymous. To guarantee the anonymity of the voter during voting process, although some relevant schemes based on zero-knowledge proofs or double envelope encryption have been proposed [7, 8], identity privacy can still be leaked through analyzing the voter-ballot relationship, once the voting result is announced. Therefore, how to enhance anonymity to ensure fairness becomes our first technical challenge.
- (ii) *Robustness*. To pursue their own self-interest, even at the expense of others, the unscrupulous candidate would bypass the E-voting system to influence the voting result. For example, to illegally gain more voting rights, stakeholders can forge numerous virtual voters; to induce voters to make nonobjective judgments, attackers may eavesdrop and expose the ballots that any candidate has received during the voting process. Recently, there are more researches for E-voting, but research on its robustness has long been neglected. For example, Jason et al. utilize the prepaid Bitcoin cards to serve as voting rights, but do not give a secure way to distribute them [9]; Bistarelli et al. introduce tokens as ballots, which can be straightly voted for expected candidates at the cost of the leakage of voting process information [10]. Therefore, E-voting for decision control system includes a mechanism to resist such misbehaved candidate, which becomes our second technical challenge.

1.2. Proposed Scheme. To provide a better electronic voting service and address the above challenges, we propose a more secure Bitcoin-enabled E-voting scheme termed as BEvote. In contrast to existing similar work, BEvote attempt to

implement the functions is shown in Table 1. In particular, in our scheme, we introduce a coin mixing-based system model, in which Bitcoin is viewed as ballot and the buyer and the seller in a transaction, respectively, represent the candidate and the voter. To achieve strong anonymity, we use coin mixing technique to cut off the relationship between the voter's real identity and its Bitcoin address before voted, and meantime, this anonymous address would be used in the entire voting process. To reduce the cost and improve the credibility, we use the Bitcoin blockchain to store voting data and execute the preset condition. To keep the voting numbers private during the whole voting process and thus achieve strong robustness, we adopt the joint Shamir random secret sharing technique, which can render the voting rights to be safely distributed to each voter.

The contributions of this study are regarded as the following to be threefold:

- (i) The proposed BEvote abstracts a Bitcoin transaction as the voting process. Meantime, coin mixing is used to separate Bitcoin address from the real identity of voter, to achieve strong anonymity.
- (ii) We devise a secret sharing-based E-voting protocol to realize the secure distribution of voting rights, which can prevent voting number from being leaked ahead.
- (iii) We use security analysis to prove BEvote's anonymity and robustness. In addition, we conduct comprehensive simulations to demonstrate its efficiency.

The remainder of this study is organized as follows. Section 2 introduces relevant background materials and the related literature. Section 3 depicts the overall design of our scheme and then points out what specific threats it would face. Section 4 proposes a secure E-voting protocol to solve them. Sections 5 and 6, respectively, carry out security analysis and simulation evaluations. Section 7 summarizes the study.

2. Background and Relevant Literature

2.1. Electronic Voting Problem definition. To make all parties reach a consensus on important issues and take action to maintain consistency, electronic voting (E-voting) follows the principle that the minority is subordinate to the majority and derives the results based on the choices of voters. Assume that there are m candidates $\tilde{C} = \{C_1, C_2, \dots, C_m\}$ and n voters $\tilde{U} = \{U_1, U_2, \dots, U_n\}$. E-Voting needs to implement the function of n voters to choose one winner anonymously among m candidates, where the criteria for this winner are to gain at least k ballots. The voting procedure $V(\tilde{C}, \tilde{U})$ can be formalized as follows:

$$V(\tilde{C}, \tilde{U}) = f_1(\tilde{U}) \cdot f_2(\tilde{C}), \quad (1)$$

where $f_1(\tilde{U})$ is used to vote on the candidates and $f_2(\tilde{C})$ is used to collect ballots and generate statistics on them. Given $C_i \in \tilde{C}$, when $f_2(C_i) > k$, we have the winner C_i .

TABLE 1: Function comparison between BEvote and previous work.

	[7]	[8]	[9]	[10]	[11]	[12]	BEvote
Strong anonymity	N	N	N	Y	Y	Y	Y
Robustness	Y	Y	N	N	Y	N	Y

- (i) *Anonymity*. To protect the voters' safety, their identities should never be revealed throughout the voting stage.
- (ii) *Validity*. In the event that adversaries tend to disguise their identity as system roles (e.g., voter or candidate) in attempts to participate in voting, there must be a mechanism to identify these forged roles.
- (iii) *Robustness*. In any case, the voters cannot hold more voting rights than their own calculations would deem necessary. Thus, we need to prevent the Sybil attack and ballot forgery.
- (iv) *Fairness*. To guard against bias, whether the voters or candidates, they cannot know ballot numbers before the end.
- (v) *Receipt-free*. To prevent ballot trafficking, the bribed voters cannot prove to the candidate that they had the right to vote in advance.
- (vi) *Verifiability*. Considering that the sophisticated attackers may tamper with the identity information of candidates, the entire voting process could be verified by any entity.
- (vii) *Scalability*. With the scale of decision control system enlarging day by day, both voter numbers and candidate numbers should not be restricted by the performance issues.

2.2. Related Work. In recent years, as the distributed decision control system got more popular, the electronic voting problem has become a research hot spot. So far, several E-voting schemes have been proposed. For example, Chaum et al. proposed an E-voting protocol, which provided a secure transmission scheme for voting using Web applications such as email [13]; Adida et al. proposed an open-audit voting system that any willing observer can audit the entire process [14]; and Chondros et al. utilized a distributed subsystem to solve the single point of failure problem of E-voting [15]. In addition, Veronique et al. explained the verifiability notions of E-voting protocols [16]. Nevertheless, Candidates may bribe voters, which leads to collusion attacks, which is a sociological puzzle that cannot be technically solved. Benaloh et al. proposed the notion of receipt-free to comply with, which can prevent collusion to some extent [17]. Due to the lack of a trusted third party, the above schemes are difficult to realize the efficiency and fairness of voting.

Since the birth of blockchain technology, its anonymity and public verifiability have been proved to meet the need of the secure multiparty computation scenario [18]. Meantime, E-voting requires multiple parties to make a joint decision without revealing the privacy of voters and

ballots, which is a typical secure multiparty computation scenario [19]. So far, there have been attempts to design the E-voting schemes based on blockchain platforms, including Ethereum and Zcash [20–23]. As is well known, the supreme status of Bitcoin blockchain is hard to shake, although other existing blockchain platforms have better technical characteristics in certain aspects. This is also the main reason why the upper layer protocols such as the Bitcoin lightning network that optimizes and enhances Bitcoin's performance and functions are still booming [24]. Therefore, this study mainly focuses on investing in Bitcoin-enabled E-voting schemes.

Depending on whether the coin mixing is used, existing Bitcoin-enabled E-voting protocols are classified as "with coin mixing" or "without coin mixing."

2.2.1. Bitcoin-Enabled E-Voting Schemes without Coin Mixing. Zhao et al. earlier utilized Bitcoin blockchain to design an E-voting protocol [7], which requires additional stages to distribute secret random numbers through the zero-knowledge proof algorithm zk-SNARKs. However, it can only distribute random numbers for two candidates, which results in the protocol only supporting 1-of-2 voting. Besides, all voters need to construct a reveal transaction before voting, which is exposed to the public. Because that associates the ballots with the voter, the candidate can know whether any voter has voted for him, which leads to the loss of anonymity. Jason et al. proposed a kind of card that contains prepaid Bitcoin addresses and corresponding private keys, in which regulators can place the PBC in an envelope when it is issued to ensure that it cannot be traced back to voters [9]. Nevertheless, this way of distributing physical objects runs counter to the original intention of E-voting to save manpower and material costs. Moreover, electronic virtual cards could be used, but failed to come up with a plan that would guarantee the anonymous distribution of cards. Furthermore, it cannot prevent dishonest staff from disclosing information related to cards and voters, and meet the requirements of voting anonymity. Adiputra et al. proposed to combine Bitcoin blockchain and the double envelope encryption technique for E-voting [8]. However, the public key to encrypt all the ballots generated by the electoral commission can only guarantee the anonymity of the voter during the voting process. Once the electoral commission releases the private key, the voter and the ballot would be associated. Thus, this scheme has serious anonymity issues. In addition, Bitcoins cannot be redeemed even if the vote fails, so the robustness is poor. Besides, the electronic commission equivalent to the supervisor of our protocol is responsible for too many tasks, which leads to the scheme being too centralized. Zhang et al. proposed the chaintegrity protocol. It utilizes a blind signature to ensure the anonymity and can only be used in permissioned chains without transaction fees [25]. The reason for this is that prepaid transaction fees can be associated with the user's identity. In addition, the so-called platform-independent feature is not established since it does not support permissionless blockchains, particularly Bitcoin. To sum up,

coin mixing is necessary for Bitcoin-enabled E-voting scheme.

2.2.2. Bitcoin-Enabled E-Voting Schemes with Coin Mixing. Bartolucci et al. designed a share-based blockchain voting scheme called SHARVOT [11], which utilizes the circle shuffle to obfuscate the relationship between the ballots and the voter’s identity. However, considering that the size of the transaction data in the Bitcoin protocol is limited, the P2SH script corresponding to each unlock condition of the vote commitment transaction needs to contain all the ballots obtained by a candidate, which makes the multi-signature used in the P2SH script have only 15 public key positions. This means that, after excluding the two required public key positions, a maximum of 13 ballots can be placed, which leads to a $n < 13m$ limit between the maximum number of voters n and the number of candidates m . It also limits the maximum number of shares to reconstruct private key to 13. These restrictions make SHARVOT unable to meet the requirements of multiple candidates and multiple voters. Takabatake et al. adopted Zerocoin to assist Bitcoin to provide anonymity for voting, in which Zerocoin can be used to obtain a zero-knowledge commitment before it can be exchanged for a new Bitcoin address [12]. However, the Zerocoin blockchain is not compatible with Bitcoin. Using two kinds of blockchains would greatly increase the complexity of actual operations. In addition, the ballots are placed directly in the OP_RETURN field of the Bitcoin output script. All the ballots need to be checked to count the winners. The efficiency is lower when the voting scale is larger. Bistarelli et al. proposed an end-to-end Bitcoin voting platform, which utilizes anonymous Kerberos to conceal the relationship between the Voter’s identity and the Bitcoin address, as well as uses tokens to represent the ballots [10]. Nevertheless, voters sending tokens directly to the candidates through a public Bitcoin transaction would cause severe consequences. Since all transactions cannot be packaged into new blocks by miners at the same time, the voters could know the current number of ballots of any candidate by the number of tokens received. The leakage of the voting situation tremendously damages the fairness of voting. In short, the above schemes are not applicable for the large-scale distributed decision control system due to their deficiency in anonymity and scalability.

3. Bitcoin-Enabled E-Voting Scheme

In this section, we introduce the system model and the functionality of system components. Afterwards, we present the potential threats faced by BEvote and defer their solutions in Section 3. Table 2 lists the notations in our paper.

3.1. Motivation and Assumptions. We exploit the Bitcoin blockchain platform for implementing voting. Both verifiability and scalability requirements are considered as the main limiting factors for electronic voting in large-scale distributed decision control system. However, over time, technology advances increase the feasibility of large-scale

TABLE 2: Notations used to describe the BEvote design.

Notation	Description
U_i	The Voters
C_j	The Candidates
v_i	Ballots of U_i
$(pu_i, pr)_i$	The public/private key pair of Voters
(PU_j, PR_j)	The public/private key pair of Candidates
(P, S)	The public/private key pair of secret sharing
s_i	The secret shares
p_i	The public key share of s_i
G	Basic point of elliptic curve
$VoteTx_i$	Voting transactions of U_i
$WinTx_j$	Winning transactions of C_j
$RefundTx_i$	Refund transactions of U_i
ABA_i	Anonymous Bitcoin addresses of U_i
AVL	Anonymous voters list
ID_{C_j}	Identity number of C_j
info	Identity information
Reg	Registration
Enc	Encryption
Sig	Signature
T	Timeout time

E-voting solution. Along with the spreading of blockchain in secure multiparty computation, researchers start to propose the blockchain-enabled E-voting, where the digital transaction process is abstracted as one voting. In traditional E-voting, it is hard to achieve high availability and open verifiability simultaneously. Yet, by virtue of the traceability in blockchain, they are readily available. Going a further step, to allow more people to participate in voting and verify results, Bitcoin blockchain, as a public trading platform with daily business transaction of up to 500 million USD, is an appealing option. In this, the scalability of E-voting could also be ensured. In addition, the pay-per-use nature of transaction service encourages the Bitcoin platform to support voting service. Consequently, it is not only technically sound but also economically preferable to migrate E-voting to Bitcoin blockchain platform.

We make a few assumptions to assist BEvote’s design, part of which have already been supported by the current blockchain technologies, while others can be satisfied through existing research:

- (1) We assume that the blockchain generates new blocks at fixed intervals without forks.
- (2) We assume that the data in the blockchain are always public auditable, while the entire transaction history can always be read. However, only if valid transactions are submitted and the consensus is obtained the blockchain can be written.
- (3) We assume that no adversary can destroy the blockchain’s proof of work consensus mechanism. This means that the data cannot be tampered with.

3.2. System Model. Although Bitcoin blockchain adopts the pseudonym mechanism that tries to achieve exchange anonymous security, the sophisticated attackers still alone utilize the simple analysis technology to analyze all

transactions that are transparently recorded in any one of the chain nodes, which could infer the true identities of transaction parties. In this case, utilizing Bitcoin blockchain directly cannot guarantee the strong anonymity of E-voting. To solve such an issue, coin mixing becomes the natural choice, providing a service that obfuscates the ownership of Bitcoin to interrupt the interlinkage of transaction parties. However, the traditional coin mixing usually engages a set of chain nodes as middlemen and then allows them to combine multiple transactions into one transaction, which significantly affects its scalability, considering Bitcoin's maximum transaction size. Apparently, it is not applicable for the large-scale E-voting system, because on one hand the smaller size anonymous set cannot support strong anonymity for E-voting and on the other hand the large computation overhead degrades the efficiency of voting. For this, we have proposed a scalable coin mixing scheme [26, 27], which breaks down the trading process into transferring stage and paying stage. The former deposits the transaction Bitcoins on a specified middleman (termed as holding Mixer) and further cuts off the link between these Bitcoins and the seller; the latter specify another middleman (termed as Paying Mixer) to advance the Bitcoins to buyer and then pay back the Bitcoins to this middleman after the mixing is over. In doing so, we can not only improve the size of anonymous set but also improve the execution efficiency, which can satisfy the requirement of large-scale mixing Bitcoins. Based on it, we embed such coin mixing into our E-voting scheme.

In Bitcoin-enabled E-voting, each voting can be abstracted as a transaction, where the voter and candidate can be viewed as the buyer and the seller, respectively. Moreover, the voter requires two Mixers to interrupt its interlinkage with the candidate before voting, which could facilitate concealing the voter's identity during the entire voting stage. Furthermore, motivated by superior returns, abundant chain nodes are willing to provide mixing service and serve as Mixers. Meantime, to achieve flexibility, any system role is allowed to enter or exit at any time. In this case, compared with decentralization, a completely centralized structure is more efficient, which could reduce the expense of management. Guided by these principles, as depicted in Figure 1, we devise a three-tiered system model based on coin mixing. In data persistence tier, all the status information related to voting (including the course and the result) would be recorded in Bitcoin blockchain; in business tier, Voters, Mixers, and Candidates, as partners, would be scheduled in a fixed order so as to realize the voting task; in management tier, all system roles should be centrally controlled with great care.

- (i) *Supervisor* provides functionality for validating each requester's qualifications, including *Voter*, *Candidate*, and *Mixer*. It would maintain a member list for each system role. Once monitoring any bad behavior, it excludes this member from the corresponding list. In addition, it also provides *Mixer* recommendation service for *Voters*. Generally, it is authorized by the government.

- (ii) *Voter* is the one that could obtain voting rights. This means that it can generate ballots and vote for its desired candidates.
- (iii) *Candidate* is the one who is voted. When the polls close, the candidate with the most ballots wins.
- (iv) *Mixers* provide functionality for concealing voters' identities, in which holding Mixer is used to host the voter's Bitcoins, and trading Mixer is used to transfer them to the specified candidate.
- (v) *Bitcoin blockchain* is utilized as an infrastructure for data storage. It would record all information relating to the state of voting in an anonymous and tamper-resistant manner.

Under the ideal network environment, the workflow of BEvote can be stated as follows:

- (i) *Step 1. Registering*: Each participant (including *Voter*, *Mixer* and *Candidate*) is required to submit registration request to *Supervisor*. Only successful registration can provide relevant functions.
- (ii) *Step 2. Confusing Voter's identity*: Each *Voter* has two Bitcoin addresses: an original address that contains Bitcoins and a brand new address without Bitcoins. To mix its identity with others, it resorts to *Mixer's* mix coin strategy and further transfers Bitcoins from the original address to the new address without leaving a trace. Thus, the new one is anonymous.
- (iii) *Step 3. Generating ballots*: Each *Voter* uses the public key of *Supervisor* to encrypt the information of *Candidate* to generate the ballot.
- (iv) *Step 4. Constructing voting transaction*: Each *Voter* utilizes the scripts in the Bitcoin protocol to construct a voting transaction. There are two unlock conditions for the transaction output: the one associated with ballots is performed by the *Supervisor*; another is performed by the *Voter* itself after a timeout.
- (v) *Step 5. Collecting ballots*: The *Supervisor* searches the voting transactions in the Bitcoin blockchain according to an anonymous *Voter* list, then decrypts the ballots with its private key, and counts them. As long as there is a *Candidate* who derives enough ballots before the timeout, the voting is success. Afterwards, *Supervisor* constructs the winning transaction to collect all the ballots of the winner. Meantime, those *Voter* without voting for the winner need to construct a refund transaction to unlock its corresponding transaction and redeem Bitcoins. Conversely, if no candidate wins, the voting fails. Each *Voter* unlocks its transaction and redeems coins.

3.3. *Voter's Identity Confusion Strategy*. To confuse its identity in voting, the $VoterU_i$ needs to apply to both *Supervisor* and *Mixers* for the coin mixing service so as to

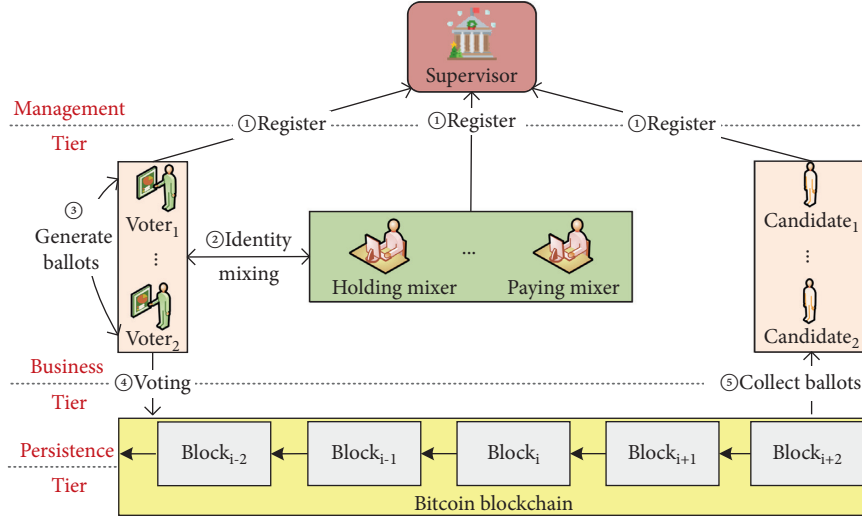


FIGURE 1: System model.

transfer its Bitcoins from original address OBA_i to anonymous address ABA_i without any tracks. As is depicted in Figure 2, the primary principle of coin mixing can be stated as follows: when receiving mixing request, Supervisor randomly select two Mixers with lower load and recommend them to U_i , in which one is the hosting Mixer and another is the paying Mixer. First, U_i constructs a transaction that transfers its Bitcoins from OBA_i to hosting Mixer's escrow address. Once confirming this transaction, the hosting Mixer needs to reply with a voucher. Second, U_i directly forwards this voucher to the paying Mixer and requires it to construct a new transaction that transfers the equal number of Bitcoins from this Mixer's private address to ABA_i . At last, Supervisor gives Bitcoins back to the paying Mixer so as to recover costs, after the task is finished. Looking at the whole process, we can easily find a vulnerability that U_i 's identity privacy would still be exposed when any Mixer colludes with adversaries. In this, we introduce the group blind signature and utilize its unlinkability feature to cut off the interlinkage between these Mixers.

