

Attacks, Challenges and New Designs in Security and Privacy for Smart Mobile Devices 2021

Lead Guest Editor: Ding Wang

Guest Editors: Kim-Kwang Raymond Choo, Weizhi Meng, and Marko Hölbl





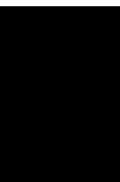
**Attacks, Challenges and New Designs in
Security and Privacy for Smart Mobile Devices
2021**

Wireless Communications and Mobile Computing

**Attacks, Challenges and New Designs in
Security and Privacy for Smart Mobile
Devices 2021**

Lead Guest Editor: Ding Wang

Guest Editors: Kim-Kwang Raymond Choo, Weizhi Meng, and Marko Hölbl





Copyright © 2022 Hindawi Limited. All rights reserved.

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

Chief Editor

































Zhipeng Cai , USA

Associate Editors

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

Academic Editors

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

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

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

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






Contents

Lightweight and High-Performance Data Protection for Edge Network Security

Xiaojie Chen , Bin Li , and Qinglei Zhou 


Research Article (24 pages), Article ID 8458314, Volume 2022 (2022)

Adaptive Weight Adjustment and Searching Perception Strategy for Multivariate Complex Environments

Wenshan Wang , Jianguo Sun , Sizhao Li , Junpeng Wu , and Qingan Da 

Research Article (12 pages), Article ID 6710661, Volume 2022 (2022)

A Hierarchical Provable Massive Data Migration Method under Multicloud Storage

Ma Haifeng, Yu HaiTao , Zhang Ji, Wang Junhua, Xue Qingshui, and Yang Jiahai






Research Article (12 pages), Article ID 7609543, Volume 2021 (2021)

Simultaneous Jamming-and-Transmitting Scheme for Spectrum-Sharing Relaying Networks with Nonlinear Energy Scavenging

Triet Pham-Minh , Khuong Ho-Van , and Khanh Nghi-Vinh 

Research Article (15 pages), Article ID 2368201, Volume 2021 (2021)

A Cross-Domain Authentication Optimization Scheme between Heterogeneous IoT Applications

Shichang Xuan , Haibo Xiao , Dapeng Man , Wei Wang , and Wu Yang 

Research Article (14 pages), Article ID 9942950, Volume 2021 (2021)

A Secure and Efficient Lightweight Vehicle Group Authentication Protocol in 5G Networks

Junfeng Miao , Zhaoshun Wang , Xue Miao , and Longyue Xing 





Research Article (12 pages), Article ID 4079092, Volume 2021 (2021)

Analyzing the Effectiveness of Touch Keystroke Dynamic Authentication for the Arabic Language

Suliman A. Alsubibany  and Afnan S. Almuqbil 




Research Article (15 pages), Article ID 9963129, Volume 2021 (2021)

Enabling Efficient Decentralized and Privacy Preserving Data Sharing in Mobile Cloud Computing

Jiawei Zhang , Ning Lu , Teng Li , and Jianfeng Ma 







Research Article (15 pages), Article ID 8513869, Volume 2021 (2021)

Multiagent Minimum Risk Path Intrusion Strategy with Computational Geometry

Jianguo Sun , Zining Yan , and Sizhao Li 

Research Article (18 pages), Article ID 9974279, Volume 2021 (2021)

Fast Policy Interpretation and Dynamic Conflict Resolution for Blockchain-Based IoT System

Yaozheng Fang , Zhaolong Jian , Zongming Jin , Xueshuo Xie , Ye Lu , and Tao Li 



Research Article (14 pages), Article ID 9968743, Volume 2021 (2021)

Privacy Threats of Acoustic Covert Communication among Smart Mobile Devices

Li Duan , Kejia Zhang , Bo Cheng, and Bingfei Ren 

Research Article (16 pages), Article ID 9179100, Volume 2021 (2021)

A Blind Signature-Aided Privacy-Preserving Power Request Scheme for Smart Grid

Weijian Zhang, Zhimin Guo, Nuannuan Li, Mingyan Li , Qing Fan, and Min Luo 

Research Article (10 pages), Article ID 9988170, Volume 2021 (2021)

A Survey on Adversarial Attack in the Age of Artificial Intelligence

Zixiao Kong, Jingfeng Xue, Yong Wang , Lu Huang, Zequn Niu, and Feng Li

Review Article (22 pages), Article ID 4907754, Volume 2021 (2021)

Research Article

Lightweight and High-Performance Data Protection for Edge Network Security

Xiaojie Chen ¹, Bin Li ², and Qinglei Zhou ²

¹State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China

²School of Computer and Artificial Intelligence, Zhengzhou University, Zhengzhou 450001, China