For each registered Mixer _{i} , Supervisor would assign a group certificate $v_i = (y_i + 1)^{1/e} \pmod{n}$ and an escrow address to it, where e is a bilinear pair and y_i denotes the proof of ownership for Mixer _{i} 's private address. Meantime, it releases the Mixer list $L = \{\text{Mixer}_0, \dots, \text{Mixer}_m\}$ on the blockchain platform. In the following, we illustrate the group blind signature-based coin mixing in detail.

Step 1: After U_i has registered successfully, it immediately records the current time as T_1 . When receiving the Mixers recommended by Supervisor, it sends an confusion parameter message $M_1 = \langle T_4, T_5 \rangle$ to the paying Mixer on an anonymous channel, where T_4 is the deadline for U_i to provide the voucher and T_5 is the deadline for this Mixer to submit tx_3 .

Step 2: Once the paying Mixer accepts the message M_1 , it sends the message $M_2 = \langle \text{Sig}\{M_1, \text{nonce}\}_{x_b}, M_1, \text{nonce} \rangle$ to U_i on the anonymous channel, where nonce is random number and x_b denotes the private key of the paying Mixer.

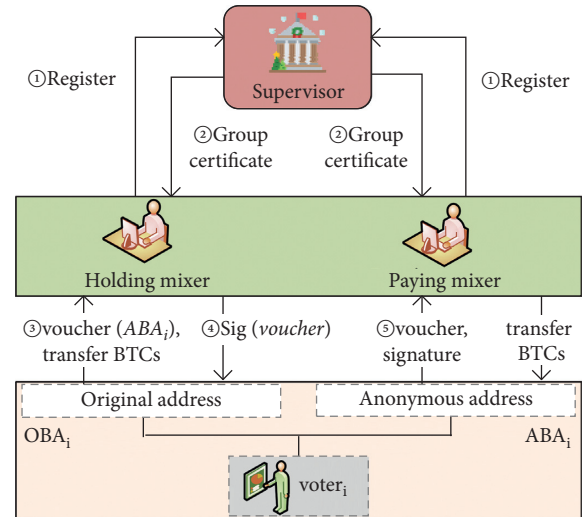


FIGURE 2: An example of identity confusion.

Step 3: In the meantime, U_i sends an confusion parameter message $M_3 = \langle T_2, T_3 \rangle$ to the hosting Mixer, where T_2 is the deadline for U_i to submit the Bitcoin transaction tx_2 and T_3 is the deadline for U_i to execute group blind signature.

Step 4: Once the hosting Mixer accepts the message M_3 , it sends $M_4 = \langle \text{Sig}\{M_3, \text{hosting address}, \text{nonce}\}, M_3, \text{hosting address}, \text{nonce} \rangle$ to U_i , where hosting address denotes the escrow address of the hosting Mixer and x_a denotes the private key of the hosting Mixer.

Step 5: When receiving M_4 , U_i constructs the transaction tx_2 : $U_i \rightarrow$ hosting Mixer before the time point T_2 and transfers its Bitcoins from U_i 's original address OBA_i to the escrow address of the hosting Mixer. Then, it sends a signed message $M_5 = \langle \text{Sig}\{ID_{tx_2}, \text{Own}_v\}_{y_v} \rangle$ by the private key of U_i to the hosting Mixer and expose it on the blockchain platform, where Own_v is the proof of

ownership of the U_i to OBA_i and y_b denotes the public key of the paying Mixer.

Step 6: When the hosting *Mixer* receives the message M_5 through blockchain platform, it needs to complete the following verifications: (1) whether the transaction amount of tx_2 is f , where f is the fixed denomination of the transaction, and (2) whether Own_v has not been used. Once M_5 is validated, the hosting *Mixer* executes the blind SKLOGLOG protocol and blind SKROOTLOG protocol before the time point T_3 , and meantime, the entire execution process would expose on the blockchain platform. For the details, refer to Ref. [28]. Then, it sends message $M_6 = \langle (t_i^{SKLOGLOG} + eb), t_i^{SKROOTLOG} (af)^b \rangle$ to U_i and exposes it on the blockchain platform, where t_i is an arbitrary big value.

Step 7: After receiving the message M_6 , U_i calculates $c_1 = SKLOGLOG_1[\alpha|z = g^{aa}](m)$ and $c_2 = SKROOTLOG_1[\beta|z = g^{\beta c}](m)$ and further obtains the group blind signature (g, z, qr_1, qr_2) of the voucher $\{ABA_i, \text{payingMixer}, \text{nonce}\}$, where qr_i is the quadratic residue in the referenced protocol, g is the generator of the cyclic group, a is the identity element of the cyclic group, and z is the group member key. Then, it sends a message $M_7 = \langle M_2, \{ABA_i, \text{payingMixer}, \text{nonce}\}, \langle g, z, c_1, c_2 \rangle$ to the paying Mixer and publishes it on the blockchain platform before time point T_4 .

Step 8: When the paying Mixer receives the message M_7 through blockchain platform, it needs to complete the following verifications: (1) whether (g, z, c_1, c_2) is the group blind signature of $\{ABA_i, \text{payingMixer}, \text{nonce}\}$, (2) whether M_7 has not been used, (3) whether M_2 is equal to the agreement signature in Step 2, and (4) whether M_2 has not been used. When the verifications are completed, the paying Mixer constructs the exchange transaction tx_3 : paying Mixer $\rightarrow U_i$ before the time point T_5 and transfers its Bitcoins from the private address of the paying Mixer to the U_i 's anonymous address ABA_i .

Supervisor can regularly audit the confusion data recorded on Bitcoin blockchain platform to detect the malicious *Mixers* and punish them. For example, through auditing the hosting *Mixer*'s commitment and tx_2 , the lazy behavior is detected; through auditing the voucher of the paying *Mixer*, the denial-of-service behavior is detected.

3.4. Voting Transaction Construction Strategy. In the Bitcoin blockchain platform, the script is the common technique to construct the voting transaction [29]. Generally speaking, each transaction can contain multiple input scripts and multiple output scripts, in which each input script is associated with the output script of the source transaction up to coinbase transaction. In BEvote, we adopt the P2PKH script and the $M - N$ combined P2SH script. The former could provide the Check Lock Time Verify (CLTV) operator. Its output script only stores the hash value of the public key, and input script stores the public key for verifying whether it matches the hash value. The latter uses a redeem script to store the public key of single or multiple signatures. Assume to have N public keys, and at least M of the public keys must be provided with a signature corresponding to the unspent transaction output. Its input script must give all the private keys and the serialized redeem scripts.

We use an example to illustrate the voting transaction construction. As is shown in Figure 3, there is a voting transaction $VoteTx_i$ with a ballot. Its output is x Bitcoins, and input address is the anonymous Bitcoin address ABA_i . The output script is based on an OR operator. This means that the transaction output can be unlocked only if either of the following conditions is satisfied.

Condition 1. is set to be performed by the *Supervisor*, and the ballot is recorded in the P2SH script. When creating an $M - N$ combined P2SH UTXO, the user first needs to generate a redeem script to store all public keys. In the Bitcoin protocol, the PUSHDATA operation of the stack-based language limits the maximum data to 520 bytes; hence, the redeem script can only place up to 15 public keys under this restriction. The script form is as follows:

$$M \langle \text{PubKey}_1 \rangle \langle \text{PubKey}_N \rangle N \text{ OP_CHECKMULTISIG.} \quad (2)$$

Then, the HASH160 algorithm is used to generate a 20 byte long hash of this script and an output script is created as follows:

$$\text{OP_HASH160} \langle \text{Hash of Redeem Script} \rangle \text{OP_EQUAL.} \quad (3)$$

Data can also be stored in the P2SH script, and the idle public key bits in the redeem script are just replaced with data. For example, if there are data $Da ta_1$, $Da ta_2$, the redemption script form is as follows:

$$M \langle \text{PubKey}_1 \rangle \langle \text{PubKey}_N \rangle \langle \text{Data}_1 \rangle \langle \text{Data}_2 \rangle N \text{ OP_CHECKMULTISIG.} \quad (4)$$

In BEvote, the redeem script RS corresponding to the first unlock condition of $VoteTx_i$ output script contains the public key PU_s of *Supervisor* and stores the ballot v_i . It can be unlocked by the private key of *Supervisor*. The form of 1 - 1 combination script is as follows:

$$1 \langle PU_s \rangle \langle v_i \rangle 1 \text{ OP_CHECKMULTISIG.} \quad (5)$$

The output script stores the 20 byte long hash value of RS calculated by HASH160 algorithm in the form:

$$\text{OP_HASH160} \langle \text{Hash}(RS) \rangle \text{OP_EQUAL.} \quad (6)$$

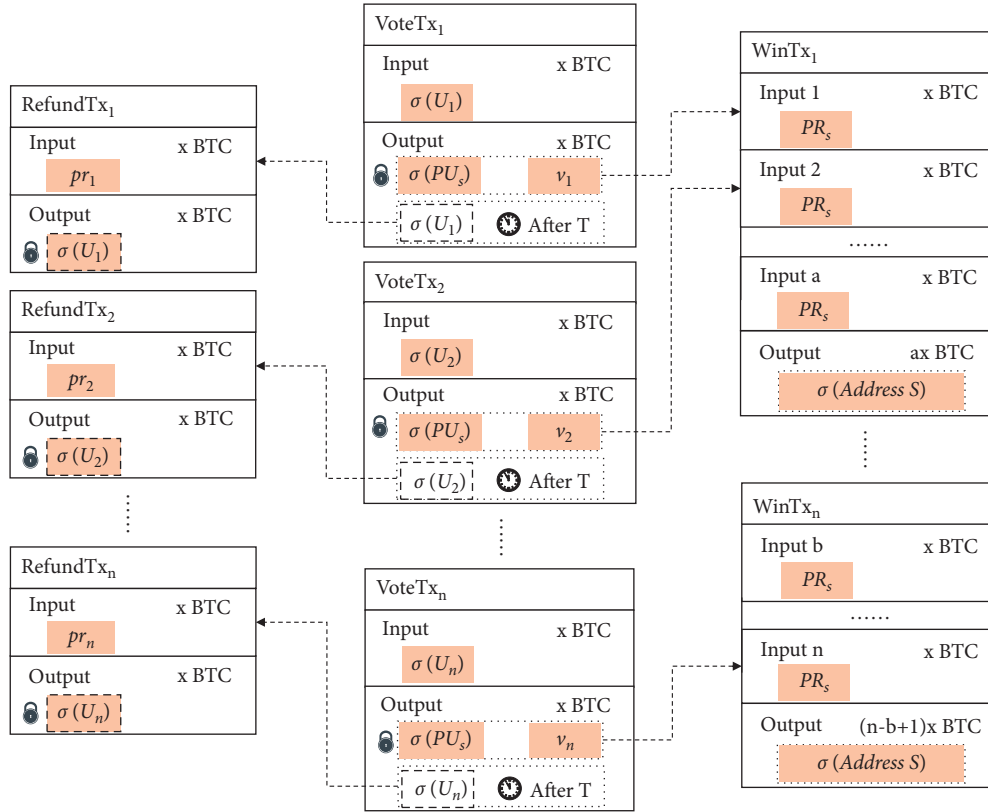


FIGURE 3: An example of voting transaction.

Condition 2. is added in the form of a time lock with the P2PKH script. CLTV can regularly lock an output of a transaction, instead of locking the entire transaction. After using the CLTV operator in the transaction output, it can

limit the output to be unlocked only after a specified time. For example, Alice transfers to Bob, usually using an output script in the form of P2PKH:

$$\text{OP_DUP OP_HASH160}\langle \text{Hash of Bob}^A\text{'s Public Key} \rangle \text{OP_EQUALVERIFY OP_CHECKSIG.} \tag{7}$$

CLTV is used to lock for a period of time; assuming 2 months, the time can be set to the current block height +8640 (block) or the current Unix epoch time +5184 000

(seconds). After the timeout, P2PKH transactions can be unlocked by Bob using his own private key signature:

$$\begin{aligned} &\langle \text{now} + 2 \text{ months} \rangle \\ &\text{OP_CHECKLOCKTIMEVERIFY OP_DROP OP_DUP OP_HASH160} \\ &\langle \text{Hash of Bob's Public Key} \rangle \text{OP_EQUALVERIFY OP_CHECKSIG.} \end{aligned} \tag{8}$$

In BEvote, the P2PKH script of the second unlock condition of VoteTx_i output script contains the voter's public key pu , which is locked for a period of time using the

CLTV operator. After the timeout, the voter can use his private key signature to unlock it. When locked for one day, the form is as follows:

$$\begin{aligned} & \langle \text{now} + 1\text{day} \rangle \\ \text{OP_CHECKLOCKTIMEVERIFY OP_DROP OP_DUP OP_HASH160} & \quad (9) \\ & \langle pu \rangle \text{OP_EQUALVERIFY OP_CHECKSIG.} \end{aligned}$$

3.5. *Potential Threats.* The above strawman design would face the following potential threats in real environments:

- (i) Sybil attack: To illegally gain more voting rights, attacker may generate multiple Bitcoin addresses to forge *Voters's* identities.
- (ii) Premature leakage of ballots: With the opportunity of generating ballots, the misbehaved insider of *Supervisor* may expose the ballots when the voting has not yet been closed.

To fix these threats and enhance its robust, we devise a secure voting protocol in Section 4.

4. Secure E-Voting Protocol for BEvote

In this section, we describe a secure E-voting protocol to defend against the above threats in BEvote.

4.1. *An Overview.* To establish an efficient countermeasures, we need to analyze the causes of these threats. First, the openness of Bitcoin blockchain platform and its multi-address allocation makes it possible for hackers to forge numerous virtual *Voters*. In this case, increasing barriers to entry would be effective to defend against the Sybil attack. Thus, adding an authentication function in E-voting protocol is necessary. Second, to avoid premature leakage of ballots by *Supervisor*, the voting transaction only can be unlocked by those winning candidates; i.e., they at least gain k votes cast. Thus, it is necessary to design a feasible encryption policy for voting transaction.

Guiding by these principles, we first design an authentication based on public key cryptography to prevent the virtual *Voters*. Second, we introduce the joint Shamir random secret sharing (joint-RSS) [30], which realizes the sharing of a secret S to n participants, while any k or more participants can recover the secret S . It mainly contains the following steps:

- (1) Each participant U_i chooses a secret $a_0^{(i)}$ and constructs a $k-1$ order polynomial $f_i(x) = \sum_j 0^{k-1} a_j^{(i)} x^j = a_0^{(i)} + a_1^{(i)} x + a_2^{(i)} x^2 + \dots + a_{k-1}^{(i)} x^{k-1}$.
- (2) Each participant U_i takes n numbers x_1, x_2, \dots, x_n and substitutes them into polynomials to get $s_j^{(i)} = f_i(x_j)$ ($j \in [1, n]$). The participant remains one of them and afterwards sends to the rest $n-1$ participants.
- (3) After U_j ($j \in [1, n]$) receiving $s_j^{(i)}$ sent by the remaining $n-1$ participants U_i ($i \in [1, n], i \neq j$), it is summed to get its share $s_j = \sum_{i=1}^n s_j^{(i)}$.

Any k or more participants can utilize the set of shares F to recover the secret S through the Lagrange interpolation formula $S = \sum_{j \in F} (s_j \prod_{i \in F, i \neq j} (i/(i-j)))$. By integrating these techniques into the basic BEvote, we propose a secure

E-voting protocol, and Figure 4 shows its overall description. Firstly, Voters, Mixers, and Candidates use public key cryptography-based registration to realize the correct verification of their Bitcoin addresses. Secondly, Voter obtains an anonymous address through the identity confusion strategy. Thirdly, with the anonymous address, Voter in AVL executes joint Shamir random secret sharing to obtain secret shares and generate ballots with them. Fourthly, Voter constructs the voting transaction and broadcast it to the Bitcoin blockchain platform. Fifthly, each Candidates searches the voting transactions in blockchain according to AVL and collects the secret shares stored in the ballots if successfully decrypted them. If sufficient secret shares are collected, a winning transaction is constructed; otherwise, the Voter constructs a refund transaction.

4.2. *Detailed Description of Proposed Protocol.* There are five steps in our proposed protocol. The implementation details can be stated as follows:

In step 1, Voters, Candidates, and Mixers, respectively, make the registration to Supervisor.

- (i) Each *Voter* submits the Bitcoin address BA_j , public key pu_j and identity information (including identity signature) to Supervisor. After Supervisor reviews the identity information and verifies that the signature corresponds to BA_j , it distributes a *Voter's* number and adds it to the private voter list.
- (ii) Each *Candidate* submits the public key $PU_j = PR_j \cdot G$ and identity information to Supervisor, where PR_j is its private key and G is the basic point of elliptic curve. After being reviewed by Supervisor, the candidate list is constructed and published.
- (iii) Each *Mixer* submits identity information to the regulator, and then, Supervisor issues a group certificate to it after it has passed the review.

In step 2, each *Voter* utilizes the identity confusion strategy to obtain the anonymous address. Then, the anonymous voter list is constructed.

In step 3, each *Voter* utilizes anonymous Bitcoin addresses to execute joint Shamir random secret sharing in order to obtain secret shares.

- (i) *Voter* selects a secret value $a_0^{(i)}$ to construct a $k-1$ order polynomial $f_i(x) = \sum_{j=0}^{k-1} a_j^{(i)} x^j$.
- (ii) *Voter* takes n numbers x_j ($j \in [1, n]$) and substitutes them with the polynomial. Then, the results $f_i(x_j)$ are sent to the remaining $(n-1)$ *Voters*. Each *Voter* needs to sum up the n data received to get the private key share $s_j = \sum_{i=1}^n f_i(x_j)$ ($i \in [1, n]$). In

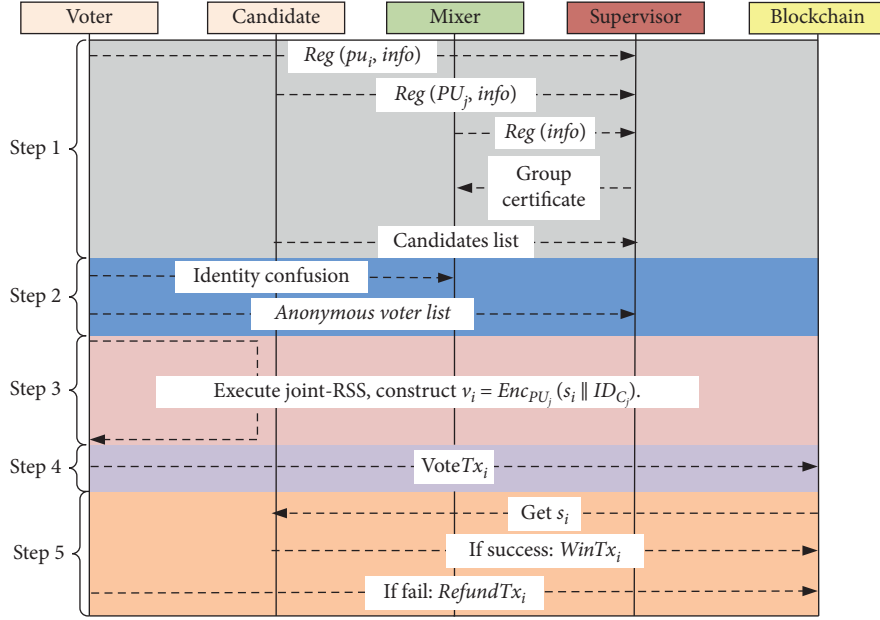


FIGURE 4: Secure E-voting protocol for BEvote.

order to construct the correct P2SH script to broadcast the voting information, the public key corresponding to this private key needs to be calculated. Then, the public key share $p_j = s_j \cdot G$ is calculated and sent it to other legitimate Voters.

- (iii) When receiving the remaining $n - 1$ public key shares p_i , a complete public key $P = \sum_{i=1}^k \lambda p_i = S \cdot G$ is constructed. Afterwards, each Voter utilizes the public key of his supported candidate C_j to encrypt the secret share s_i and ID_{C_j} to generate the ballot. For example, if a Voter U_i votes for a Candidate C_j , the form of the ballot is $v_i = \text{Enc}_{PU_j}(s_i || ID_{C_j})$.

In step 4, we need to put the secret sharing share in the ballot and change the first unlocking condition to secret shared private key. The redeem script RS of the first unlock condition contains the secret shared public key P and stores the ballot v_i . It can be unlocked by utilizing the corresponding secret shared private key signature. The form of this 1 - 1 combination script is as follows:

$$1 \langle P \rangle \langle v_i \rangle 1 \text{ OP_CHECKMULTISIG}. \quad (10)$$

In step 5, Candidates collect their own ballots to obtain secret shared shares. The Candidate C_j queries for VoteTx_i on the blockchain according to the transaction records of all addresses in AVL , checks the public ballot v_i in the P2SH script, and then tries to decrypt v_i with his private key PR_j in turn. Successful decryption can obtain the private key share s_i and the candidate identity number ID_{C_j} .

Depending on whether Candidate would collect enough secret shares contained in the ballots before timeout, there are two cases:

- (i) *Voting Success.* If a Candidate C_j successfully collects k or more private key shares s_i , the secret shared private key $S = \sum_{i \in F} (s_i \prod_{j \in F, j \neq i} (j / (j - i)))$ can be reconstructed by the Lagrange interpolation formula. The Candidate can construct a winning transaction WinTx_j for each voting transaction or use the output of multiple voting transactions as the input of a winning transaction. S is used to sign each input to unlock the first condition of the voting transaction output script. All UTXOs are obtained in n voting transactions. Other entities can verify that the *Candidate* has obtained sufficient secret shares, successfully reconstructed the private key, and won the voting by querying the winning transactions recorded in the blockchain. The input script of a winning transaction unlocks UTXO in the form of P2SH in the voting transaction. A signature of S and a serialized redeem script are required: $OP_0 \langle \text{Sig}_s \rangle \langle \text{Serialized Redeem Script} \rangle$.
- (ii) *Voting Failed.* If no Candidate gets enough valid ballots to reconstruct the secret shared private key S , the voting fails. This voting protocol uses Bitcoin's time lock script to design a secure rollback mechanism. Even in the event of a vote failure, the Bitcoins submitted by Voters can still be redeemed. All Voters get Bitcoins back and vote again. Only when the time exceeds T , the CLTV operator of the second unlock condition would be invalidated. T denotes the agreed voting timeout time before voting. It can prevent voters from transferring Bitcoins before the failure. After that, each Voter constructs a refund transaction RefundTx_i and returns $n \cdot x$ Bitcoins to the original anonymous address ABA_j . This transaction input is the second condition of the voting transaction output script and is signed by the voter utilizing the private key.

5. Security Analysis

This section mainly analyzes the effectiveness and robustness of BEvote. In particular, we focus on proving its features of validity, robustness, anonymity, fairness, verifiability, and receipt-free.

Theorem 1. (validity). *Only valid entities reviewed can participate in the voting, which ensures the credibility of results.*

Proof. Before voting, *Voters* need to prove that they have enough Bitcoin for voting, and *Supervisors* will check the validity of the identity information of *Voters*, *Can di dates*, and *Mixers*. Although valid *Voters* obtained the ABA through the mix coin strategy while cutting off the physical connection between ABA and the real identity, ABA will be included in AVL. While in the pre-voting stage, only valid *Voters* in AVL can perform joint-RSS to obtain private key shares s_i to construct ballots. In the voting stage, only transactions constructed with addresses in AVL are considered valid.

Theorem 2. (robustness). *The system has certain fault tolerance to resist attacks and avoid errors.*

Proof. *Voters* who have not passed the review will not appear in doc missing and cannot participate in secret sharing to obtain shares. So, it is impossible to construct a valid ballot or launch an Sybil attack by generating multiple Bitcoin addresses. Ballots that are not constructed in accordance with the protocol's prescribed format, as well as ballots constructed using counterfeit shares, cannot reconstruct the key S . Hence, the ballots will be considered invalid. *Voters* may use the same shared secret to construct multiple ballots for the purpose of more voting rights, but the openness of the Bitcoin transaction script determines that such actions can be found and held accountable. This behavior also means that the number of bytes in the transaction script will increase, which will lead to an increase in transaction fees the *Voters* need to pay, so that it will be suppressed to a certain extent. Therefore, ballot forgery is in vain. In addition, external adversaries may launch denial-of-service attacks on system nodes to attempt to impact the voting process and results, yet it will be prevented by Bitcoin's distributed peer-to-peer network. Meanwhile, external adversaries will be spotted if they try to participate in voting by disguising themselves as system characters since their Bitcoin address has not been reviewed by Supervisor and is not on the public list.

Theorem 3. (anonymity). *Anonymity should be satisfied for the purpose of protecting the privacy of voters.*

Proof. This e-voting protocol achieves the purpose of sending and disclosing ballots by attaching voting data to transaction scripts. During the mix coin phase, the entity relationship between the anonymous Bitcoin address ABA,

and the voter U_i was severed. Therefore, after mix coin, *Voters* are anonymous during the execution of secret sharing and participation in Bitcoin transactions. At the same time, the voucher exchange method between multiple *Mixers* in the mix coin avoids the possibility of a single *Mixer* leaking user information.

Theorem 4. (fairness). *The decision of voters cannot be influenced by the fairness of voting protocol.*

Proof. Each *Voter's* share of the private key s_i is only owned by himself before voting and is different from each other. The secret share s_i and candidate number ID_{C_j} in the ballot are encrypted by the public key of the selected candidate PU_j , and only the supported *Can di date* C_j has the private key PR_j to decrypt the ballot v_i . Due to the use of anonymous Bitcoin addresses, *Can di dates* cannot associate ballots with *Voters's* true identities. These designs make it impossible for *Voters* and *Can di dates* to know the current election situation or influence the decision of *Voters*, which ensures the fairness of voting.

Theorem 5. (verifiability). *Any entities could verify the voting process and the result even if the execution of protocol has ended.*

Proof. In our protocol, other entities can query the candidate list and anonymous voter list published by the regulator to verify the legitimacy of *Voters* and *Can di dates*. During the voting stage, ballots are recorded in transactions, and all transaction records are publicly available on the Bitcoin blockchain. Only if the *Can di date* collects enough secret shares to reconstruct the secret key, he can generate a winning transaction and withdraw BTCs. Other entities consult the transaction records stored in the blockchain, first verify that the serialized redeem script matches the hash value in UTXO, and then check whether the signature meets the multi-signature unlocking condition to verify that the *Can di date* has indeed enough ballots to reconstruct the key and win the vote.

Theorem 6. (receipt-free). *It means that the voting design needs to ensure that ballots that could not be proved in advance are sent by specific voters.*

Proof. This protocol cuts off the association between the anonymous Bitcoin address and the real identity during the mix coin phase; therefore, *Voters* cannot prove to a third party in advance that they have the right to vote. Meanwhile, during the voting stage, *Voters* need to execute joint-RSS to obtain shares. The share in the ballot is generated jointly by random parameters sent by all *Voters*. There is no way to prove to a third party that a specific ballot will be generated. These measures make it impossible for *Voters* to provide proof of voting to a third party in advance and guarantee the protocol receipt-free.

6. Performance Evaluation

In this section, we mainly evaluate the efficiency of BEvote. We first use the theoretical analysis to look at its computation and communication overhead. Then, we build the simulation platform to perform extensive experiments.

6.1. Theoretical Analysis. In BEvote, there are three key stages to affect its efficiency, including confusing *Voter's* identity, generating ballots, and constructing voting transaction. Considering that BEvote utilizes the Bitcoin blockchain platform as the storage infrastructure, the efficiency on the third stage depends on the throughput of such blockchain. It is widely known that the rapid development of Bitcoin lightning network has significantly enhanced its transaction speed [24], and thus, the performance evaluation regarding the voting transaction construction is not necessary. In this case, we focus on investigating the efficiencies of the first two. When voters need to confuse their identities or generate ballots, the main execution is the identity confusion strategy and joint-RSS. Thus, we, respectively, evaluate their efficiencies [31].

The *Voter's* identity confusion strategy contains three parts: *Mixer* registration, identity confusion, and confusion audit. Considering that the modular multiplication operation m and the modular exponentiation operation M are two time-consuming operations, we mainly focus on analyzing the number of such operations in each part. Table 3 shows the theoretical analysis results. Apparently, most of the computational overhead is concentrated in the confusion phase. The reason is that both *Voters* and *Mixers* need to calculate group blind signatures and RSA signatures.

We utilize the amount of data transmitted in the ballot generation stage to estimate the communication complexity. With regard to joint-RSS, each *Voter* is required to transmit a bits to the rest $n - 1$ voters. Afterwards, each participant calculates b bits $p_i = s_i \cdot G$ and broadcasts it. As a result, there are $n \cdot a(n - 1)$ bit transmission and $n \cdot b$ bit broadcast overhead. The communication overhead estimation is listed in Table 4. The $b + a(n - 1)$ bit overhead is affordable for each one, while the total $n(b + a(n - 1))$ bit overhead is trivial to the current network.

6.2. Experimental Analysis. The simulation utilizes the Java language, with the help of the JPBC library to implement the operations in the elliptic curve group and utilize multiple threads to simulate multiple voters [32]. The simulation environment is Windows 10 64 bit operating system with i7-8750H (@2.2 GHz) CPU and 16 GB memory. The process of program execution is that the user randomly constructs a polynomial by taking random numbers, then substitutes n numbers to evaluate the polynomial, and sends it to other users. Each user sums all the values they receive as their secret share. The following experimental values are all averaged after running 100 times in the Eclipse IDE [33].

To further proceed to investigate the execution time of voter's identity confusion, we, respectively, simulate the modular multiplication and modular exponentiation

TABLE 3: Theoretical execution overhead of voter's identity confusion.

Part	Modular multiplication	Modular exponentiation
<i>Mixer</i> registration	0	$2n \cdot M$
Identity confusion	$4n \cdot m$	$21n \cdot M$
Confusion audit	$2n \cdot m$	$n \cdot M$

TABLE 4: Theoretical communication overhead of ballot generation.

Joint-RSS	Broadcast	Transmission	Sum
Individual	b	$a(n - 1)$	$b + a(n - 1)$
Total	$n \cdot b$	$n \cdot a(n - 1)$	$n(b + a(n - 1))$

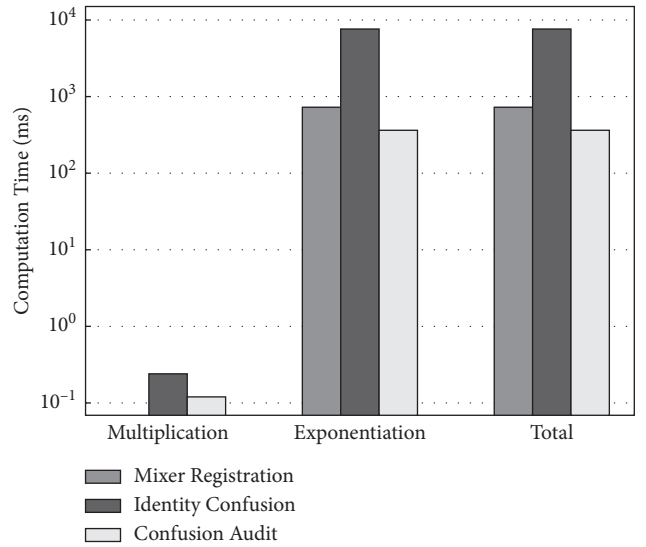


FIGURE 5: Execution time of voter's identity confusion.

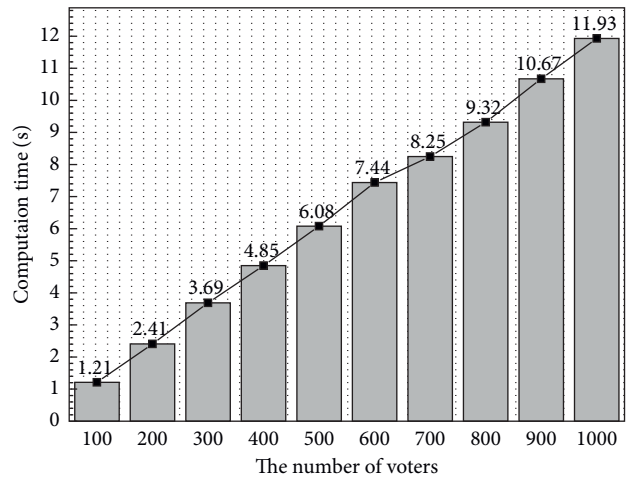


FIGURE 6: Execution time of ballot collection.

operations in each part. Figure 5 shows the simulation results. Since the computation complexity of modular exponentiation is far greater than modular multiplication, the

total execution time of identity confusion part is more than ten times as much as *Mixer* registration and confusion audit.

In addition, we consider the running time of ballot collection with the number of *Voters* from 0 to 1000. The results are shown in Figure 6. Apparently, the time overhead increases roughly linearly with the number of *Voters*. The computation time for the scale of thousands of *Voters* is less than one minute, so the time overhead for the large-scale system is within an acceptable range.

7. Conclusion

In this study, we propose a Bitcoin-based electronic voting scheme with anonymity and robustness, which abstracts a Bitcoin transaction as the voting process. Its characteristics can be summarized as follows: firstly, we design a coin mixing-based system model to achieve strong anonymity; secondly, we devise a secret sharing-based E-voting protocol to keep the voting numbers private; and finally, we carry out security analysis and experimental evaluations to demonstrate its efficiency and robustness.

There are many directions in which this work can be extended. The first is to consider the low throughput and high network delay of Bitcoin blockchain, which would cause the scalable issue in regional collaborative medical system. A promising solution is to directly utilize MEC nodes to build a private blockchain towards E-voting, instead of public blockchain. In this case, we can make this blockchain to be more voting-compatible, with both scalability and robustness. Another direction is to study the new applications of E-voting, such as decision support or recommendation system [34–36].

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Disclosure

Xin Xu is the co-first author of this work.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Nos. 62072092, 62072093, and U1708262); the China Postdoctoral Science Foundation (No. 2019M653568); the Key Research and Development Project of Hebei Province (No. 20310702D); the Natural Science Foundation of Hebei Province (No. F2020501013); and the Fundamental Research Funds for the Central Universities (No. N2023020).

References

- [1] Y. Xu, H. Gao, and R. Li, Y. Yin, Z. Cao, and Z. Mai, QoS prediction for service recommendation with features learning in mobile edge computing environment,” *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 4, pp. 1135–1145, 2020.
- [2] M. Cao, J. Xiao, Q. Xu, H. Gao, K. Xu, and Y. Yin, “The deep features and attention mechanism based method to dish healthcare under social IoT systems: an empirical study with a hand-deep local-global net,” *IEEE Transactions on Computational Social Systems*, pp. 1–12, 2021.
- [3] M. Blaze, J. Braun, and C. G. Advisors, “Defcon 25 voting machine hacking village,” in *Proceedings of the DEFCON*, pp. 1–18, Washington, DC, USA, September 2017.
- [4] M. A. Specter, J. Koppel, and D. Weitzner, “The ballot is busted before the blockchain: a security analysis of voatz, the first internet voting application used in us federal elections,” in *Proceedings of the 29th {USENIX} Security Symposium ({USENIX} Security 20)*, pp. 1535–1553, Anaheim, CA, USA, 2020.
- [5] T. Moura and A. Gomes, “Blockchain voting and its effects on election transparency and voter confidence,” in *Proceedings of the 18th Annual International Conference on Digital Government Research*, pp. 574–575, Staten Island, NY, USA, June 2017.
- [6] J. Zhang, S. Zhong, T. Wang, H.-C. Chao, and J. Wang, “Blockchain-based systems and applications: a survey,” *Journal of Internet Technology*, vol. 21, no. 1, pp. 1–14, 2020.
- [7] Z. Zhao and T.-H. H. Chan, “How to vote privately using bitcoin,” in *Proceedings of the International Conference on Information and Communications Security*, pp. 82–96, Beijing, China, December 2015.
- [8] C. K. Adiputra, R. Hjort, and H. Sato, “A proposal of blockchain-based electronic voting system,” in *Proceedings of the 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, pp. 22–27, IEEE, London, UK, October 2018.
- [9] P. C. Jason and K. Yuichi, “E-voting system based on the bitcoin protocol and blind signatures,” *IPSI Transactions on Mathematical Modeling and its Applications*, vol. 10, no. 1, pp. 14–22, 2017.
- [10] S. Bistarelli, M. Mantilacci, P. Santancini, and F. Santini, “An end-to-end voting-system based on bitcoin,” in *Proceedings of the Symposium on Applied Computing*, pp. 1836–1841, Marrakech, Morocco, April 2017.
- [11] S. Bartolucci, P. Bernat, and D. Joseph, “Sharvot: secret share-based voting on the blockchain,” in *Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain*, pp. 30–34, Gothenburg, Sweden, March 2018.
- [12] Y. Takabatake, D. Kotani, and Y. Okabe, “An anonymous distributed electronic voting system using zerocoin,” Technical Report, IEICE, 2019.
- [13] D. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms,” *Communications of the ACM*, vol. 24, no. 2, 1981.
- [14] B. Adida, “Helios: web-based open-audit voting,” in *Proceedings of the USENIX Security Symposium*, vol. 17, pp. 335–348, California, CA, USA, July 2008.
- [15] N. Chondros, B. Zhang, T. Zacharias et al., “Distributed, end-to-end verifiable, and privacy-preserving internet voting systems,” *Computers & Security*, vol. 83, pp. 268–299, 2019.

- [16] V. Cortier, D. Galindo, R. Küsters, J. Mueller, and T. Truderung, "Sok: verifiability notions for e-voting protocols," in *Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP)*, pp. 779–798, IEEE, San Jose, CA, USA, August 2016.
- [17] J. Benaloh and D. Tuinstra, "Receipt-free secret-ballot elections," in *Proceedings of the ACM Symposium on the Theory of Computing (STOC)*, vol. 94, pp. 544–553, Montreal, PQ, Canada, May 1994.
- [18] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, "Secure multiparty computations on bitcoin," in *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, pp. 443–458, IEEE, San Jose, CA, USA, May 2014.
- [19] D. Chaum, C. Crépeau, and I. Damgard, "Multiparty unconditionally secure protocols," in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pp. 11–19, Chicago, IL, USA, May 1988.
- [20] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in *Proceedings of the International Conference on Financial Cryptography and Data Security*, pp. 357–375, Springer, Sliema, Malta, January 2017.
- [21] P. Tarasov and H. Tewari, "The future of e-voting." *IADIS International Journal on Computer Science & Information Systems*, vol. 12, no. 2, 2017.
- [22] E. Yavuz, A. K. Koç, U. C. Çabuk, and G. Dalkılıç, "Towards secure E-voting using ethereum blockchain," in *Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, pp. 1–7, IEEE, Antalya, Turkey, March 2018.
- [23] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," *IEEE Access*, vol. 7, pp. 24477–24488, 2019.
- [24] J. Poon and T. Dryja, *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*, 2016, <https://lightning.network/lightningnetwork-paper.pdf>.
- [25] S. Zhang, L. Wang, and H. Xiong, "Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability," *International Journal of Information Security*, vol. 19, no. 3, pp. 1–19, 2019.
- [26] N. Lu, Y. Chang, W. Shi, and K.-K. Raymond Choo, "CoinLayering: an efficient coin mixing scheme for large scale bitcoin transactions," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–17, 2020.
- [27] T. Fei, Y. Chang, J. Wang, N. Lu, and W. Shi, "Anonymous bitcoin mixing scheme based on semi-trusted supervisor," in *Proceedings of the 2020 IEEE 3rd International Conference on Electronics Technology (ICET)*, pp. 845–850, Chengdu, China, May 2020.
- [28] A. Fiat and A. Shamir, "How to prove yourself: practical solutions to identification and signature problems," in *Proceedings of the Advances in Cryptology-CRYPTO'86*, Santa Barbara, CA, USA, December 2000.
- [29] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," Technical Report, Manubot, 2019.
- [30] Z. Chen, S. Li, Q. Huang, J. Yan, and Y. Ding, "A joint random secret sharing scheme with public verifiability," *International Journal on Network Security*, vol. 18, no. 5, pp. 917–925, 2016.
- [31] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," *Future Generation Computer Systems*, vol. 105, pp. 13–26, 2020.
- [32] A. De Caro and V. Iovino, "JPBC: Java pairing based cryptography," in *Proceedings of the 16th IEEE symposium on computers and communications*, pp. 850–855, IEEE, Kerkyra, Corfu, Greece, July 2011.
- [33] E. Foundation, "Enabling open innovation collaboration. The eclipse foundation," 2021, <https://www.eclipse.org>.
- [34] H. Gao, X. Qin, R. J. D. Barroso, W. Hussain, Y. Xu, and Y. Yin, "Collaborative learning-based industrial IoT API recommendation for software-defined devices: the implicit knowledge discovery perspective," *IEEE Transactions on Emerging Topics in Computational Intelligence*, pp. 1–11, 2020.
- [35] M. Cao, X. Yang, and S. Zhou, "An approach to alleviate the sparsity problem of hybrid collaborative filtering based recommendations: the product-attribute perspective from user reviews," *ACM/Springer Mobile Networks and Applications*, vol. 25, no. 2, pp. 376–390, 2020.
- [36] H. Gao, W. Hussain, Y. Huang, and H. Xu, "Sur: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 370–381, 2021.