Correspondence should be addressed to Bin Li; cctvlibin@163.com

Received 18 June 2021; Revised 30 October 2021; Accepted 4 January 2022; Published 22 February 2022

Academic Editor: Ding Wang

Copyright © 2022 Xiaojie Chen et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

To strengthen the security of edge network data and reduce network latency, in this paper, we combine an advanced reduced instruction set computing machine (ARM) and a field programmable gate array (FPGA) to propose a lightweight ARM-FPGA computing architecture for edge network data security protection and acceleration. Firstly, the access control lists are set through FPGA to authorize and filter illegal data, thereby reducing the transmission and processing of invalid data on the network. Secondly, based on the principles of dynamization, diversification, and randomization, the initial random key is generated using a pseudo-random number generator and a scrambling factor, and the hash of the data packet value updates the key to ensure “one frame, one key.” Then, an ARM microprocessor is used to monitor the working status of the system in real-time. If an abnormality is found, different disturbance factors are activated using key management to change the system running status and restore the stability of the system. Finally, pipeline technology and critical path optimization on FPGA are used to parallelize the underlying encryption algorithm and data compression algorithm to achieve high-speed memory communication and meet the performance requirements of different networks. The experimental and analysis results show that the computing architecture designed in this paper has high network encryption performance and can effectively prevent data leakage. In addition, the effectiveness of the architecture in terms of network delay and network load is verified.

1. Introduction

The rapid popularization of 5th-generation mobile communication technology (5G) networks will lead to the connection of a large number of edge devices to the internet, such as mobile devices, autonomous vehicles, security monitoring devices, and smart homes. According to relevant statistics and forecasts, by 2025, the number of devices connected to the internet will reach 500 billion [1], which will lead to an explosion of data between edge nodes and cloud servers. Such large amounts of data bring large overhead for limited network resources, and the security risks and privacy protection issues of edge networks will also increase. The results of a survey conducted by the Internet Crime Complaint Center (IC3) show that network security issues have brought huge economic losses [2]. Cyberspace is currently facing a variety of attack methods, such as malware infection, injection attacks with camouflage, and distributed

denial of service (DOS) attacks, all of which make it difficult to take safety precautions on existing networks. Network security has become an issue of widespread concern among countries and academic institutions worldwide [3] and a topic of extensive research.

Traditional networks are static, similar, and deterministic in their composition, and it is easy for attackers to study their operating rules, identify security flaws, and conduct detection and continuous intrusions. Among the many types of attacks, network sniffing [4] is a major threat to network security. In a network sniffing attack, various key information transmitted on the access network is monitored and can be stolen or tampered with. In addition, there are a large number of security vulnerabilities in current network equipment and components. Attackers can use vulnerabilities in routing equipment to directly eavesdrop on user data in the core network [5]. In response to this problem, the American academic community has proposed a “game-

changing” moving target defense (MTD) [6] technology. By constantly and randomly changing deployment mechanisms and strategies, the difficulty of conducting an attack is increased, and the flexibility of the system is improved. Examples include internet protocol (IP) address changes [7–10], dynamic ports [11], dynamic 3-layer encryption schemes [12], full protocol stack randomization [13], security function virtualization [14], route randomization [15], and data virtualization [16]. In China, Wu proposed mimic security defense (MSD) [17], which dynamically and pseudo-randomly selects different equivalent execution entities under active and passive conditions to establish a variable execution environment and reduce the security risk of the system.

Among various network security defense measures, the hardware structure and operating system security are the foundation, and cryptography is the key technology. Network encryption technology can ensure the safe transmission of data and prevent network sniffing attacks. However, in traditional network encryption, the same key is used to encrypt all data packets during the key life cycle. If an attacker intercepts a large number of data packets encrypted with the same key, a ciphertext-only attack may be successfully implemented [18]. To combat ciphertext-only attacks, for some scenarios with high-security requirements, such as confidential systems and military departments, it is necessary to implement a dynamically variable key to encrypt each data packet, i.e., to use “one packet, one key” [19].

In the era of large-scale growth of edge network data, problems caused by data transmission, such as network delays, transmission efficiency, and network bandwidth congestion, will bring major challenges. Data compression technology can provide effective coding to reduce repetitive data under the premise of ensuring data reliability, thereby reducing the amount of network data. To meet the data transmission rate and real-time requirements of high-energy physics experiments under limited bandwidth, Truong et al. [20] developed a real-time lossless compression method based on incremental coding technology and implemented it efficiently on FPGA, which greatly improved the amount and speed of data processed in the experiment.