Research Article

A Novel Video Copyright Protection Scheme Based on Blockchain and Double Watermarking

Jingjing Zheng ¹, Shuhua Teng ^{2,3}, Peirong Li ⁴, Wei Ou ⁴, Donghao Zhou ⁵,
and Jun Ye ⁴

¹School of Computer Science and Technology, Hainan University, Haikou 570228, Hainan, China

²Hunan Communications Research Institute Co., LTD., Changsha 410015, Hunan, China

³School of Information Science and Engineering, Hunan First Normal University, Changsha 410205, Hunan, China

⁴School of Cyberspace Security (School of Cryptology), Hainan University, Haikou 570228, Hainan, China

⁵School of Computer, National University of Defense Technology, Changsha 410073, Hunan, China

Correspondence should be addressed to Wei Ou; ouwei@hainanu.edu.cn

Received 13 September 2021; Revised 17 October 2021; Accepted 11 November 2021; Published 13 December 2021

Academic Editor: Honghao Gao

Copyright © 2021 Jingjing 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.

With the continuous development of multimedia, more and more digital works such as videos are spread, stored, and used in the network. In recent years, digital copyright infringement disputes have occurred frequently. The traditional copyright protection system has some problems, such as difficulty confirming copyright, monitoring infringement, and obtaining evidence for rights protection. To this end, we have designed and implemented a novel video copyright protection scheme based on the blockchain and double watermarking technology. We use the image correlation coefficient method to extract video keyframes. And we combine with Contourlet Transform domain, QR decomposition, and SIFT algorithm to improve the robustness of watermark against geometric attacks on the premise of invisibility. After that, we use Arnold Transformation (Cat Map) based on the Maximum Entropy Threshold Segmentation to encrypt the robust watermark and strengthen the security. Moreover, based on the characteristics of the fragile watermarking, we accurately locate the attacked video's tamper position and complete the integrity authentication of the watermarked video. In addition, the hash digest of the video watermark and the user ID of the copyright owner is signed by SM2 and uploaded to the blockchain. The user can register the copyright after passing the identity authentication. We conduct tests and security analysis on the blockchain performance of the system, the performance of the commercial cryptography algorithm, and the security of the watermarking system. The experimental results show that the blockchain used in this system conforms to the industry standard, the performance of SM2 and SM3 is better than ECC-256 and SHA-256, and the system security is well guaranteed.

1. Introduction

With the advent of the Internet era, the new media industry is growing at high speed worldwide [1], resulting from the integration of network technology and cultural industry. The number of video resources that people are exposed to in their daily life is rapidly expanding. And the number of online video users in China is gradually increasing in proportion to the total number of netizens. As of June 2019, the number of online video users had reached 759 million [2]. In the case of China, the short video industry, such as Tik Tok, Kuaishou, and other platforms, currently has more than 600 million

active users and a market volume of more than 10 billion CNY [3]. The official data survey on video infringement cases shows the severe and rampant infringement phenomenon behind the prosperous video industry in China. From January 2019 to October 2020, the 12426 Copyright Monitoring Centre monitored more than 100,000 original short video authors, the National Copyright Administration's early warning list, short video clips of key film, and other works. The number of works covered exceeded 10 million, and a total of 30,095,200 suspected infringing short videos were monitored, which involved up to 2.72 trillion clicks.

The frequent occurrence of video copyright infringement is also related to the characteristics of the video, such as easy modification and hard distinguishment. A large amount of video information is exchanged and transmitted on the network [4, 5], and the video can be easily modified by various means [6], such as interception, copy, tamper, and redistribution [7]. Pirated video resources can be found everywhere on the Internet. It is difficult to distinguish the authenticity of video information, and there are many disputes over copyright issues [8]. The commercialization of the video business is severely hampered, resulting in severe economic damage [9]. The Internet brings not only opportunities to the field of video works but also the problem of industry copyright disorder. This problem is the challenge in this field. If it cannot be solved in time, it will be a significant obstacle for the development of China's online video works copyright industry [10]. Copyright protection in the field of video has become a matter of urgency and cannot be delayed.

Along with the acceleration of technology application and innovation in the emerging markets of intellectual property rights (IPR) capitalization, a large number of international investment treaties have included IPRs in the scope of investment [11–13]. China's policies related to IPR protection have also continued to increase. IPR has been mentioned many times in the document "Outline of the 14th Five-Year Plan and 2035 Vision for National Economic and Social Development of the People's Republic of China." China is actively promoting digital industrialization and industrial digitization, and the digital economy has become a new variable to improve the quality and efficiency of the Chinese economy [14, 15].

Traditional video digital watermarking technology has the following problems [16–18]: Firstly, the algorithm's robustness is poor. The vector of the video watermarking algorithm is video. For video attacks, in addition to image attacks, there are also frame average, frame deletion, frame reassembly, and other attacks. Therefore, for video watermarking technology, it is required to resist the attacks mentioned above. Moreover, the robustness of geometric attacks, compression attacks, and other attacks still needs to be improved. Secondly, the balance of the video watermarking scheme is poor. Video single watermarking algorithm is mutually constrained in terms of robustness and vulnerability. The robust watermarking ensures that the watermark information confirming the copyright can still be extracted after the video is attacked. The fragile watermarking can locate and quantify the tampered location when tampering is detected. Furthermore, the single watermarking systems often cannot balance robustness and vulnerability. Thirdly, traditional digital copyright protection systems use centralized central databases. So, the security of data is easily threatened. Nowadays, with the rapid development of the Internet, there are more and more copyright protection issues. And the centralized databases are no longer meet the growing demand for copyright protection on the Internet. Fourthly, the watermark is poorly associated with its owner. In order to protect their IPR, individuals or groups often embed the watermark of relevant

information with certainty and confidentiality into the resources they want to protect. However, when their watermarks are not notarized by trusted third-party certification bodies, the relationship between them and individuals or groups cannot be guaranteed, which leads to the watermark's poor relevance to the owner. Usually, the authentication steps of third-party certification bodies are tedious and costly.

Given the above problems, we propose and implement a video copyright protection system based on the blockchain and double watermarking technology. We are committed to protecting video copyright and solving traceability and other needs. The system makes use of SM2 to sign the digest of robust watermark and user ID and then uploads the signature to the blockchain platform. The consensus mechanism of the blockchain can effectively guarantee the authenticity of the data. During the uploading procedure, we also verify the user's identity to confirm that the user is who he claims to be. The combination of Contourlet Transform domain, QR decomposition, and SIFT algorithm makes the robust watermark improve the robustness against geometric attacks under the premise of invisibility. The watermark is encrypted by using Arnold Transformation (Cat Map) based on the Maximum Entropy Threshold Segmentation and pinpoints the location of the tampered location by using the fragile watermarking.

2. Background

Due to the increasing number of disputes caused by video copyright issues, people's awareness of video copyright protection is growing, and the demand for video copyright protection has become intense. Digital watermarking technology has emerged. In 1993, Tirkel et al. first proposed the expression "watermark." In 1994, Tirkel et al. [19] proposed "a digital watermark," detailed the definition of digital watermarking, and described the application areas of digital watermarking. As a result, many famous universities and institutions at home and abroad have started to devote themselves to the research of digital watermarking technology, and the research results are widely used in real life. Video digital watermarking technology can be mainly divided into video watermarking based on the spatial domain (pixel domain) and video watermarking based on the transform domain [20]. Most video watermarking based on spatial domain has poor robustness, such as the LSB algorithm, which embeds the watermark in the least significant bit of data [21]. It is easy to be removed and challenging to resist attacks. The transform domain-based video watermarking technology can transform the spatial domain to the transform domain, perform image operations on the transform domain, and finally inverse transform to the spatial domain. The above operations can spread the transform to each pixel point in the spatial domain to enhance the robustness.

Currently, the ordinary and practical watermarking algorithms embed the watermark in the transform domain, such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and other methods. However, the two-dimensional wavelet has limited directionality and cannot represent image contours and edge information in the most

efficient sparse form. The Contourlet Transform has been proposed to solve this problem. Literature [22] proposed a zero watermarking algorithm based on Contourlet Transform, which constructs a zero watermarking without changing the video content, and the algorithm is also more robust to most attacks. Zhang et al. [23] proposed a block adaptive compressed sensing reversible watermarking algorithm based on the trade-off between high embedding capacity and invisibility of digital image reversible watermark. Literature [24] proposed robust reversible watermarking technology based on an independent embedding threshold and robust reversible watermarking technology based on the JND threshold in the frequency domain. Naskar and Chakraborty [25] developed a statistical modeling technique to derive a reversible watermarking algorithm based on pixel prediction. The exported metrics and performance trends are apparent, and the developed model is accurate and consistent. Literature [26] proposed a visual watermarking algorithm, which has better transparency and antiattack.

In recent years, with the continuous improvement of digital watermarking technology. The research of the video watermarking algorithm has become the main direction, and a large number of video watermarking algorithms have been proposed. Shukla and Sharma [27] extracted the keyframes of scene changes and embedded the watermark in the low-frequency subband of the three-level DWT. The method has good watermark invisibility, but the watermark embedding capacity needs to be improved. Moreover, the watermark embedding position is always fixed in the low-frequency subband of the video frame. The robustness against various attacks has much room for improvement. Bao and Yang [28] designed a blind video watermarking algorithm combined with DWT-Schur decomposition. The experimental results show that the method has good robustness against noise attacks and video attacks, but the watermark embedding position is fixed. Wang [29] proposed a video watermarking algorithm in the DWT domain based on extreme learning machines, which have better watermark invisibility and can effectively resist multiple attacks. However, the watermark embedding capacity is too small, and the watermark embedding position has been fixed in the low-frequency subband.

For a long time, the research on the algorithm based on video watermarking mainly focused on a single watermarking. The advantages of a single watermarking algorithm are good transparency and clear functions, but a single watermarking sometimes cannot meet different requirements of users. The research of video double watermarking algorithm arises. The video double watermarking algorithm has the characteristics of high transparency and good security, and the double watermarking algorithm in the transform domain has higher transparency and robustness. Therefore, the transform domain double watermarking algorithm has been more widely used.

In literature [30], the whole wavelet transform is first applied to the carrier image, embedding a robust watermark in the low-frequency subband and a fragile watermark in the high-frequency subband. The literature [31] first embeds the robust watermark into the discrete wavelet coefficients of the image

YCbCr color space. Moreover, it embeds the fragile watermark into the least significant bit of the image RGB color space. However, the extraction effect of the two watermarks is not very well. The literature [32] performs DWT on the image, then selects some coefficients to do singular value decomposition, and embeds the robust watermark in the singular values. Finally, they perform quaternion DCT on the image and embed the fragile watermark in the least significant bit of its coefficients. However, this algorithm does not resist crop attacks and rotation attacks well.

Blockchain technology was proposed by Satoshi Nakamoto in a Bitcoin paper, which has attracted widespread attention. It provides an effective solution to solve the digital copyright challenge [33–35]. Blockchain technology and digital copyright protection have a natural fit. Firstly, the blockchain can establish a hard link between user addresses and data objects, which realize data identification and clear ownership of rights and interests. Secondly, the characteristics of tamper-proof, forgery-proof, and traceable data on the chain can provide evidential proof and solidify evidence for digital works.

The current digital copyright protection based on blockchain has been studied in the academic field. The literature [36] designed a digital copyright protection and trading system based on blockchain technology. It uses the consortium blockchain technology to provide full-service digital copyright protection and trading services, such as digital content copyright registration, tracking, authentication, query, and trading. However, this literature only mentions depositing the eigenvalues of digital content into the blockchain. It does not explain for different types of works which digital content eigenvalue extraction technology is used. The literature [37] designed a digital copyright transaction system model based on the consortium blockchain, which can guarantee the immutability and traceability of copyright information. However, it does not describe too much about copyright registration. The literature [38] proposed a Hyperledger-based digital copyright registration model based on blockchain technology, which is mainly for the registration of works in the form of text as the carrier and focuses on the part of copyright registration. The paper [39] proposed a federated audio and video copyright blockchain system based on the improved Practical Byzantine Fault Tolerance algorithm. The literature [40] proposed a distributed digital copyright management mechanism based on a blockchain credit system, which focuses on the copyright transaction process. The scheme achieves the irreversibly encrypted record of the copyright transaction process and makes lightweight adjustments to the data structure of the distributed ledger. In addition, scholars in the literature [41, 42] have proposed new digital rights management schemes by combining digital watermarking technology and blockchain.

3. Video Double Watermarking Copyright Protection Scheme

3.1. Architecture. The architecture of the system is shown in Figure 1, which is mainly divided into client-side, video copyright protection platform, blockchain network, and server-side.

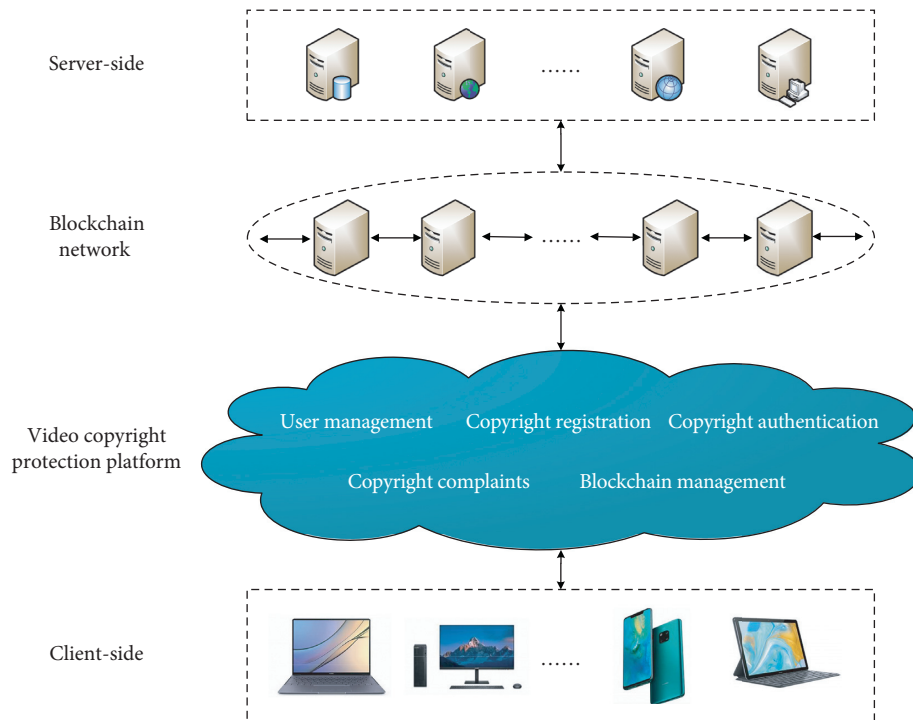


FIGURE 1: Architecture.

- (1) Client-side: this part has encapsulated the complex and abstract transaction logic into a concise and beautiful visual interface to present to users, which has understandable operation logic and well interaction and user operation experience.
- (2) Video copyright protection platform: the platform includes five functional modules, comprising user management, copyright registration, copyright authentication, copyright complaints, and blockchain management. The following is the system process:
 - (i) The users register and become legal users.
 - (ii) The users upload the video to be registered. And the system performs the copyright audit of the video, which uses similarity detection to determine whether the video is registered and whether the watermark meets the requirements. The G component of the video keyframes is processed with the second-level Contourlet Transform. Then, the QR decomposition is performed on the low-frequency subband, and the R matrix is selected as the robust watermark embedding carrier. And the fragile watermark is embedded in the least significant bit of the B component of the video keyframes. After passing the authentication, the signature of the watermark hash digest value and user ID generated by SM2 are uploaded to the blockchain to generate the block. After that, the copyright registration is completed.
 - (iii) The users upload the video to be authenticated and perform copyright detection after extracting keyframes. The platform compares the user watermark with the watermark hash value on the blockchain to realize the binding of user identity and robust watermark. We achieve the matching of the robust watermark with the embedded video by comparing the user watermark with the NC value of the extracted watermark. After that, the copyright authentication is completed.
 - (iv) When users find others have preregistered their videos, they can submit credible proof. If the administrator approves, the platform will transfer the video copyright, upload the transaction information, update the database, and after that complete the copyright complaints.
- (3) Blockchain network: this part is responsible for the erection and management of the Fabric network, including distributed ledger, smart contract, consensus mechanism, and other components, which is the basis for the well operation of blockchain services.
- (4) Server-side: it is the foundation of the platform application services, which are responsible for the client's transactions logic processing and communication with the blockchain network. It includes the processing and execution of functional modules of blockchain management and other services. In addition, it includes MySQL local database and provides security services such as identity authentication and permission management for the platform. We use an enterprise application framework for development, with good security and coupling degree and through the way as "Java back-end to SDK to

blockchain” to achieve efficient communication with the Fabric network.

3.2. Copyright Registration. Copyright registration mainly includes copyright audit, watermark embedding, and identity authentication functions. The process is shown in Figure 2.

(1) Copyright audit:

In copyright registration, keyframes are first extracted from the video. Then, the keyframes are audited for similarity by using the perceptual hash algorithm. User watermarks are also audited in the same way. It is divided into four steps: ① scaling the image; ② converting the grayscale image; ③ calculating DCT; ④ shrinking DCT; ⑤ calculating the difference value; ⑥ calculating the fingerprint. After getting the pHash value of the picture, we compare the hamming distance of the pHash value of the two pictures. Usually, a group of pictures with hamming distance less than 10 is commonly considered as similar pictures.

(2) Watermark embedding:

Users register, become legal users, and then log in to this system. They need to provide the video for copyright registration and the watermark containing personal information, which is the video to be embedded with the watermark and the robust watermark. Firstly, the keyframes of the video to be registered are extracted using the image correlation coefficient method to prepare for embedding the digital watermark. Secondly, the robust watermark is encoded with the hamming code. Thirdly, we embed the robust watermark in the video by using the Contourlet-based digital double watermarking technology, and the fragile watermark is generated by the robust watermark. Furthermore, the video with a double watermark is obtained.

(i) Video keyframe extraction

The image correlation coefficient method is used to measure the similarity of adjacent image frames in the video to realize the extraction of keyframes. Suppose that the video has a total of NOF frames and $i = 1$; then the keyframe extraction steps are as follows:

Step 1: Obtain matrix A by reading frame i of the video.

Step 2: Read the next frame, namely, the matrix B of frame $i + 1$.

Step 3: Use A and B matrixes of the same size to calculate the similarity r of adjacent image frames. If the difference value is greater than a certain threshold, frame i is selected as the keyframes and output i .

Step 4: If $i + 1 > \text{NOF}$, all keyframes of the video have been extracted, otherwise $i = i + 1$, and go back to Step 1.

(ii) Robust watermark preprocessing

Set the binary image W_1 of size $m \times n$ as the robust watermark image. The preprocessing steps are as follows:

Step 1: Transform the binary image W_1 into matrix A with 4 columns and $m \times n/4$ rows (zero padding).

Step 2: Each row of matrix A is coded with (7, 4) hamming code to obtain the matrix A' containing error correction codes, namely, the robust watermark image W_1^* .

(iii) Robust watermark embedding

Set the color image I of size $M \times N$ as the carrier image, and the process of robust watermark embedding is shown in Figure 3.

Detailed steps are as follows:

Step 1: Separate components R, G, and B in the RGB color space model of the color carrier image I. Then, we perform the second-level Contourlet Transform on the component G to extract the second-level low-frequency subband.

Step 2: Divide the second-order low-frequency subband into 4×4 blocks. And we perform QR decomposition of each small block to obtain $(M \times N)/256$ Q matrixes and $(M \times N)/256$ R matrixes.

Step 3: Select element (C_{12}) in row 1 and column 2 as the coefficient value of the embedding position and embed the watermark there.

Step 4: Perform Arnold Transformation (Cat Map) based on the Maximum Entropy Threshold Segmentation for the robust watermark W_1^* to form an encrypted robust watermark, denoted as W_1^{**} .

Step 5: Set the quantization step L as the optimal value 50 obtained in the previous experiment. Then, divide the coefficient value C_{12} at the above embedding position by L to get the quantization value, namely, $q = C_{12}/L$. And then, we embed the robust watermark W_1^{**} into the R matrix to get the matrix R' with robust watermark.

Set the quantization value as q and the pixel value of the encrypted robust watermark as w . If $w = 0$, then the coefficient value C_{12}' of the element (C_{12}) in row 1 and column 2 of R matrix after embedding the watermark is

$$C_{12}' = \begin{cases} q \times L & \text{mod}(q, 2) = 0 \\ (q - 1) \times L & \text{mod}(q, 2) = 1 \end{cases}. \quad (1)$$

If $w = 1$, then the coefficient value C_{12}' of the element (C_{12}) in row 1 and column 2 of R matrix embedded with watermark is

$$C_{12}' = \begin{cases} (q + 1) \times L & \text{mod}(q, 2) = 0 \\ q \times L & \text{mod}(q, 2) = 1 \end{cases}. \quad (2)$$

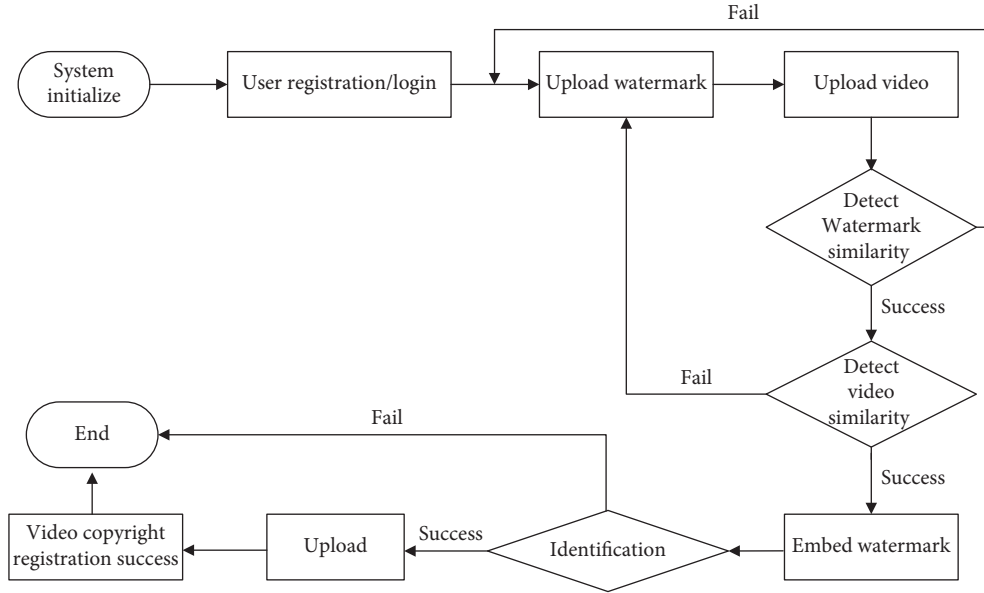


FIGURE 2: Copyright registration.

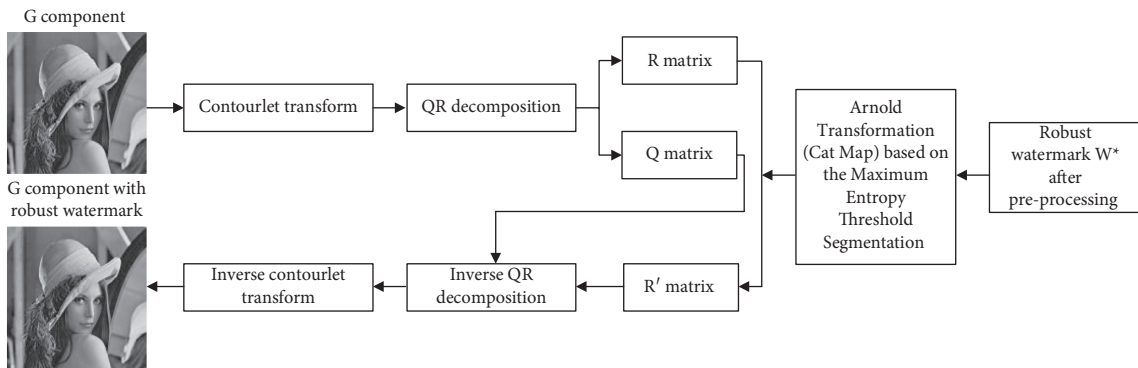


FIGURE 3: Embed robust watermark.

Step 6: perform Inverse QR decomposition on matrix R' embedded with robust watermark. Moreover, the Inverse Contourlet Transformation is performed to obtain component G containing robust watermark, denoted as G^* .

(iv) Fragile watermark embedding

Use the components R and B separated in the robust watermark embedding process and the component G^* containing the robust watermark for the formation and embedding of the fragile watermark. The process of embedding fragile watermarks is shown in Figure 4.

Detailed steps are as follows:

Step 1: Set the least significant bit of the gray value of component B to 0, denoted as B' .

Step 2: Divide the components R , G^* , and B' into 2×2 blocks and calculate the mean value of the three components. The value is changed into 8-bit binary numbers. And the highest 4

bits is extracted to form a 2×2 small matrix to form the fragile watermark W_2 .

Step 3: The fragile watermark W_2 is correspondingly embedded into the least significant bit of the B' component and obtain the B' component containing the fragile watermark, denoted as B^* .

Step 4: Components R and G^* containing robust watermark and B^* containing fragile watermark are combined to form a color image I^* containing double watermark.

(3) Identity authentication:

After the watermark is embedded, SM3 is used to hash the robust watermark and the user ID, respectively. Then, we use the digest value of the user ID as the private key, and SM2 is used to generate the corresponding public key. The robust watermark digest value and user ID are signed with the private key. The public key is used for verification before uploading to the blockchain. If the ID obtained by

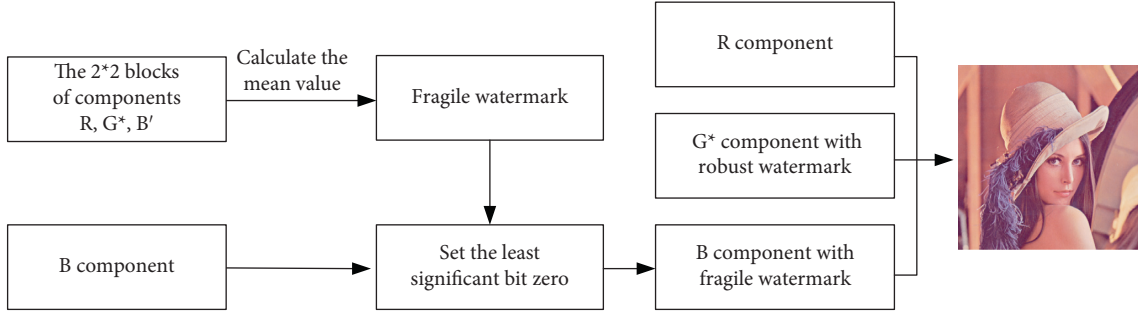


FIGURE 4: Embed fragile watermark.

decryption matches the user's identity, the authentication is passed. And then, the system uploads the signature to the blockchain platform. After that, the copyright registration is completed. On the contrary, it will be refused to upload to the blockchain, failing to complete the copyright registration. The specific process is shown in Figure 5.

3.3. Copyright Authentication. Copyright authentication requires proving the watermark's relevance with the video and the watermark's relevance with the individual. Suppose it is proved that the user's watermark is embedded in the video and the user watermark is owned by the user. Then, the video is also owned by the user. The copyright registration module mainly includes watermark extraction, watermark owner authentication, and video owner authentication. The process is shown in Figure 6.

(1) Watermark extraction

When the users upload the video to be detected, we call the SIFT algorithm to process the video to be detected. Then, we carry out the reverse process of the watermark embedding algorithm. If the extraction fails, it means that the video has not been registered on this platform. If the extraction succeeds, the watermark in the video to be detected is obtained. Whether the watermark is the user's watermark requires further authentication.

The blind watermarking algorithm is used to extract fragile watermark and robust watermark. The process of extracting fragile and robust watermark is shown in Figure 7.

The detailed process of extracting the fragile watermark and robust watermark is as follows:

(i) Fragile watermark extracting:

Step 1: Separate the color channels R , G , and B of the color image with double watermark of size from each other. And we extract the least significant bit of component B and set it to zero to form a fragile watermark matrix W'_2 of size $M \times N$.

Step 2: Divide the components R , G , and B into 2×2 blocks and calculate the mean value.

Moreover, the maximum 4 bits of the mean value are extracted and form a 2×2 small matrix, denoted as T_k ($k = 1, 2, \dots, M \times N/4$). Step 3: Divide fragile watermark matrix W'_2 into 2×2 blocks, denoted as W''_{2k} ($k = 1, 2, \dots, M \times N/4$). If W''_{2k} and T_k are equal, then the k th ($k = 1, 2, \dots, M \times N/4$) small matrix of the positioning matrix L is the null matrix. Otherwise, it is the matrix of all ones.

(ii) Robust watermark extracting

Step 1: Separate the color channels R , G , and B of the color image with double watermarks of size $M \times N$. And we perform a second-level Contourlet Transform on the G component and extract its low-frequency subbands.

Step 2: The low-frequency subbands are divided into 4×4 blocks, and QR decomposition is performed to obtain $(M \times N)/256$ matrix Q' and $(M \times N)/256$ matrix R' .

Step 3: Calculate the quantization value $q' = \text{round}(C'_{12}/L)$ of the coefficient value C'_{12} in row 1 and column 2 of the matrix R' . Among them, L is the quantization step. Furthermore, the extraction of the robust watermark W_{1T} is performed. A pixel value w_{1T} of the extracted robust watermark W_{1T} (undecrypted and with supervisory code) is

$$w_{1T} = \begin{cases} 0 & \text{mod}(q', 2) = 0 \\ 1 & \text{mod}(q', 2) = 1 \end{cases}. \quad (3)$$

Step 4: Firstly, the matrix W_{1T} is decrypted by inverse Arnold Transformation (Cat Map) based on the Maximum Entropy Threshold Segmentation. Then, the robust watermark matrix W'_{1T} containing only the supervisory code is obtained.

Step 5: Transform the robust watermark matrix W'_{1T} with supervisory code into A' with 7 columns and calculate the correctors of each row in the matrix A' .

Step 6: Correct the element values in each row of matrix A' . Then, we extract the first 4 columns of elements in matrix A' and turn them

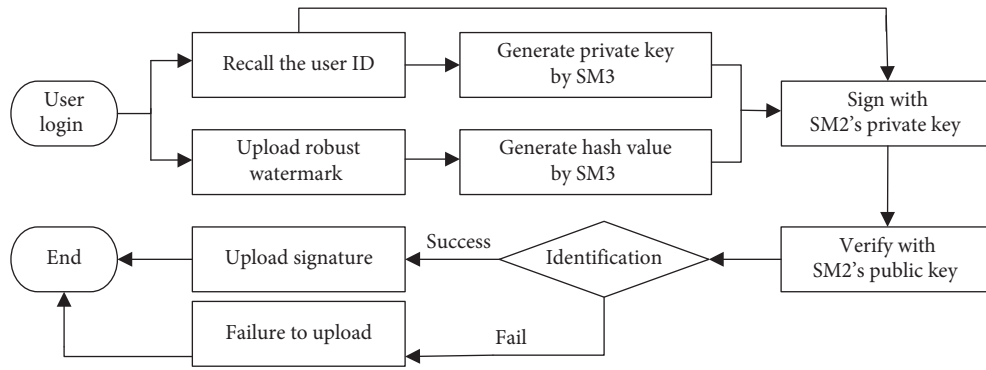


FIGURE 5: Identity authentication.

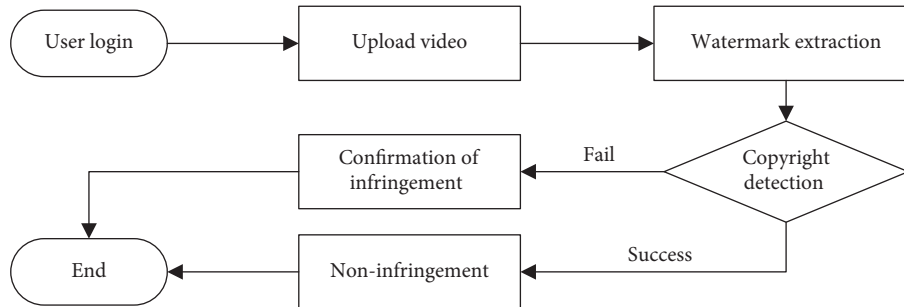


FIGURE 6: Copyright authentication.

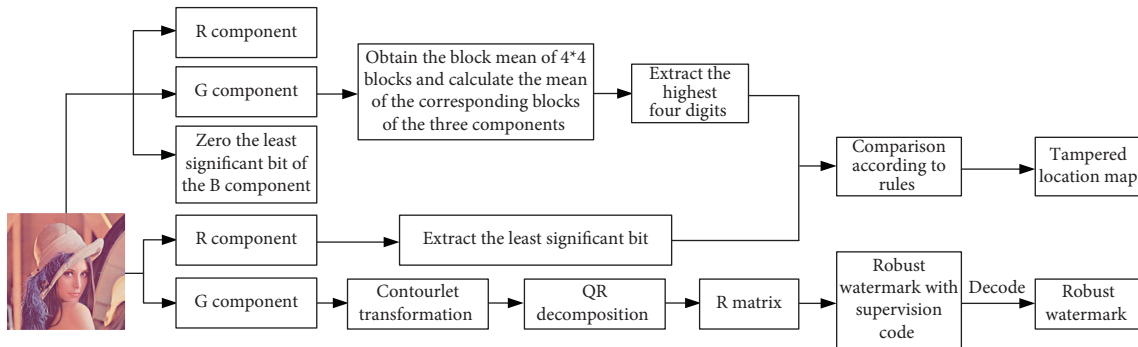


FIGURE 7: Extract watermark.

into a square matrix denoted as W_1' . The robust watermark was finally extracted and restored.

(2) Watermark owner authentication:

Blockchain digital copyright registration mainly relies on the timestamp and the hash value. The timestamp is the added time of data content, once generated, that cannot be falsified and synchronized to the connected block. It is not possible to modify a newly generated block record unless the attackers have at least 51% of the total network capacity, but it is impossible. Consequently, it could ensure the heterogeneity and reliability of the information before and after. We call the corresponding public key through the user ID to verify the signature on the blockchain and obtain the digest value of the watermark and the user ID. Hence, the user watermark is owned by the user,

which proves the correlation between the watermark and the user.

(3) Video owner authentication:

Copyright authentication module requires users to provide the user watermark and the video to be authenticated. If the user stores the user watermark, it is easy to lose. Besides, storing for a long time or after the transmission can easily cause a certain degree of distortion of the watermark image. Therefore, we use the database directly to retrieve the corresponding user watermark. The platform compares the normalized correlation coefficient between the extracted watermark and the user watermark. If the watermark passes the threshold value, it indicates that the watermark in the video is on the blockchain, proving the correlation between the video and the watermark.

3.4. Blockchain Management. We use Hyperledger Fabric to construct the blockchain module. Fabric is a consortium blockchain with features such as permissioned networks, confidential transactions, and pluggable architecture. Only individuals approved to join the blockchain network can participate in transactions. It offers a unique approach to the consensus that enables performance at scale while preserving privacy and can meet the needs of building a video copyright protection platform. Blockchain management is shown in Figure 8.

Node configuration: when building the blockchain, it is required to set the configuration information of different nodes. This module carries out CA authentication for nodes and sets basic configurations such as consensus algorithm and block size in the blockchain configuration file. When necessary, the number of nodes can be dynamically added through node configuration and allowing nodes certified by CA to join the blockchain to build the video copyright protection ecology together.

Channel creating: the channel feature in the Fabric can be used to separate the data of different channels in the ledgers shared by different nodes according to their requirements. In this system, it only needs to complete the basic node configuration and build a channel.

Smart contract deployment: the smart contract in the blockchain needs to be deployed at every node in the channel to be effective. So, the watermark information uploaded to the blockchain needs to be written into the smart contract. And the smart contract needs to be deployed and instantiated.

Copyright information uploading: when the users provide a robust watermark, the video platform will call the copyright information uploading function in the smart contract. And it uploads the signature of the watermark hash digest value and user ID generated by SM2 to the blockchain and generates a block.

When the video platform receives the uploading request, it will issue information to the blockchain module. The blockchain workflow is as follows: ① The transmitting node broadcasts the new watermark digest information to the whole blockchain network. ② The receiving node checks the record information of received data, such as whether the record information is legitimate. After passing the inspection, the data record will be included in a block. ③ All receiving nodes in the whole network perform the consensus algorithm for the block. ④ The block is formally incorporated into the blockchain after processing the consensus algorithm, and each network node achieves agreement on the incorporation of the block. The method of acceptance is to regard the random hash value of the block as the latest block hash value. And the manufacture of new blocks will be extended based on this blockchain.

In the way of uploading data to the blockchain, we choose to adopt the digital signature to store proof. The signature is the hash value of the robust watermark signed by SM2. Its hash value, also known as “digital fingerprint,” can be obtained by hashing the robust watermark. We use SM2 to sign the hash of the robust watermark and the user ID together and upload the signature to the blockchain.

4. Experiment and Analysis

In order to make the experimental results more accurate, we collected and organized 50 different videos in uncompressed MP4 format from the network to carry out the test, mainly taking the “landscape map” video as an example. The frame image is RGB color space with a size of 720×1280 , the data rate is 20,604 kpbs, the total bit rate is 20,604 kpbs, the frame rate is 25.00 frames/sec, the audio sampling frequency is 44.100 kHz, the video size is 41.7 MB, the total number of video frames is 413 frames, and the duration is 17 seconds. The size of the watermark is a 9×12 binary image. The system uses MySQL8.0.22 as the back-end database. Bootstrap is used as the component development framework in the front-end, and the double watermarking processing is mainly implemented in MATLAB. Moreover, Hyperledger Fabric2.3 is used to build the blockchain platform, and the back-end uses IDEA for debugging. Table 1 shows the software and hardware environment.

4.1. Experiment

4.1.1. Blockchain Performance. We use Caliper to test the performance of our blockchain network. Caliper is a blockchain performance testing framework that can test the performance of a blockchain network with a defined set of tests and generate test reports. Caliper supports the tests of transaction success rate, transactions per second (TPS), transaction latency, and resource consumption performance metrics. The blockchain industry standards are shown in Table 2.

The results of the blockchain test are shown in Figure 9. The transaction success rate of this test is 100%, the average transaction delay is 0.71 s (the maximum transaction delay is 2.54 s, and the minimum transaction delay is 0.07 s), and the throughput is 221.2 transactions/second.

The test results show that it conforms to the industry standard.

4.1.2. Commercial Cryptography Algorithm Performance. This system combines SM2 and SM3 with blockchain technology and is mainly applied to the digital signature of transactions. SM3 and SHA-256 are both hash algorithms. SM2 is a public key cryptography algorithm based on the discrete logarithm problem on the elliptic curve, and its key length is 256 bits. To compare SM2 with the international mainstream cryptography algorithm, we select ECC-256, the public key cryptography with the same key length as the comparison object. During the process of digital signature and signature verification, SM2 and ECC use SM3 and SHA-256 to perform hash operations, respectively. Therefore, we will design test experiments on SM2 and ECC to compare the advantages of the blockchain using the commercial cryptography algorithm compared with the ordinary blockchain architecture.

(1) Test environment:

The two algorithms use elliptic curves based on the prime number field, and the equation on the prime number field F_p is

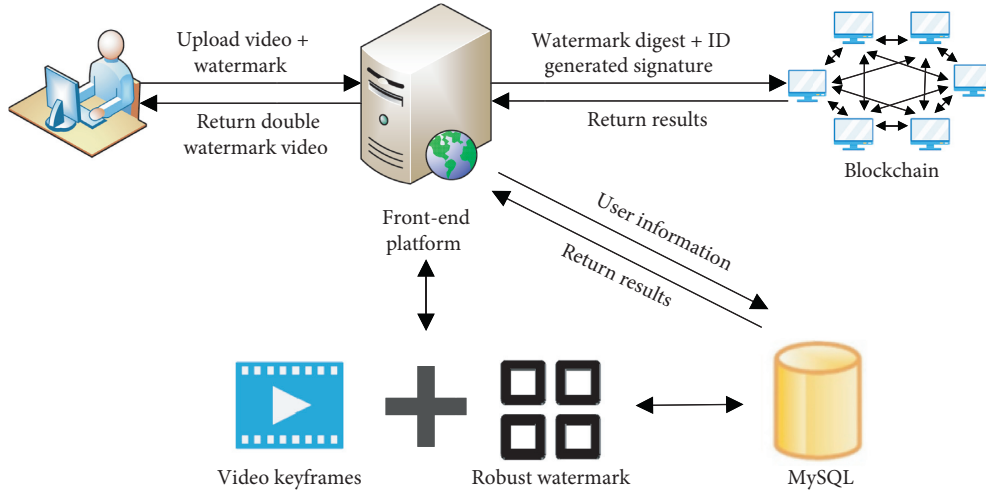


FIGURE 8: Blockchain management.

TABLE 1: Software and hardware environment.

Name	Environment
CPU	i7-10875H
GPU	RTX2080SMQ
Memory	32G
OS	Ubuntu18.04
Blockchain	Fabric2.3
Database	MySQL8.0.22
Watermarking development tool	MATLAB R2018b
Server-side debugging tools	IDEA
Front-end debugging tool	Visual studio code

TABLE 2: Blockchain industry standards.