Edge networks and edge devices have high energy efficiency and high security requirements. Effective network security technologies mainly use the randomness and dynamics of the system to resist attacks, and they use encryption technology to protect data privacy. In this work, existing defense technology is combined with the computing characteristics of the edge network to propose a lightweight high-performance data protection scheme. The main contributions of our scheme can be summarized as follows:

- (1) A lightweight encryption system structure for edge networks is proposed, which makes full use of the uncertainty caused by the randomness, dynamics, and diversity of key transformations, making it difficult for attackers to establish a continuous and reliable attack chain.
- (2) Compression and encryption processing of edge network data are performed on FPGA. An ARM

microprocessor is used to control the initialization of the key, and the disturbance factor of the key is configured using state monitoring to form the heterogeneous lightweight data protection system structure of ARM-FPGA. FPGA is used to control the access of data frames, filter some attacks, and increase the attack threshold.

- (3) The ShangMi (SM) public key encryption algorithm SM2, the SM message digest algorithm SM3, and the SM symmetric encryption algorithm SM4 are optimized on FPGA to achieve high-performance data encryption processing. At the same time, FPGA realizes a multichannel parallel data compression algorithm using a serial-parallel structure, which reduces the amount of original data transmission and increases the network load.
- (4) Incorporating the idea of blockchain, the SM3 operation is performed on the sent data frame using a one-way and nontamperable modification of the Hash function to obtain the hash value, and a nonlinear operation is used to update the key to realize the “one frame, one encryption” method for network data and effectively resist network sniffing and ciphertext-only attacks.

2. Related Works

Data protection mechanisms have been studied extensively worldwide. In terms of physical structure defense, Wang et al. [21] elaborated on each type of attack by examining 11 typical vulnerable protocols and suggested corresponding countermeasures for wireless sensor networks (WSNs). Okhravi et al. proposed a real-time migration of key applications across heterogeneous platforms. The mimic defense web server proposed by Tong et al. [22] uses dynamic heterogeneous redundancy (DHR) to establish a software layer and a data layer. Multilayer mimic defense, such as in the operating system layer, can effectively resist a variety of intrusion detection methods and attacks. Pavithran et al. proposed a novel cryptosystem based on deoxyribonucleic acid (DNA) cryptography and finite automata theory [23]. The proposed scheme can protect the system against numerous security attacks, such as brute force attacks, known plaintext attacks, differential cryptanalysis attacks, cipher text-only attacks, man-in-the-middle attacks, and phishing attacks. Zhang et al. [24] proposed a lightweight encryption scheme for mobile ad hoc networks based on network coding to improve the security of network transmission.

With the development of edge computing and cloud computing, security technologies for edge networks and mobile networks have developed rapidly. Dar et al. [25] presented a context-aware encryption protocol suite that selects an optimal encryption algorithm according to device specifications and the level of data confidentiality. Qiu et al. [26] proposed a provably secure three-factor authentication and key agreement (AKA) protocol based on extended chaotic maps for mobile lightweight devices by adopting the techniques of “fuzzy verifiers” and “honeywords.” Wang

et al. [27] exploited the Rivest–Shamir–Adleman (RSA) cryptosystem’s computational imbalance at the encryption side and decryption side and made full use of the computation and storage capability of the cloud center to design a cloud-aided, efficient user authentication scheme with forward secrecy for Industry 4.0. Zhao et al. [28] designed a privacy-preserving data aggregation scheme for edge computing-supported vehicular ad hoc networks (VANETs) based on bilinear pairing and Paillier homomorphic encryption that not only preserves the privacy of uploaded data but also realizes batch operations.

FPGA enables energy-efficient computing and is widely used in edge network devices. Many security applications have also been implemented in FPGAs to allow security applications to run in real time [29], such as firewalls and data on high-speed network packet scanning. Soliman et al. [30] added a new dimension of security using frequency hopping to generate a pseudo-random pattern for switching between 5 lightweight cryptographic ciphers and an internal configuration access port controller, which decreased area utilization and power consumption by 58% and 80%, respectively. Pontarelli and others introduced a high-speed FPGA network intrusion detection system (NIDS) [31, 32]. NIDS checks the traffic flowing in the network to detect malicious content, such as spam and viruses.

Cryptographic algorithms are a core security technology and are of great significance in network security. Related algorithms proposed in China have received widespread attention and applications. The scalar multiplication calculation can be performed only once when co-signing. Zhang et al. [33] proposed an efficient and secure two-party distributed signature protocol based on the SM2 signature algorithm for key replay attacks. When a valid signature is generated, there is no need to rebuild the entire private key. Fan et al. [34] proposed a multiengine synchronous work method to carry out the SM4 algorithm in cipher block chaining (CBC) mode and achieve high-speed data encryption storage in solid-state hard disks. Verification on FPGA confirmed that this method can meet the requirements of high-speed communication interfaces. Yang et al. [35] implemented the high-performance encryption algorithms SM4-XTS and SM2 and large-integer modular exponentiation operations on FPGA to address the high concurrency and security issues of big data applications.

Data compression technology is an effective solution to reduce network delay and network load problems. Wang et al. [36] proposed a two-color image encryption algorithm based on two-dimensional compressed sensing and wavelets that can effectively reduce the amount of data, simplify the key, and improve the efficiency of data transmission and key distribution. Fouad et al. [37] proposed a hybrid data compression algorithm to process data and then added RSA-encrypted data to the compressed data using steganography, thereby improving data security and reducing the amount of data transmission and storage space required.

In summary, existing research on network security mechanisms has shown that the complexity of the system will increase with the complexity of the defense mechanism. Chinese encryption standards play a key role in existing

protection mechanisms. In addition, network load and storage problems are becoming increasingly prominent. Therefore, this article proposes a lightweight, high-performance edge network data processing solution for edge networks that combine mimic defense, cryptographic algorithms, and data compression to meet data privacy protection and increased network load requirements.

3. Edge Network Data Security Protection Scheme

3.1. Edge Network Data Protection Design. Edge computing is an important part of new network tasks and application scenarios. It includes any computing resource or network resource between the data source and the cloud data center [38], and the transmission between the edge device and the cloud is processed and important. The value of network data and the protection of edge network data are of great significance to the interests of countries and individuals. Edge network data face issues, such as data security, privacy protection, and computing energy efficiency. Therefore, this paper designs a lightweight, high-performance data protection structure for edge networks. As shown in Figure 1, the ARM-FPGA heterogeneous data processing structure comprises the input port A and output port B of network communication, ARM, and FPGA computing components for data processing, and high-speed storage double data rate (DDR) memory.

FPGA is the core algorithm layer and the core of the entire framework. It includes the SM2 public key encryption algorithm, SM3 message digest encryption algorithm, SM4 symmetric encryption algorithm, and key generation algorithm, which can meet different encryption applications. It also includes the Lempel-Ziv (LZ) algorithm implementation (LZ4) as a lossless data compression algorithm to reduce the amount of communication data. A and B are network interfaces. In practical applications, Gigabit and 10-Gigabit networks can be used according to the requirements. The ARM processor is mainly responsible for the control of the upper layer, including key management, key agreement, and state management. The separation of control and calculation in different processing units can reduce the degree of coupling at the system layer. DDR memory is a cache library for network data, and it is also a data exchange center between ARM and FPGA.

In the data processing mechanism implemented by ARM-FPGA, the data are mainly communicated, calculated, and stored in ARM, FPGA, and DDR hardware, and the data processing flow is shown in Figure 2.

The specific process steps of ARM-FPGA system data protection are as follows:

- (1) The data frame is received from network port A and transmitted to FPGA through the I/O interface. Then, FPGA decapsulates the data frame, divides the data into abnormal data, network protocol data, and data to be encrypted using the access control list (ACL), and it discards them. Forwarding and data encryption are performed from network port B.

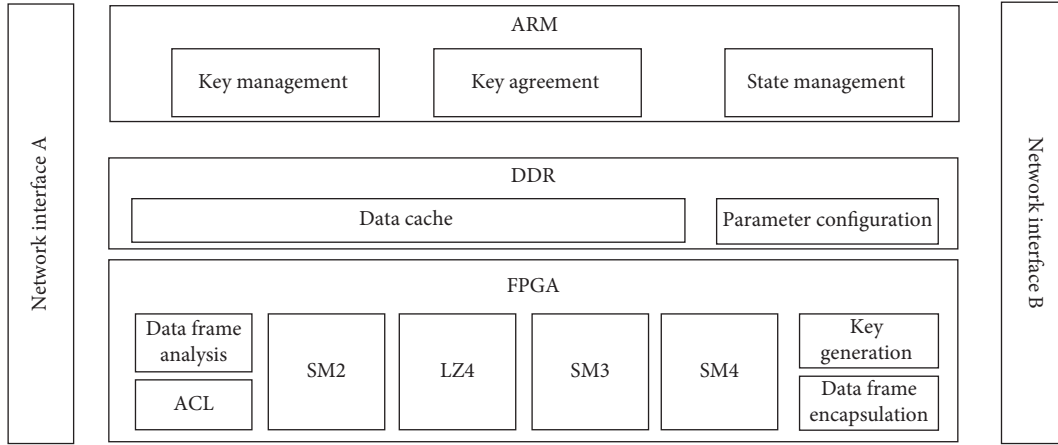


FIGURE 1: ARM-FPGA heterogeneous data processing structure.