Rule requirements	Rule item	Requirements
Test scenarios	Stress test	The number of transactions received per second is basically the same as the number of uploads, and the success rate of uploads is higher than 95%
	Spike test	The number of transactions received per second is significantly higher than the number of uploads, and the success rate of uploads is higher than 75%
	Stability test	Low-load operation with no system crashes
Results	Performance indicators	Upload success rate (95%) TPS (>200) average delay time (<0.5 s)

$$y^2 = x^3 + ax + b. \tag{4}$$

Among them, SM2 adopts the commercial cryptography standards, and the parameters are as follows:

$a = 0xFF00000000FFFFFFFFFFFFFFFFFC$
 $b = 0x28E9FA9E9 D9F5E344 D5 A9E4BCF6509 A7F39789F515AB8F92 DD BCB D 414 D940E93$

ECC adopts the secp256k1 curve, and the parameters are as follows:

$a = 0x00$
 $0000000000000000000000000000000000$

$b = 0x00$
 0007

(2) Test method:

We, respectively, use SM2 and ECC to complete 10,000 signing and verifying operations and calculate the time and memory costs of the signing and verifying for 32-byte, 64-byte, and 128-byte strings.

(3) Test results:

(i) Time overhead

As can be seen from Table 3, the SM2 signing and verifying have a faster execution speed. It saves about 20% time compared with the secp256k1 curve adopted in Bitcoin.


```

##test result:##
-----
Name | Succ | Fail | Send Rate (TPS) | Max Latency (s) | Min Latency (s) | Avg Latency (s) | Throughput (TPS) |
-----
writeAsset | 11023 | 0 | 243.1 | 2.54 | 0.67 | 0.71 | 211.2
-----

## resource stats ##
-----
Name | CPU(max) | CPU(avg) | Memory(max) [MB] | Memory(avg) [MB] | Traffic In [MB] | Traffic Out [MB] | Disc Write [MB] | Disc Read [MB] |
-----
dev-peer1.org2.example.com-mycc-1.0 | 2.21 | 1.88 | 9.44 | 9.15 | 8.21 | 2.62 | 0.00 | 0.00 |
dev-peer0.org1.example.com-mycc-1.0 | 2.95 | 1.72 | 12.2 | 11.9 | 8.98 | 3.01 | 0.00 | 0.00 |
dev-peer0.org2.example.com-mycc-1.0 | 2.13 | 1.81 | 10.1 | 10.1 | 0.008479 | 0.008542 | 0.00 | 0.00 |
ctl | 1.32 | 0.97 | 8.35 | 7.45 | 0.00 | 0.00 | 0.00 | 0.00 |
peer0.org2.example.com | 13.23 | 7.94 | 343 | 315 | 34.3 | 0.584 | 102 | 0.00 |
orderer.example.com | 11.19 | 7.47 | 122 | 104 | 36.4 | 69.23 | 70.2 | 0.00 |
peer0.org1.example.com | 20.10 | 16.41 | 334 | 312 | 45.4 | 20.2 | 102 | 0.00 |
peer1.org2.example.com | 21.30 | 15.39 | 326 | 295 | 44.1 | 50.3 | 102 | 0.00 |
peer1.org1.example.com | 13.76 | 9.22 | 331 | 311 | 34.2 | 37.9 | 102 | 0.00 |

```

FIGURE 9: Blockchain performance test.

(ii) Memory overhead

As shown in Table 4, the signing and verifying by SM2 + SM3 take up less memory than the ECC-256 + SHA-256, which saves about 10% of the memory.

4.1.3. Security.

(1) Test indicators

(i) Invisibility:

The test of invisibility of the watermark is described by the peak signal-to-noise ratio (PSNR). The larger the PSNR, the smaller the difference between the two. Conversely, the more significant the difference between the two, the smaller the PSNR. The calculation formula of PSNR is as follows:

$$\text{PSNR}(F, F') = 10 \log_{10} \left(\frac{hw255^2}{\sum_{i=1}^h \sum_{j=1}^w (F_{i,j} - F'_{i,j})^2} \right), \quad (5)$$

where F and F' represent two images and h and w , respectively, represent the number of rows and columns of the image. Generally, if the PSNR is greater than 35 dB, the visual quality of the original video frame is not significantly different from the watermark video frame.

(ii) Robustness:

The NC value can be used to evaluate the robustness of the watermark. After analyzing and summarizing a large number of traditional watermarks related literature data, we conclude that, in the scenario of assuring image quality (the PSNR is greater than 35

TABLE 3: Signing and verifying time of SM2 and ECC-256.

Algorithm	Signing time/s	Verifying time/s
SM2	981	1975
ECC-256	1145	2321

TABLE 4: Memory overhead of the signing and verifying of SM2 and ECC-256.

Algorithm	ROM/Byte	RAM/Byte
SM2	10895	3015
ECC-256	10157	3202

dB), if the NC of the watermark information is higher than 0.85, then this watermarking algorithm could be considered to have robustness.

$$\text{NC}(i, j) = \frac{\sum_{m=1}^M \sum_{n=1}^N T(m, n) S^{ij}(m, n)}{\sqrt{\sum_{m=1}^M \sum_{n=1}^N T^2(m, n) \sum_{m=1}^M \sum_{n=1}^N (S^{ij}(m, n))^2}} \quad (6)$$

Among them, $T(m, n)$ is the n th line from the bottom and the m th pixel value of the template image. $S(i, j)$ is the part covered by the template, which is called the search subgraph, i and j are the image point coordinates in the lower-left corner of the search subgraph in the reference graph S .

(2) Attack tests

(i) Invisibility:

We embedded watermarks on different video frames and tested their PSNR. The detailed results are shown in Table 5.

TABLE 5: Detailed effect display.

Original video frame	Embedded watermark video frame
	 PSNR: 45.706 dB
Original video frame 	Embedded watermark video frame  PSNR: 45.4470 dB
Original video frame 	Embedded watermark video frame  PSNR: 45.9029 dB

TABLE 6: The effect of extracting watermark after the attack.



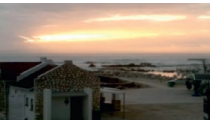


























Original video frame	Embedded watermark	Embedded watermark video frame	Clipped video frame	Extracted watermark
				 NC: 0.9840
Original video frame 	Embedded watermark 	Embedded watermark video frame 	Clipped video frame 	Extracted watermark  NC: 0.9761
Original video frame 	Embedded watermark 	Embedded watermark video frame 	Clipped video frame 	Extracted watermark  NC: 0.9940
Original video frame 	Embedded watermark 	Embedded watermark video frame 	Clipped video frame 	Extracted watermark  NC: 0.9826

TABLE 6: Continued.

Original video frame	Embedded watermark	Embedded watermark video frame	Clipped video frame	Extracted watermark
				 NC: 0.9941

TABLE 7: Statistics of precision rate and recall rate.

Embedded watermark video frame	Embedded watermark video frames after clipping attacks	Location map
	 Precision rate: 95.22%	 Recall rate: 90.68%
	 Precision rate: 96.81%	 Recall rate: 92.63%
	 Precision rate: 85.73%	 Recall rate: 82.66%

As shown in Table 5, the results of PSNR all exceed 45 dB, which indicates that the difference between video frames before and after watermark embedding is slight and the invisibility is well.

(ii) Robustness:

Attacks can be used to detect the actual performance of a system. There are two types of attacks in the actual transmission process: unintentional and intentional. Traditional image attack methods include gamma correction, median filtering, shear attack, rotation attack, histogram equalization, Gaussian noise, motion blur, contrast ratio adjustment, and sharp attack. The attacks against video include frame deletion and frame displacement. Table 6 shows the different attack methods used on video frames, and the NC and PSNR values are tested.

As shown in Table 6, NC values all exceed 0.9. It indicates that the extracted watermark and

embedded watermark have high similarity and well robustness.

(iii) Tampering location:

The system adopts double watermarking technology, in which the fragile watermark can realize the tamper location function. Experiments on deleting, replacing, and adding malicious tampering are carried out to the watermark videos, respectively.

The precision rate and recall rate are used to evaluate and analyze the tamper location results.

$$\begin{aligned} \text{precision rate} &= \frac{AB}{A} \times 100\%, \\ \text{recall rate} &= \frac{AB}{B} \times 100\%. \end{aligned} \tag{7}$$

Among them, A is the area of the location area of the experimental results, B is the area of the real tampering area, and AB is the intersection

of *A* and *B*. Table 7 shows the statistics of precision and recall rate.

As shown in Table 7, for physical attacks, the precision rate is above 95%, and the recall rate is about 90%, which well realizes the tamper location function of the fragile watermark.

4.2. Analysis. Confidentiality. When watermark and video are uploaded to the system, they need to pass similarity detection. After that, performs the hash operation on user ID by SM3 before uploading it to the blockchain platform. The user ID hash is used as the private key, which is used to sign the robust watermark hash and ID and upload the signature to the blockchain. When a copyright query or authentication is performed, the data can be obtained only by decrypting it with its corresponding public key, which realizes the confidentiality of user data. The confidentiality of the system is thus realized.

Integrity. After the user watermark is uploaded to the system, the user watermark and user ID are first hashed, and the user ID hash is used as the private key. The private key is used to sign the robust watermark and ID. Before uploading the signature to the blockchain platform, it needs to be decrypted with its public key to prevent the data from being tampered with and ensure the integrity of the system.

Authenticity. When users register for copyright, they must pass identity authentication before uploading the robust watermark information. Users use the SM2 algorithm to sign the information to be uploaded to the blockchain. The public key is invoked to verify the signature before uploading to the blockchain, ensuring that the user's identity matches the claimed identity.

Nonrepudiation. Blockchain has the characteristics of tamper-proof, openness, and transparency to achieve nonrepudiation. Transactions on the blockchain are organized through the Merkle tree. If any transactions are modified, it will cause some change in the hash value of the Merkle root. Furthermore, the timestamp can prove the order between blocks. Each data in the timestamp is secondary encryption. To tamper with the data, not only break the hash algorithm but also change the timestamp.

5. Conclusion

This paper is based on the double watermarking algorithm on Contourlet and blockchain technology. We generate a fragile watermark based on the robust watermark and embed both in the video. The double watermarking algorithm improves the robustness under the premise of ensuring the invisibility of the watermark and implements the tampering locating function. This system generates the digest value of the robust watermark based on SM3 and signs the digest value and the user ID using SM2. The signature is uploaded to the blockchain after passing the identity authentication, which significantly improves the credibility of the authentication and the security of the system. In the first part, we explain the wide application of video copyright protection and analyze the security threats faced by video copyright and the solutions. The second part introduces

the current research status on video copyright protection at home and abroad. In the third part, we propose a video copyright protection system based on blockchain and double watermarking technology for the shortcomings of the traditional video copyright protection system using digital watermarking technology, such as low security, poor balance, poor robustness, and watermark not bound to individuals. In the fourth part, we test the performance of blockchain and commercial cryptography algorithms. Besides, we test the security of double watermarking and analyze the watermarking systems' confidentiality, integrity, authenticity, and nonrepudiation. The combination of blockchain and watermarking technology optimizes the traditional copyright protection scheme. The adoption of the commercial cryptography algorithm ensures the confidentiality and autonomy of the system. The improvement of the robust watermarking scheme improves the robustness, security, and self-adaptability of the watermark. Moreover, the adoption of improved fragile watermarking realizes the watermarked video integrity identification. The next steps of our job are as follows:

- (1) In view of the low efficiency of the blockchain system itself, the multinode server is adopted to improve the efficiency of the video copyright protection system.
- (2) We will find the best embedding point of the robust watermark to achieve the maximum energy and further improve the robustness of the robust watermark against geometric attacks.
- (3) We will improve the copyright transfer module to realize copyright transactions.

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 Hainan Provincial Natural Science Foundation of China (621RC508 and 620RC563), the Science Project of Hainan University (KYQD(ZR)-21075 and KYQD(ZR)20021), and the National Natural Science Foundation of China (62162020).

References

- [1] S. Xuan, *Research on Copyright Protection of Short Videos*, East China Jiaotong University, Nanchang, China, 2020.
- [2] M. Ning, *Research on Digital Intellectual Property Protection Scheme Based on Blockchain Technology*, Xi'an University of Electronic Science and Technology, Xian, China, 2020.
- [3] Q. Liu, *Design and Implementation of Video Copyright Protection System Based on Blockchain*, Dalian University of Technology, Dalian, China, 2020.

- [4] F. Zhang, *Research on Copyright Protection Method of Stereo Image Video*, Ningbo University, Ningbo, China, 2019.
- [5] Y. Huang, H. Xu, H. Gao, and X. Ma, "SSUR: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 670–681, 2021.
- [6] M. Yang, *Research on Watermark Algorithm for Video Copyright Protection and Content Authentication*, Nanjing University of Posts and Telecommunications, Nanjing, China, 2014.
- [7] J. Hu, *Research on the Legal Protection of the Copyright of Network Film and Television Works*, Yunnan University of Finance and Economics, Kunming, China, 2020.
- [8] H. Hu, *Research on the Legal Issues in Cross-Border M&A of Intellectual Property*, Jilin University, Jilin, China, 2020.
- [9] J. Zhang, A. T. S. Ho, G. Qiu, and P. Marziliano, "Robust video watermarking of H.264/AVC," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 54, no. 2, pp. 205–209, 2007.
- [10] H. Gao, X. Qin, J. D. B. Ramon, W. Hussain, and Y. Xu, "Collaborative learning-based industrial IoT API recommendation for software-defined devices: the implicit knowledge discovery perspective," *IEEE Transactions on Emerging Topics in Computational Intelligence (TETCI)*, 2020.
- [11] M. Asikuzzaman and M. R. Pickering, "An overview of digital video watermarking," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 9, pp. 2131–2153, 2018.
- [12] J. Xiao, H. Xu, H. Gao, M. Bian, and L. Yang, "A weakly supervised semantic segmentation network by aggregating seed cues: the multi-object proposal generation perspective," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 17, no. 1, pp. 1–19, 2021.
- [13] X. Yang, S. Zhou, and M. Cao, "An approach to alleviate the sparsity problem of hybrid collaborative filtering based recommendations: the product-attribute perspective from user reviews," *Mobile Networks and Applications*, vol. 25, no. 2, pp. 376–390, 2020.
- [14] L. Li, *Research on Digital Copyright Protection Based on Blockchain Technology*, East China Jiaotong University, Jiaotong, China, 2020.
- [15] H. Gao, K. Xu, M. Cao, J. Xiao, Q. Xu, and Y. Yin, "The deep features and attention mechanism based method to dish healthcare under social IoT systems: an empirical study with a hand-deep local-global net," *IEEE Transactions on Computational Social Systems (TCSS)*, 2021.
- [16] T. Wu, *The Design and Implementation of Copyright Registration System Based on Blockchain*, Nanjing University of Posts and Telecommunications, Nanjing, China, 2019.
- [17] J. Shi, *Research and Implementation of Image Digital Copyright Protection Based on Blockchain and SIFT*, Beijing University of Posts and Telecommunications, Beijing, China, 2020.
- [18] Y. Yin, Z. Cao, Y. Xu, H. Gao, R. Li, and Z. Mai, "QoS prediction for service recommendation with features learning in mobile edge computing environment," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 4, pp. 1136–1145, 2020.
- [19] R. G. V. Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Proceedings of the 1st International Conference on Image Processing*, vol. 2, pp. 86–90, Austin, TX, USA, November 1994.
- [20] X. Liu, "An overview of digital video watermarking," *Video Engineering*, vol. 44, no. 5, pp. 11–15, 2020.
- [21] A. D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Processing Letters*, vol. 12, no. 6, pp. 441–444, 2005.
- [22] X. Chen, G. Bu, and H. Li, "A video zero-watermark algorithm based on the contourlet transform," in *Proceedings of the 3rd International Conference on Multimedia (ICMT 2013)*, pp. 216–223, Dallas, Texas, USA, April 2013.
- [23] Q. Zhang, Y. Sun, and Y. Yan, "A reversible watermark algorithm based on block Adaptive compressed sensing," *Journal of Electronics and Information Technology*, vol. 35, no. 4, pp. 797–804, 2016.
- [24] X. Miao, T. Zhu, Y. Liu, Y. Lai, and W. Liu, "Double watermark algorithm for color images based on contourlet transform," *Journal of Xi'an University of Posts and Telecommunications*, vol. 23, no. 5, pp. 77–84, 2018.
- [25] R. Naskar and R. S. Chakraborty, "A technique to evaluate upper bounds on performance of pixel-prediction based reversible watermarking algorithms," *Journal of Signal Processing Systems*, vol. 82, no. 3, pp. 373–389, 2016.
- [26] T. Li, R. Sun, and C. Xu, "Video watermarking based on pseudo-3D-DCT in Contourlet domain," *Journal of Electronic Measurement and Instrument*, vol. 25, no. 8, pp. 734–740, 2011.
- [27] D. Shukla and M. Sharma, "Robust scene-based digital video watermarking scheme using level-3 DWT: approach, evaluation, and experimentation," *Radioelectronics and Communications Systems*, vol. 61, no. 1, pp. 1–12, 2018.
- [28] S. Bao and S. Yang, "Total-blind digital video watermarking algorithm based on DWT-schur," *Journal of Chongqing University of Technology (Natural Science)*, vol. 33, no. 10, pp. 136–141, 2019.
- [29] Y. L. Wang, "Video watermarking algorithm based on extreme learning machine and discrete wavelet transform," *Chinese Journal of Liquid Crystals and Displays*, vol. 35, no. 2, pp. 180–188, 2020.
- [30] L. Baiying, Z. Xin, H. Lei et al., "Multipurpose watermarking scheme via intelligent method and chaotic map," *Multimedia Tools and Applications*, vol. 78, no. 19, Article ID 27107, 2019.
- [31] X. Liu, C. Lin, and S. Yuan, "Blind dual watermarking for color images' authentication and copyright protection," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 5, pp. 1047–1055, 2018.
- [32] S. Chen, R. Qi, and Y. Tang, "Multi-purpose watermark algorithm for color image based on multiple transform domains," *Journal of Computer Applications*, vol. 38, no. 8, pp. 2274–2279+2286, 2018.
- [33] X. Lv, *Design and Implementation of Content-Publishing Platform Based on Blockchain*, Beijing University of Posts and Telecommunications, Beijing, China, 2020.
- [34] L. Zhang, M. Peng, W. Wang, Z. Jin, Y. Su, and H. Chen, "Secure and efficient data storage and sharing scheme for blockchain-based mobile-edge computing," *Transaction Emerging Telecommunication Technology*, vol. 32, no. 5, 2021.
- [35] H. Xiong, "On the design of blockchain-based ECDSA with fault-tolerant batch verification protocol for blockchain-enabled IoMT," *IEEE Journal of Biomedical and Health Informatics*, p. 1, 2021.
- [36] C. Li, B. Dai, H. Wang, and X. Wang, "Digital copyright protection and trading system based on blockchain technology," *Modern Computer*, vol. 29, pp. 80–84, 2018.
- [37] L. Li, S. Zhou, Q. Liu, and D. He, "Blockchain-based digital copyright trading system," *Chinese Journal of Network and Information Security*, vol. 4, no. 7, pp. 22–29, 2018.

- [38] G. Zhao, Y. He, and J. Zhou, "Digital copyright registration technology based on blockchain," *Information Technology and Network Security*, vol. 38, no. 4, pp. 79–83, 2019.
- [39] Z. Chen, Q. Li, J. Gan, C. Zhang, and Z. Li, "VC chain: an alliance audio-video copyright blockchain system," *Computer Engineering & Science*, vol. 41, no. 11, pp. 1939–1948, 2019.
- [40] R. Zhou and L. Qian, "Blockchain based digital right management for distributed content delivery network," *Application Research of Computers*, vol. 37, no. 6, pp. 1794–1798, 2020.
- [41] W. Wang and Z. Ye, "Application of blockchain technology in the financing of digital publishing supply chain," *Publishing Research*, vol. 8, pp. 31–34, 2018.
- [42] R. Xu, L. Zhang, H. Zhao, and Y. Peng, "Design of network media's digital rights management scheme based on blockchain technology," in *Proceedings of the 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)*, pp. 128–133, Bangkok, Thailand, March 2017.