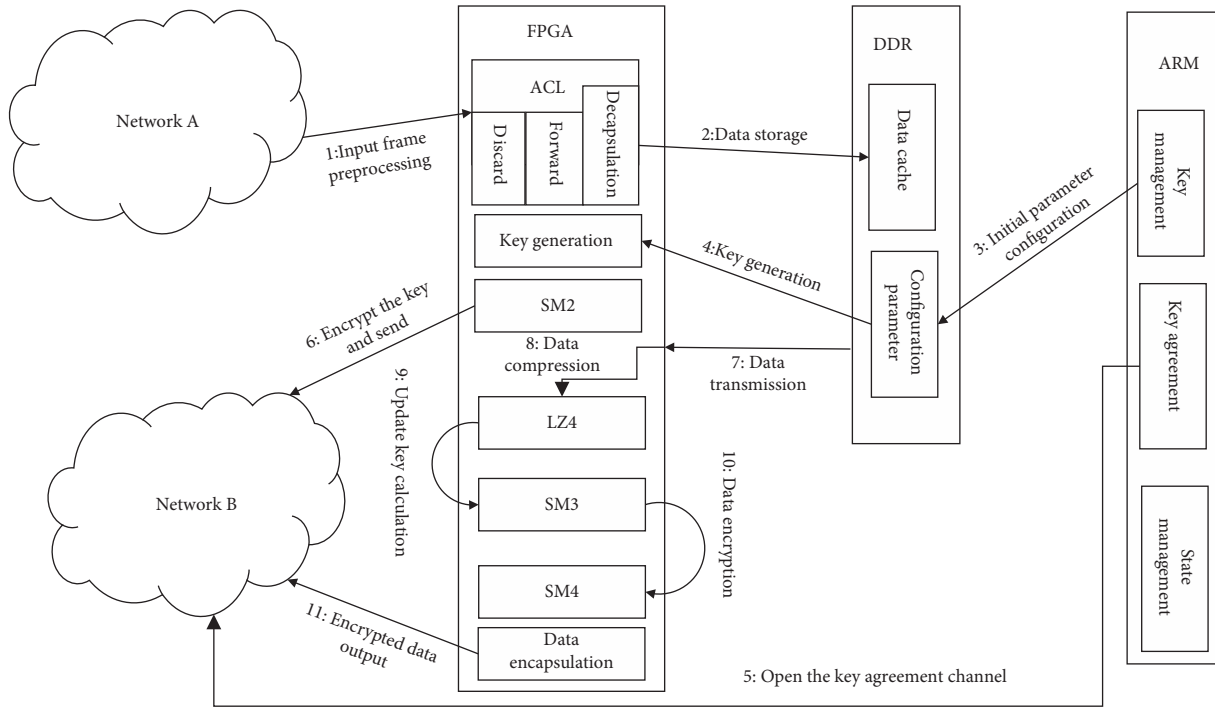


FIGURE 2: Data processing workflow.

- (2) The encrypted data to be processed are written into DDR according to the preset value address, and routing information, such as the IP address, port number, and protocol type is cached.
- (3) The ARM processor uses the key management control, starts the key generation module, and writes the initial configuration parameters into DDR.
- (4) FPGA obtains the configuration parameters from DDR, configures the key generation algorithm, and generates and stores the key. The key updates the initial key according to a random timestamp to ensure the noncontinuity of the key.
- (5) ARM opens a key agreement channel with the data-receiving peer using the upper-layer communication protocol.
- (6) FPGA calls the high-speed SM2 module for key encryption and sends the initial encryption key to the opposite end for data decryption.
- (7) FPGA and DDR establish a high-speed channel connection using the AXI bus protocol, and the data are transmitted to FPGA.
- (8) FPGA calls the LZ4 algorithm to compress the data and buffers the processed data according to the first input first output (FIFO) FIFO_1 and FIFO_2.
- (9) FPGA uses the SM3 algorithm to calculate FIFO_1 data using the empty and full signals, and the generated hash value and the initial key are calculated nonlinearly to obtain the key. The key of the current frame will also be used for the calculation in

the encryption key generation of the next frame to satisfy “one frame one key.”

- (10) The SM4 algorithm uses the data in FIFO_2 and the generated key to perform calculations to complete encryption.
- (11) In FPGA, the data are encapsulated into a network frame according to the routing information and sent out using network port B.

During the entire data processing operation, ARM will discover abnormalities at runtime using state management and detection and reconfigure the key to protect the security of the system. Data compression is added in data processing, and the data need to be decompressed when they are transmitted to the opposite end. Therefore, a 1-bit compression flag and 1-byte frame identification (FID) are added to the data frame format. If the compression flag is 0, the compressed encrypted data have not been received. If the compression flag is 1, the last frame of data is compressed. The length of the 32-bit identification compression is added to the last frame of data. The frame sequence guarantees the correctness of the data sequence during decompression, and the modified encrypted frame structure is shown in Figure 3.

3.2. Key Generation and Configuration. The key is instrumental to ensuring data security. It is the most direct “key” for opening the encrypted data and the first part that an attacker will attack. Therefore, generating a secure key is the first step in data protection.

Pseudo-random number generators [39] have a wide range of applications in the fields of spread spectrum communication, information encryption, and system testing. The most commonly used method of generating pseudo-random numbers is to use a feedback shift register, which consists of two parts: the shift register and the feedback function. When the feedback function is a linear function, the feedback shift register is a linear feedback shift register (LFSR), as shown in Figure 4.

Here, f_n is the feedback coefficient, 1 means the components are connected, and 0 means they are not connected. Clearly, the output sequence of LFSR is periodic, and an n -level LFSR provides at most $2^n - 1$ states (not including all 0 states). According to different feedback methods, the characteristic polynomial of LFSR can be defined.

$$p(x) = \sum_{i=0}^n f_i x^i = f_n + f_{n-1}x^{n-1} + \dots + f_1x + 1. \quad (1)$$

The scrambling factor can increase the scrambling effect and security of the algorithm. Cryptographic algorithms often use static parameters as the scrambling factor. To further increase the quality of the random number generated by LFSR, we perform the exclusive or (XOR) operation on the feedback value and the disturbance factor (DF), output the result, set the disturbance factors, including *FID*, *temperature*, and the random sequence (*RS*), and then, we perform the following operations:

$$\begin{aligned} randnum' &= FID \oplus randnum(a_1, a_2, a_3, \dots, a_n), \\ randnum' &= temperature \oplus randnum(a_1, a_2, a_3, \dots, a_n), \\ randnum' &= RS \oplus randnum(a_1, a_2, a_3, \dots, a_n), \end{aligned} \quad (2)$$

where $a_i (1 \leq i \leq n)$ represents LFSR status at the current moment. *FID* and *temperature* are real-time values that are used twice, which improves the utilization of data. *RS* is a random 8-row, 8-column, two-dimensional table generated by ARM, which is arranged in rows or columns and transmitted to FPGA using DDR memory. FPGA uses the lower 6 bits of *randnum* as the offset address to intercept the data and generate the scrambling factor. The *RS* example is shown in Figure 5.

This article defines 128-bit random numbers *randnum* and *randnum'*. There are 3 different LFSRs built into the random number generation scheme, which are randomly selected by FPGA, and the initial parameters are configured by ARM. The selection of the disturbance factor is dynamically configured by ARM according to the status information fed back by FPGA, which is divided into three following cases:

- (i) When the encryption system is running normally, because of the stability of FPGA, the range of power consumption changes caused by the hardware operation is small. In this case, ARM configures the disturbance factor as *FID*. The system runs stably, and *FID* can change normally in real time.
- (ii) When the encryption system is affected by external attacks or the environment, the temperature changes will be large. In this case, the configuration of the disturbance factor is *temperature*. It can stabilize the dynamics of the disturbance factor while simultaneously reducing the transmission of *FID*, changing the operating state of FPGA, and making the system operation stable again.
- (iii) ARM detects that FPGA is running abnormally, and the temperature fluctuation range is small. At this time, the disturbance factor is configured to *RS*, and FPGA needs to receive only the disturbance factor, which reduces the number of FPGA calculations. *RS* is dynamically and randomly generated by ARM, which can ensure the dynamic randomness of the key.

Through the dynamic random combination of 3 kinds of pseudo-random number generators and 3 kinds of scrambling factors, the randomness, dynamics, and security of the key can be guaranteed, and the functions of the three scrambling factors are complementary to each other, which is beneficial for the stability of the system.