Research Article

Joint Design of Beamforming and Edge Caching in Fog Radio Access Networks

Wenjing Lv,¹ Rui Wang ,^{1,2} Jun Wu ,^{3,4} Zhijun Fang,⁵ and Songlin Cheng ⁶

¹College of Electronics and Information Engineering, Tongji University, Shanghai 201804, China

²Shanghai Institute of Intelligent Science and Technology, Tongji University, Shanghai 201804, China

³School of Computer Science, Fudan University, Shanghai, China

⁴Peng Cheng Laboratory, Shenzhen, China

⁵College of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China

⁶Department of Arts and Sciences, Shanghai Dianji University, Shanghai 201306, China

Correspondence should be addressed to Rui Wang; ruiwang@tongji.edu.cn

Received 16 August 2021; Accepted 30 August 2021; Published 18 September 2021

Academic Editor: Honghao Gao

Copyright © 2021 Wenjing Lv 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 study a novel transmission framework based on statistical channel state information (SCSI) by incorporating edge caching and beamforming in a fog radio access network (F-RAN) architecture. By optimizing the statistical beamforming and edge caching, we formulate a comprehensive nonconvex optimization problem to minimize the backhaul cost subject to the BS transmission power, limited caching capacity, and quality-of-service (QoS) constraints. By approximating the problem using the l_0 -norm, Taylor series expansion, and other processing techniques, we provide a tailored second-order cone programming (SOCP) algorithm for the unicast transmission scenario and a successive linear approximation (SLA) algorithm for the joint unicast and multicast transmission scenario. This is the first attempt at the joint design of statistical beamforming and edge caching based on SCSI under the F-RAN architecture.

1. Introduction

5G is being commercially deployed, while the mobile communication networks still face some challenges. Spectrum resources are scarce, network services are emerging, and the costs of operation are surging. These dilemmas have stimulated the industry and academia to explore novel network technology and wireless technology to support diversified scenarios [1].

From the network technology perspective, exploring a new intelligent wireless access network architecture is sustainable for solving the huge capacity demand of wireless networks. The fog radio access network (F-RAN) architecture is a promising network architecture in next-generation mobile communications [2]. In the F-RAN, the edge nodes, which have functions of storage and CRRM, are collectively evolved to fog access points (F-APs). It is critical that the upgraded F-APs [3] equipped with

functions of storage and cooperative radio resource management (CRRM) can be used to store part of the contents sent by the cloud server [4], which shortens the distance between the content data and the users and relieves the pressure of large data transmission on the backhaul link in the F-RAN [5]. In a word, the F-RAN can achieve better network performance gains by deploying more functions at the F-APs [6]. Users can finally receive the required services in the F-RAN architecture at a faster speed as well as by consuming less power. The technologies deployed in the F-RAN architecture involve edge caching allocation, resource scheduling, and advanced technologies such as massive multiple-input multiple-output (MIMO) and caching strategy. Current corresponding research topics based on the F-RAN architecture are generally reflected on two timescales: delivery-level design from a short timescale or caching-level design from a long timescale.

From the wireless technology perspective, beamforming technology based on multiple antennas can improve the energy efficiency and spectrum efficiency. The existing beamforming problems are generally NP-hard. The corresponding algorithms suffer from poor scalability and high computational complexity in large-scale wireless systems [7]. Even in a basic single-cell single-group multicast transmission scenario, the multicast beamforming design problem is NP-hard. Sidiropoulos et al. [8] obtained a high-quality approximate solution based on Gaussian randomization and semidefinite relaxation (SDR). Wang et al. [9] proposed a global beamforming algorithm named second-order cone programming (SOCP) in multiuser two-way relay systems, while the application scenarios of using this algorithm are limited. Later, Lu and Liu in [10] proposed a global algorithm named the branch-and-bound (BB) algorithm for a multicast beamforming scenario. However, the complexity of these beamforming algorithms usually increases when the network scale increases.

Recently, the team of Tao in [11] studied a content-centric physical layer beamforming framework under the cloud radio access network (C-RAN) architecture. It is aimed at overcoming dilemmas of repeated content transmission in connection-oriented traditional communication architectures. Tao et al. [11] considered only a multicast beamforming design under the C-RAN architecture. From a different research perspective, Chen et al. [12] studied a similar problem but proposed a joint beamforming and BS clustering framework for nonorthogonal unicast and multicast scenarios. They adopted a two-layered-division-multiplexing structure to concurrently achieve unicast and multicast services with different beamformers. Although [11, 12] involve the design of both cache-level and delivery-level strategies, neither works consider the joint optimization of caching and beamforming. The main difficulty is that the optimizations over the caching allocation and traditional beamforming strategy generally occur on different timescales. Traditional beamforming adapts to short-term instantaneous channel information, while caching is generally optimized at the cache allocation phase, which is in the context of a long timescale [13]. Thus, it remains challenging to simultaneously optimize the mixed-timescale beamforming and caching strategy in the F-RAN architecture.

In this article, we present a compromise scheme based on statistical channel state information (SCSI) to address this mixed-timescale deployment problem in the F-RAN architecture. The major contributions are concluded as follows:

- (i) *Joint Framework Based on SCSI.* We first propose a joint framework based on SCSI under the F-RAN architecture. Moreover, our research includes the unicast scenario and the joint nonorthogonal unicast and multicast transmission scenario.
- (ii) *Problem Formulation.* A multiobjective optimization problem is further formulated. Then, we reformulate the nonconvex problems by introducing the l_0 -norm, the approximation of the smooth function, and some other mathematical processing techniques.

- (iii) *Tailored Algorithm.* To solve these problems, we provide a tailored SOCP algorithm for unicast transmission scenarios and a successive linear approximation (SLA) algorithm for the joint unicast and multicast transmission scenario.

- (iv) *Simulation.* Simulation experiments illustrate the effectiveness of the algorithms and show that the joint beamforming-caching is better than the single scheme.

2. System Model and Problem Formulation

2.1. Network Architecture. We study a content-centric transmission framework based on SCSI in the F-RAN. Consider the downlink transmission with K single-antenna users and N multiple-antenna BSs. Each BS has L antennas and a limited-capacity cache with storage Q_n for $n \in \mathcal{N} \triangleq \{1, \dots, N\}$. There are two paths for F-APs to acquire the requested information: the central processor (CP) through the backhaul links or its local cache. BSs can dynamically provide mixed multicast and unicast services. Each user can subscribe to group-specific multicast services and a dedicated unicast request. The users who request the same file can be considered as a group. Each group is served by a BS cluster. The system model is shown in Figure 1. Different transmission mechanisms are shown in Figure 2.

We denote Φ_m to represent the users of group m , $m \in \mathcal{M} \triangleq \{1, 2, \dots, M\}$. In addition, $s_{m,n} = 1$ denotes that the n th BS serves the m th group, and $s_{m,n} = 0$ denotes that the n th BS does not serve the m th group. Similarly, $s_{k,n} = 1$ denotes that the n th BS serves for the k th user; otherwise, $s_{k,n} = 0$. $C_{(k,z),n} = 1$ denotes that the k th user-requested file z has been cached in advance in the n th BS; otherwise, $C_{(k,z),n} = 0$. Correspondingly, $\hat{C}_{(m,z),n} = 1$ denotes that the m th-group-requested file z has been cached in advance in the n th BS; otherwise, $\hat{C}_{(m,z),n} = 0$. The BS cluster serving group m is marked by Ψ_m , $m \in \mathcal{M}$. The channel vectors from all BSs to user k can be written into a wide vector $\mathbf{h}_k = [\mathbf{h}_{k,1}^H, \mathbf{h}_{k,2}^H, \dots, \mathbf{h}_{k,N}^H]^H \in \mathbb{C}^{NL \times 1}$. Similarly, $\mathbf{v}_k \in \mathbb{C}^{NL \times 1}$, $k \in \mathcal{K} \triangleq \{1, 2, \dots, K\}$, and $\mathbf{w}_m \in \mathbb{C}^{NL \times 1}$, $m \in \{0\} \cup \mathcal{M}$, are the network-wide beamforming vectors for the unicast message and multicast message, respectively. Note that $\lambda = [\lambda_1, \lambda_2, \dots, \lambda_K]$ and $\gamma = [\gamma_0, \gamma_1, \gamma_2, \dots, \gamma_M]$ are the SINR vectors, where each element is the minimum required by user k and group m . Correspondingly, the transmission rate is set as $R_k = B \log(1 + \lambda_k)$ or $R_m = B \log(1 + \gamma_m)$, where B denotes the total available bandwidth. The database of Z contents is denoted as $\mathcal{X} \triangleq \{1, 2, \dots, Z\}$, and each file's size is normalized to 1. The popular files can be cached in BSs in advance according to the popularity of the z th content file, which follows a Zipf distribution: $p_z = z^{-r} / \sum_{j=1}^Z j^{-r}$.

2.2. Cost Model. The system cost consists of two parts: backhaul cost and transmission power consumption. The backhaul consumption is generally proportional to its transmission capacity and related to the cache, user's request, and matching service between RRs and the user. It is

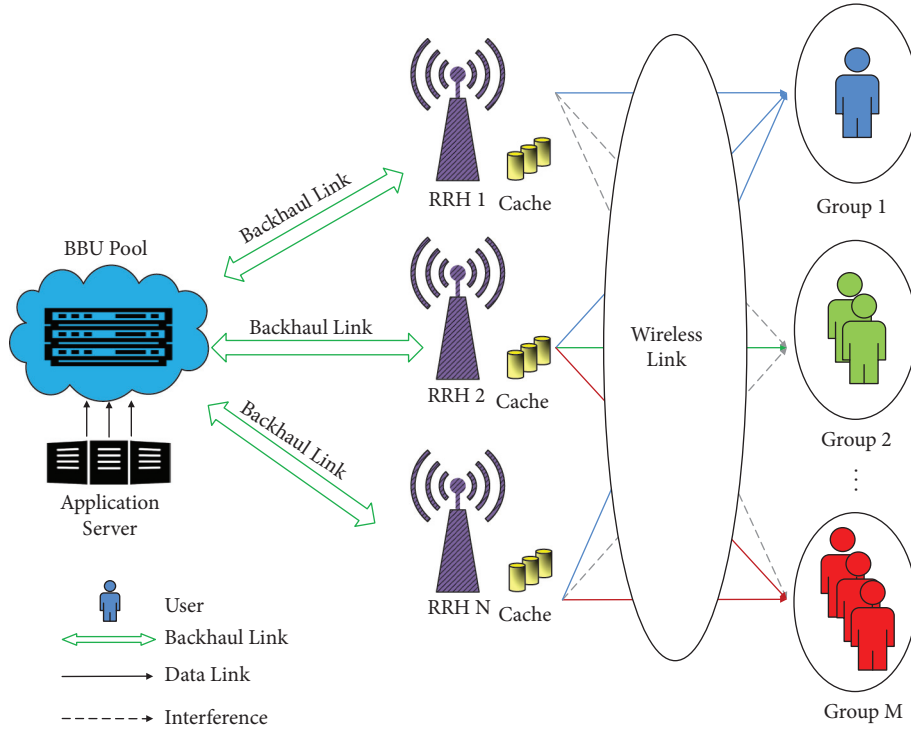


FIGURE 1: The system model based on the F-RAN architecture.

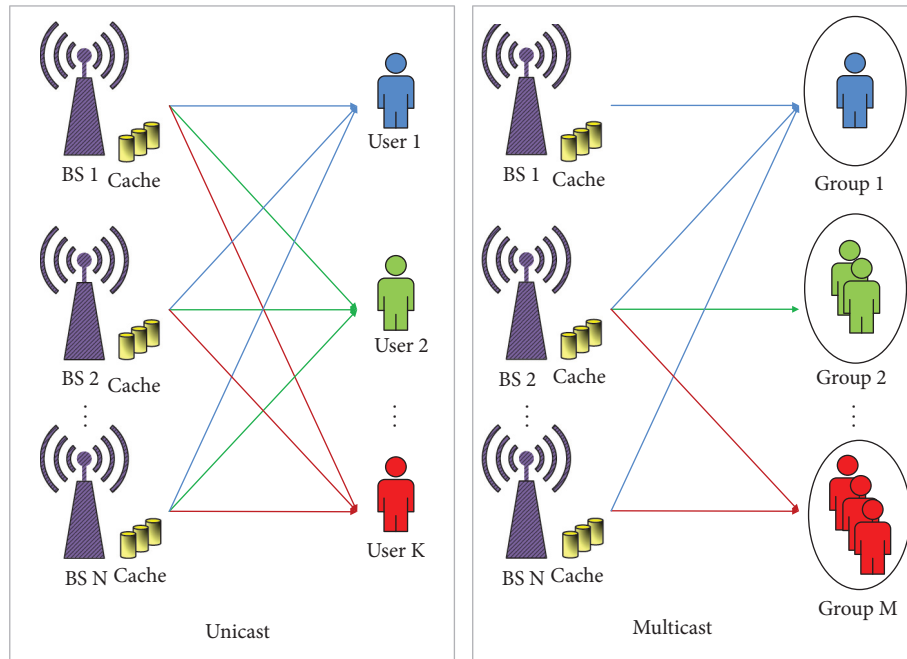


FIGURE 2: Different transmission modes.

worth remarking that if the file has been cached in advance in the BS, it can access the file directly and will not produce the backhaul link cost. Otherwise, it will produce extra backhaul cost. Thus, we use these variables to formulate the objective function on the backhaul cost. Specifically, for the unicast scenario, the system backhaul cost can be modeled as

$$P_B = \sum_{k=1}^K \sum_{n=1}^N s_{k,n} (1 - C_{(k,z),n}) R_k. \quad (1)$$

For the hybrid unicast-multicast scenario, the system backhaul cost consists of T_{B_1} and T_{B_2} , where

$$T_{B_1} = \frac{1}{K} \sum_{z=1}^Z \frac{z^{-\alpha}}{\sum_{j=1}^Z j^{-\alpha}} \sum_{k=1}^K \sum_{n=1}^N s_{k,n} (1 - C_{(k,z),n}) R_k, \quad (2)$$

$$T_{B_2} = \frac{1}{M} \sum_{z=1}^Z \frac{z^{-\alpha}}{\sum_{j=1}^Z j^{-\alpha}} \sum_{m=1}^M \sum_{n=1}^N \hat{s}_{m,n} (1 - \hat{C}_{(m,z),n}) R_m.$$

Additionally, the total BS transmission power can be expressed as a function of beamforming \mathbf{w} or \mathbf{v} . In the unicast scenario, it can be written as

$$P_{F_1} = \sum_{k=1}^K \sum_{n=1}^N \|\mathbf{v}_{k,n}\|_2^2. \quad (3)$$

In the hybrid unicast-multicast scenario, it can be written as

$$P_{F_2} = \sum_{k=1}^K \sum_{n=1}^N \|\mathbf{v}_{k,n}\|_2^2 + \sum_{m=1}^M \sum_{n=1}^N \|\mathbf{w}_{m,n}\|_2^2. \quad (4)$$

The maximum of all BSs' available power is limited to P_f .

2.3. Problem Formulation. The joint design of beamforming and edge caching is deployed based on statistical channel state information. We focus on a cost goal aimed at minimizing the backhaul cost limited to the transmission power, the SINR constraints, and the limited caching capacity. It is different for the transmission modes between the unicast scenario and the joint unicast-multicast scenario. In the joint unicast-multicast scenario, there are both unicast and multicast modes as shown in Figure 2.

- (1) In the unicast scenario, we first study a special case; suppose that there is only one user in each group which is named as a unicast scenario. The received message of the k th user can be written as follows:

$$y_k = h_k^H v_k x_k + \sum_{j=1, j \neq k}^K h_k^H v_j x_j + n_k, \quad \forall k \in \mathcal{K}, \quad (5)$$

where $n_k \sim \mathcal{CN}(0, \sigma_k^2)$ represents the white Gaussian noise, $k \in \mathcal{K}$. Accordingly, user's SINRs can be defined as follows:

$$\text{SINR}_k = \frac{|\mathbf{h}_k^H \mathbf{v}_k|^2}{\sum_{j=1, j \neq k}^K |\mathbf{h}_k^H \mathbf{v}_j|^2 + \sigma_k^2}, \quad \forall k \in \mathcal{K}. \quad (6)$$

We make an average operation on the channel state information. Then, we get the SINR expression of the k th user:

$$\mathbb{E}(\text{SINR}_k) \geq \lambda_k, \quad (7)$$

and it can be written approximately as follows:

$$\frac{\mathbf{v}_k^H \mathbb{E}(\mathbf{h}_k \mathbf{h}_k^H) \mathbf{v}_k}{\sum_{j=1, j \neq k}^K \mathbf{v}_j^H \mathbb{E}(\mathbf{h}_k \mathbf{h}_k^H) \mathbf{v}_j + \sigma_k^2} \geq \lambda_k. \quad (8)$$

The system backhaul cost is written as

$$P_B = \sum_{k=1}^K \sum_{n=1}^N s_{k,n} (1 - C_{(k,z),n}) R_k. \quad (9)$$

The total transmission power consumption is

$$P_F = \sum_{k=1}^K \sum_{n=1}^N \|\mathbf{v}_{k,n}\|_2^2. \quad (10)$$

In the unicast scenario, the optimized problem based on statistical channel state information can be formulated as follows:

$$P^U: \quad \min_{\{\mathbf{v}_{k,n}, s_{k,n}, C_{(k,z),n}\}} \frac{1}{K} \sum_{z=1}^Z \frac{z^{-\alpha}}{\sum_{j=1}^Z j^{-\alpha}} P_B, \quad (11a)$$

$$s.t. \quad \sum_{k=1}^K \sum_{n=1}^N \|\mathbf{v}_{k,n}\|_2^2 \leq P_f, \quad (11b)$$

$$\frac{\mathbf{v}_k^H \mathbb{E}(\mathbf{h}_k \mathbf{h}_k^H) \mathbf{v}_k}{\sum_{j=1, j \neq k}^K \mathbf{v}_j^H \mathbb{E}(\mathbf{h}_k \mathbf{h}_k^H) \mathbf{v}_j + \sigma_k^2} \geq \lambda_k, \quad \forall k \in \mathcal{K}, \quad (11c)$$

$$\sum_{(k,z)} C_{(k,z),n} \leq Q_n, \quad \forall n \in \mathcal{N}. \quad (11d)$$

- (2) Hybrid unicast and multicast scenario: users requesting the same file can be regarded as a small group and served using multicast beamforming as shown in Figure 2. We next study the joint non-orthogonal unicast and multicast transmission scenario. Suppose that the multicast message is first decoded, and then the unicast message is decoded by subtracting the multicast message in advance. We can successively decode the mixed multicast and unicast signal based on statistical channel state information. The signals from other users and groups are treated as interference. The SINRs of the unicast and the multicast are defined as follows:

$$\text{SINR}_k^U = \frac{|\mathbf{h}_k^H \mathbf{v}_k|^2}{\sum_{i=1, i \neq m}^M |\mathbf{h}_k^H \mathbf{w}_i|^2 + \sum_{j=1, j \neq k}^K |\mathbf{h}_k^H \mathbf{v}_j|^2 + \sigma_k^2}, \quad \forall k \in \mathcal{K},$$

$$\text{SINR}_k^M = \frac{|\mathbf{h}_k^H \mathbf{w}_m|^2}{\sum_{i=1, i \neq m}^M |\mathbf{h}_k^H \mathbf{w}_i|^2 + \sum_{j=1}^K |\mathbf{h}_k^H \mathbf{v}_j|^2 + \sigma_k^2}, \quad \forall k \in \Phi_m. \quad (12)$$

The system backhaul cost consists of T_{B_1} and T_{B_2} , where T_{B_1} is

$$T_{B_1} = \frac{1}{K} \sum_{z=1}^Z \frac{z^{-\alpha}}{\sum_{j=1}^Z j^{-\alpha}} \sum_{k=1}^K \sum_{n=1}^N s_{k,n} (1 - C_{(k,z),n}) R_k \quad (13)$$

and T_{B_2} is

$$T_{B_2} = \frac{1}{M} \sum_{z=1}^Z \frac{z^{-\alpha}}{\sum_{j=1}^Z j^{-\alpha}} \sum_{m=1}^M \sum_{n=1}^N \hat{s}_{m,n} \left(1 - \hat{C}_{(m,z),n}\right) R_m. \quad (14)$$

The optimized problem based on statistical channel state information is formulated as follows:

$$P^{UM}: \quad (15a)$$

$$\min_{\{\mathbf{v}_{k,n}, \mathbf{w}_{m,n}, s_{k,n}, \hat{s}_{m,n}, C_{(k,z),n}, \hat{C}_{(m,z),n}\}} T_{B_1} + T_{B_2}, \quad (15a)$$

$$\text{s.t.} \quad \sum_{k=1}^K \sum_{n=1}^N \|\mathbf{v}_{k,n}\|_2^2 + \sum_{m=1}^M \sum_{n=1}^N \|\mathbf{w}_{m,n}\|_2^2 \leq P_f, \quad (15b)$$

$$\mathbb{E}(\text{SINR}_k^U) \geq \lambda_k, \quad \forall k \in \mathcal{K}, \quad (15c)$$

$$\mathbb{E}(\text{SINR}_k^M) \geq \gamma_m, \quad \forall k \in \Phi_m, \quad (15d)$$

$$\sum_{(k,z)} C_{(k,z),n} + \sum_{(m,z)} \hat{C}_{(m,z),n} \leq Q_n, \quad \forall n \in \mathcal{N}. \quad (15e)$$

Due to the combinatorial nature of different variables from multiple levels, to solve the above problems P^U , P^{UM} is still a challenge.