3.3. High-Speed Memory Data Transmission and Management. Because of the high computational complexity of data compression, the processing performance is low. Therefore, the data to be processed needs to be temporarily stored in memory to prevent network data congestion and loss because of mismatched data transmission

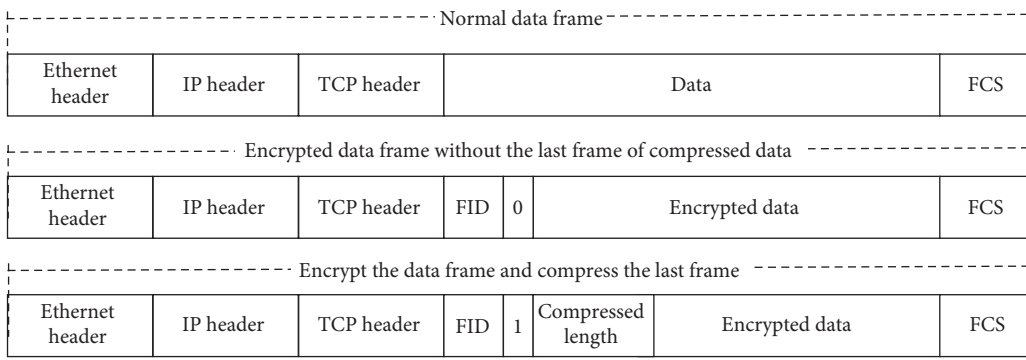


FIGURE 3: Data encryption frame format.

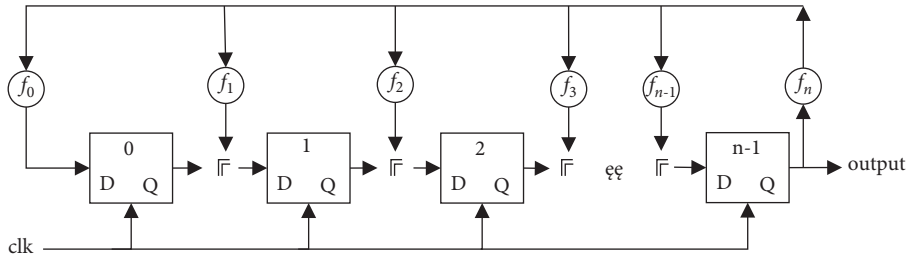


FIGURE 4: LFSR structure.

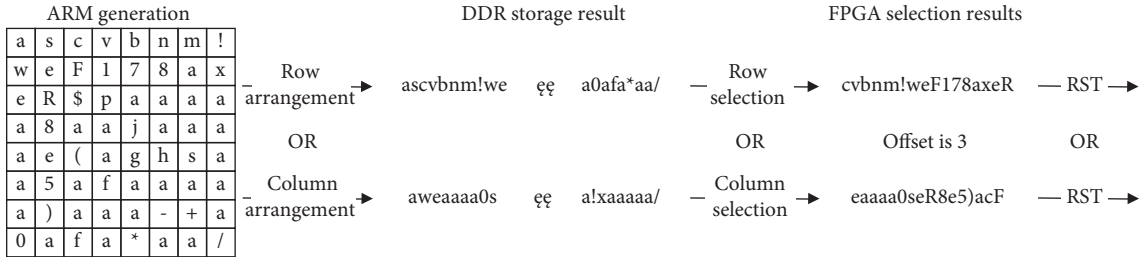


FIGURE 5: RS generation example.

and data processing in high-speed networks. In addition, data transmission between DDR and FPGA needs to meet high-performance requirements. Therefore, to achieve high-speed data exchange between FPGA and DDR, AXI4 (advanced extensible interface) protocol is adopted. The AXI4 protocol is the most important part of the advanced microcontroller bus architecture (AMBA) proposed by ARM and is mainly used in high-performance address mapping communication scenarios. The AXI4 communication protocol supports burst transmission, i.e., in data transmission, data can be obtained continuously. At a burst length of 16 and a data width of 256 bits, the amount of data transferred at one time is 512 bytes, i.e., one set of offset addresses corresponds to 16 sets of data, and FPGA and DDR are connected using memory interface generator (MIG) communication. Data transmission is carried out at the physical level. The memory communication design structure of the data to be compressed is shown in Figure 6.

The solid line in Figure 6 is the true transmission flow direction of data, and the dotted line points to the mapping position of the data in DDR. Data storage control and

reading control are connected to MIG's user-side memory interface using the AXI4 protocol. The control signals include the read address, read data, read feedback, write address, write data, write response, and write feedback. The memory controller is based on read and write requests, and it stores or reads data from the physical layer interface in order. In the memory communication design structure, the data transmission between the modules is carried out using a FIFO buffer so that the memory communication and data calculation are separated. The storage control module, the read control module, and the compression module are independent of each other and are calculated in parallel, thereby reducing the degree of data coupling and delay in data communication.