3. Proposed Algorithms for Different Scenarios

To address the aforementioned challenges, we explore a tailored second-order cone programming (SOCP) algorithm for the unicast transmission scenario and a successive linear approximation (SLA) algorithm for the mixed unicast and multicast transmission scenario. In this section, we first reformulate problems as an edge caching and statistical beamforming optimization problem by introducing l_0 -norm approximation, Taylor approximation, and some other techniques. Then, we provide the detailed algorithms in the next section.

For one thing, we reformulate a sparse and tractable beamforming problem equivalently. Denote

$$\hat{s}_{m,n} = \begin{cases} 0 & \text{if } \hat{C}_{(m,z),n} = 0, \\ 0 \text{ or } 1 & \text{if } \hat{C}_{(m,z),n} = 1. \end{cases} \quad (16)$$

$\hat{s}_{m,n}$ can be substituted by the l_0 -norm:

$$\hat{s}_{m,n} = \|\|\mathbf{w}_{m,n}\|_2\|_0. \quad (17a)$$

Similarly, we have

$$s_{k,n} = \|\|\mathbf{v}_{k,n}\|_2\|_0. \quad (17b)$$

By substituting (17a) and (17b) into (11a) and (15a), the corresponding problems can be transformed into two equivalent sparse problems with sparsity from the l_0 -norm.

For another thing, the discontinuous l_0 -norm in the objective functions can be taken place by a continuous function. Specifically, we choose the next frequently used smooth logarithmic concave function:

$$f_\theta(x) = \frac{\log(x/\theta + 1)}{\log(1/\theta + 1)}. \quad (18)$$

Here, θ is a parameter that characterizes the smoothness. Its first-order Taylor expansions $\tilde{f}_\theta(x)$ can be written as follows:

$$\tilde{f}_\theta(x) = \frac{\log(x_0/\theta + 1)}{\log(1/\theta + 1)} + \frac{1}{x_0 + \theta} \cdot \frac{1}{\log(1/\theta + 1)} \cdot (x - x_0). \quad (19)$$

In addition, we denote $\mathbb{E}(\mathbf{h}_k \mathbf{h}_k^H) = \Sigma_k$; if the condition $\text{rank}(\Sigma_k) = 1$ is satisfied, we have the decomposition formula $\Sigma_k = \mathbf{H}_k \mathbf{H}_k^H$. Based on the above processing, the formulated optimization problems can be, respectively, solved by using different optimization algorithms. The details of the tailored algorithms are described as follows.

3.1. SOCP-Based Optimal Algorithm for the Unicast Scenario.

Considering nonconvex SINR (11c), without loss of optimality, there always exists a phase shift version making the formula $\mathbf{H}_k^H \mathbf{v}_k$ to be real as well as positive; that is, multiplying a phase shift transformation $e^{j\theta}$ will not affect the value of the objective function and still keep the constraints satisfied, and we can get $\mathbf{H}_k^H \mathbf{v}_k \geq \sqrt{\gamma_k} / \gamma_k + 1 \cdot \sqrt{\sum_{j=1}^K |\mathbf{H}_k^H \mathbf{v}_j|^2 + \sigma_k^2} \mathfrak{I}\{\mathbf{H}_k^H \mathbf{v}_k\} = 0, \quad \forall k \in \{1, 2, \dots, K\}$. This formula can be further written as a standard second-order cone (SOC) constraint form: $\|\mathbf{A}_k \mathbf{x} + \mathbf{b}_k\| \leq \mathbf{c}^T \mathbf{x} + d$. In addition, we denote $C_{B_2} = \tilde{f}_\theta(\|\mathbf{I}_n(\mathbf{E}_k \mathbf{X})\|_2^2) (1 - C_{(k,z),n}) R_k$. Then, the problem P^U can be written as follows:

$$P_U: \quad (20a)$$

$$\min_{\{\mathbf{x}, C_{(k,z),n}\}} \frac{1}{K} \sum_{z=1}^Z \frac{z^{-\alpha}}{\sum_{j=1}^Z j^{-\alpha}} \sum_{k=1}^K \sum_{n=1}^N C_{B_2}, \quad (20a)$$

$$\text{s.t.} \quad \sum_{k=1}^K \sum_{n=1}^N \|\mathbf{I}_n(\mathbf{E}_k \mathbf{X})\|_2^2 \leq P_f, \quad (20b)$$

$$\|\mathbf{A}_k \mathbf{X} + \mathbf{b}_k\|_2 \leq \mathbf{C}_k^T \mathbf{X}, \quad \forall k, \quad (20c)$$

$$\sum_{(k,z)} C_{(k,z),n} \leq Q_n, \quad \forall n, \quad (20d)$$

where $\mathbf{E}_k = [0_1^{NL \times NL}, 0_2^{NL \times NL}, \dots, 1_k^{NL \times NL}, \dots, 0_K^{NL \times NL}]$,

$$\begin{aligned}
\mathbf{H}_k &= [\mathbf{H}_{k,1}^H, \mathbf{H}_{k,2}^H, \dots, \mathbf{H}_{k,N}^H]^H \in \mathbb{C}^{NL \times 1}, \quad \mathbf{H}_{k,n} \in \mathbb{C}^{L \times 1}, \\
\mathbf{I}_n &= [0_1^{L \times L}, 0_2^{L \times L}, \dots, 0_n^{L \times L}, \dots, 0_N^{L \times L}], \\
\mathbf{C}_k^T &= \sqrt{\frac{1 + \gamma_k}{\gamma_k}} [0, \dots, \mathbf{H}_k^H, \dots, 0], \\
\mathbf{b}_k &= [0, 0, 0, \dots, \sigma_k]^H \in \mathbb{C}^{(M+1) \times 1}, \\
\mathbf{A}_k &= \begin{bmatrix} \mathbf{H}_k^H & 0 & 0 & \dots & 0 & 0 \\ 0 & \mathbf{H}_k^H & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & \mathbf{H}_k^H \\ 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}.
\end{aligned} \tag{21}$$

Based on the above series of transformations over the nonconvex SINR constraint, approximations, and other techniques, it is shown that the original problem can be equivalently transformed into a standard SOCP paradigm. We can finally use the mature optimization algorithm to efficiently solve this SOCP via the available software package solver.

3.2. Generalized Algorithm for the Nonorthogonal Unicast and Multicast Scenario. SINR constraints (15c) and (15d) are nonconvex. Firstly, we perform an expected value calculation over the nonconvex SINR constraints. For nonconvex unicast SINR constraint (15c), similar to the aforementioned processing techniques over (11c), we can transform (15c) into SOC constraints as follows:

$$\begin{aligned}
\mathbf{H}_k^H \mathbf{v}_k &\geq \lambda_k \sqrt{\sum_{i=1, i \neq k}^M |\mathbf{H}_k^H \mathbf{w}_i|^2 + \sum_{j=1, j \neq k}^K |\mathbf{H}_k^H \mathbf{v}_j|^2 + \sigma_k^2}, \\
\Im(\mathbf{H}_k^H \mathbf{v}_k) &= 0, \quad \forall \lambda_k.
\end{aligned} \tag{22}$$

Different from the unicast SINRs, for given γ_m in the multicast scenario, since there is more than one user sharing a multicast beamforming \mathbf{w}_m and the channel matrices $\{\mathbf{H}_k\}$ are linearly independent, only one of users' SINRs can be rewritten as a SOC constraint; let us assume that it is the K th user; we have

$$\begin{aligned}
\mathbf{H}_K^H \mathbf{w}_m &\geq \gamma_m \sqrt{\sum_{i=1, i \neq m}^M |\mathbf{H}_K^H \mathbf{w}_i|^2 + \sum_{j=1, j \neq K}^K |\mathbf{H}_K^H \mathbf{v}_j|^2 + \sigma_K^2}, \\
\Im(\mathbf{H}_K^H \mathbf{w}_m) &= 0, \quad K \in \Phi_m.
\end{aligned} \tag{23}$$

Others of the multicast SINR constraints are still nonconvex. By introducing the auxiliary variables and letting the

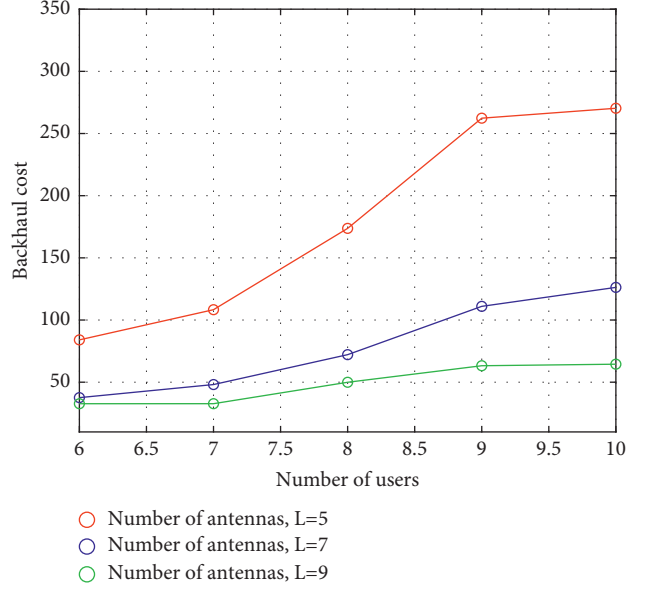


FIGURE 3: Backhaul cost against the number of users in the proposed SOCP algorithm.

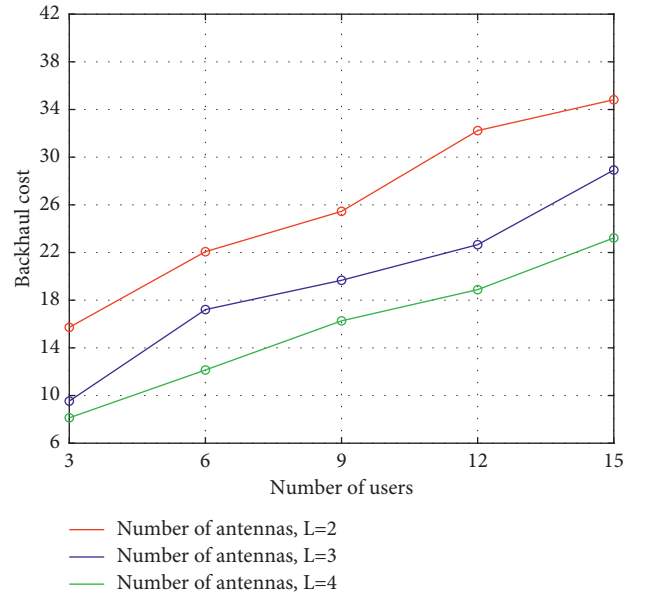


FIGURE 4: Backhaul cost against the number of users (the number of groups $M=2$) in the proposed SLA algorithm.

t th interaction point to be $\{g_{k,m}^t \in \mathbb{R}^2\}$, $\forall k \in \Phi_m / \{K\}$, the nonconvex multicast constraint can be transformed into

$$\begin{aligned}
&\|g_{k,m}^t\|^2 + 2(g_{k,m}^t)^T (g_{k,m} - g_{k,m}^t) \\
&\geq \gamma_m \sqrt{\sum_{i=1, i \neq m}^M |\mathbf{H}_k^H \mathbf{w}_i|^2 + \sum_{j=1}^K |\mathbf{H}_k^H \mathbf{v}_j|^2 + \sigma_k^2}.
\end{aligned} \tag{24}$$

Based on the above series of approximation transformations on nonconvex SINR constraints (15c) and (15d), by

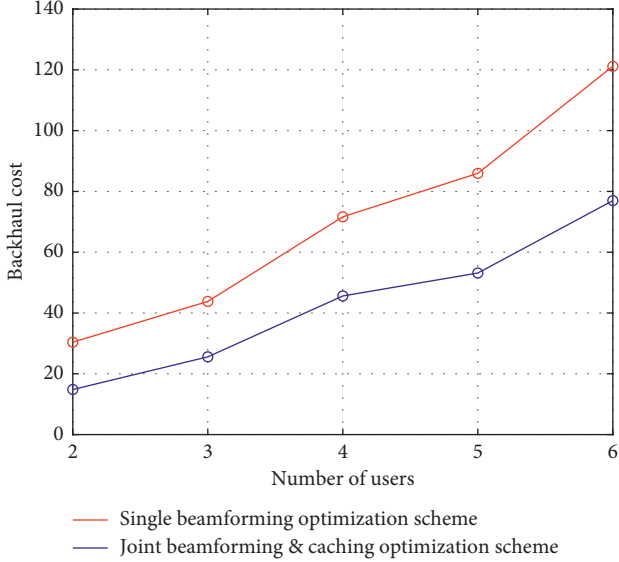


FIGURE 5: Performance comparison between the single beamforming scheme and joint beamforming-caching scheme for the SOCP algorithm.

substituting the formulas l_0 -norm and smooth logarithmic function into the objective function of P^{UM} , we can finally reduce P^{UM} to the following problem as follows:

$$P_{UM}: \quad \min_{\{v_{k,n}, w_{m,n}, C_{(k,z),n}, \hat{C}_{(m,z),n}\}} T_{B_1} + T_{B_2} \quad (24a)$$

$$s.t. (15b), (15e), (22), (23), \text{ and } (24). \quad (24b)$$

Using the SLA method, problem P_{UM} can finally be solved. The main step of the SLA method is to solve a series of convex subproblems as conducted in (24a) and (24b).

4. Simulation Results

4.1. Performance Comparison under Different Setups. Figure 3 demonstrates the backhaul cost against the number of users under different setups of BS antennas. It shows that the backhaul consumption increases with the number of users increasing. Moreover, the more the BS antennas in the network are, the less the backhaul cost the system consumes.

Figure 4 demonstrates the backhaul cost against the number of users under different numbers of BS antennas with three setups. As is shown, the more the antennas of the BS, the less the consumption of the backhaul link. Moreover, the backhaul consumption becomes higher with the number of users increasing. In addition, we can observe that the gap becomes smaller with the number of antennas increasing, which further illustrates the feasibility and effectiveness of the proposed framework.

Figures 3 and 4 separately demonstrate the backhaul cost against the number of users under different setups of BS antennas. Here, the backhaul consumption increases when the number of users increases. Moreover, when there are

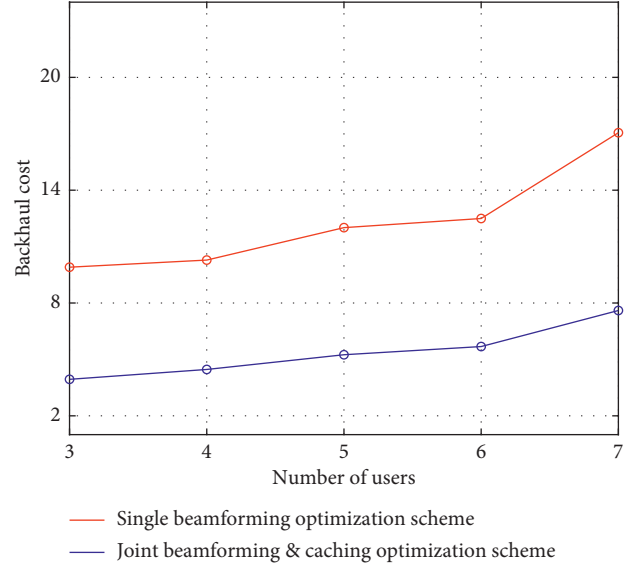


FIGURE 6: Performance comparison between the single beamforming scheme and joint beamforming-caching scheme for the SLA algorithm.

more BS antennas in the network, the system consumes a lower backhaul cost. The explanation for this phenomenon is that when the BS is equipped with more antennas, there is more antenna cooperative transmission. As a result, under the limited number of BSs and caching capacity, the transmission pressure on the backhaul link decreases, which reduces the backhaul consumption.

4.2. Performance Comparison between the Single Transmission Scheme and the Joint Beamforming-Caching Scheme. Figures 5 and 6 demonstrate the performance comparison between the single beamforming framework and the joint beamforming-caching framework for the SOCP algorithm in the unicast scenario and SLA algorithm in the joint unicast-multicast scenario, respectively. We observe that the joint beamforming-caching scheme performs better than the single beamforming scheme, which illustrates that the introduction of local caching can effectively reduce the backhaul consumption. Using the F-APs' caching function, part of the contents can be cached in advance, which shortens the actual distance between the user and content data and effectively alleviates the transmission pressure of the backhaul link.

5. Conclusion

In this article, we study a novel framework which is based on SCSI by incorporating beamforming and edge caching in a content-centric F-RAN architecture. A novel design on joint beamforming, edge caching, and dynamic F-AP clustering strategy with respect to SCSI is first explored. We formulate a mixed nonconvex problem aimed at minimizing backhaul consumption subject to the limited caching capacity, the BS power constraints, and SINR requirements. Accordingly, we provide a tailored second-order cone programming (SOCP)

algorithm for the unicast transmission scenario and a successive linear approximation (SLA) algorithm for the joint unicast and multicast transmission scenario. It is the first attempt about the joint design on beamforming and edge caching based on SCSi under the F-RAN architecture. Simulation results demonstrate the advantages of our framework based on SCSi compared with conventional schemes. In addition, it also makes sense to continue the study for the multicast scenario in the F-RAN architecture based on SCSi.

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.

References

- [1] H. Gao, X. Qin, R. J. D. Barroso, W. Hussain, Y. Xu, and Y. Yin, "Collaborative learning-based industrial IoT API recommendation for software-defined devices: the implicit knowledge discovery perspective," *IEEE Transactions on Emerging Topics in Computational Intelligence*, pp. 1–11, 2020.
- [2] D. You, T. V. Doan, R. Torre et al., "Fog computing as an enabler for immersive media: service scenarios and research opportunities," *IEEE Access*, vol. 7, no. 7, pp. 65797–65810, 2019.
- [3] A. Sengupta, R. Tandon, and O. Simeone, "Fog-aided wireless networks for content delivery: fundamental latency tradeoffs," *IEEE Transactions on Information Theory*, vol. 63, no. 10, pp. 6650–6678, 2017.
- [4] Y. Huang, H. Xu, H. Gao, X. Ma, and W. Hussain, "SSUR: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 670–681, 2021.
- [5] M. Peng, S. Yan, K. Zhang, and C. Wang, "Fog-computing-based radio access networks: issues and challenges," *IEEE Network*, vol. 30, no. 4, pp. 46–53, 2016.
- [6] M. Peng and K. Zhang, "Recent advances in fog radio access networks: performance analysis and radio resource allocation," *IEEE Access*, vol. 4, pp. 5003–5009, 2016.
- [7] J. Xiao, H. Xu, H. Gao, M. Bian, and Y. Li, "A weakly supervised semantic segmentation network by aggregating seed cues: the multi-object proposal generation perspective," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 17, no. 1s, pp. 1–19, 2021.
- [8] N. D. Sidiropoulos, T. N. Davidson, and Z. Q. Luo, "Transmit beamforming for physical-layer multicasting," *IEEE Transactions on Signal Processing*, vol. 54, no. 6, pp. 2239–2251, 2006.
- [9] R. Wang, M. Tao, and Y. Huang, "Linear precoding designs for amplify-and-forward multiuser two-way relay systems," *IEEE Transactions on Wireless Communications*, vol. 11, no. 12, pp. 4457–4469, 2012.
- [10] C. Lu and Y. F. Liu, "An efficient global algorithm for single-group multicast beamforming," *IEEE Transactions on Signal Processing*, vol. 65, no. 14, pp. 3761–3774, 2017.
- [11] M. Tao, E. Chen, H. Zhou, and W. Yu, "Content-centric sparse multicast beamforming for cache-enabled cloud RAN," *IEEE Transactions on Wireless Communications*, vol. 15, no. 9, pp. 6118–6131, 2016.
- [12] E. Chen, M. Tao, and Y. F. Liu, "Joint base station clustering and beamforming for non-orthogonal multicast and unicast transmission with backhaul constraints," *IEEE Transactions on Wireless Communications*, vol. 17, no. 9, pp. 6265–6279, 2018.
- [13] H. Gao, K. Xu, M. Cao, J. Xiao, Q. Xu, and Y. Yin, "The deep features and attention mechanism-based method to dish healthcare under social IoT systems: an empirical study with a hand-deep local-global net," *IEEE Transactions on Computational Social Systems*, pp. 1–12, 2021.