ARM is the FPGA controller. The key in FPGA needs to be configured, and FPGA can be customized in real time using the running status fed back by FPGA. The communication data between ARM and FPGA needs to be cached in DDR and controlled by the direct-memory-access (DMA) controller. The structure is shown in Figure 7.

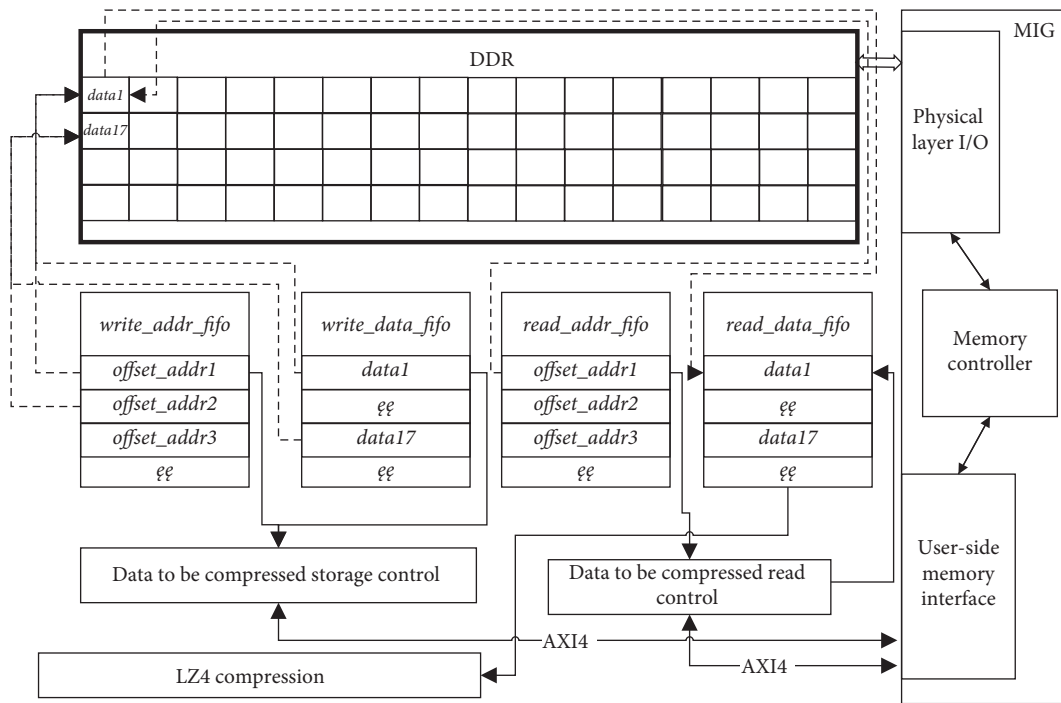


FIGURE 6: High-speed memory data communication structure.

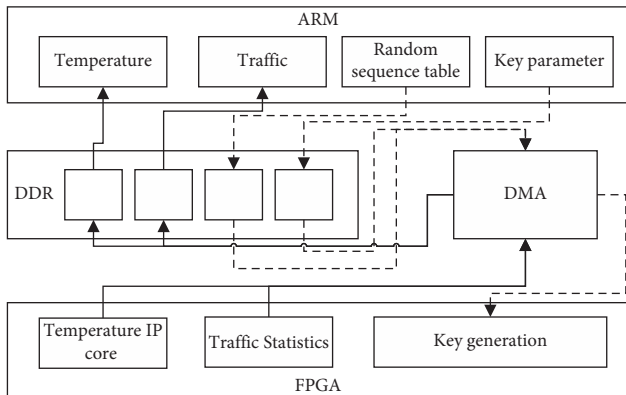


FIGURE 7: ARM and FPGA data communication structure.

The solid line in Figure 7 shows that FPGA transmits temperature and flow data to ARM using the temperature IP core and flow statistics module. The dotted line is the key configuration data of ARM to FPGA, and different addresses are allocated for different data in DDR. The read and write operations of different data in FPGA are calculated in parallel, and the arbitration transmission is carried out using DMA to ensure that the data can be transmitted to the correct address. ARM needs to start a DMA transmission channel to read and write data from DDR, and it operates on different data by polling tasks.

3.4. Fine-Grained Data Access Control. Access control allows legitimate users to access the operating data using authorization, and unauthorized users are prohibited from accessing the operating data illegally. An ACL is an

important access authorization strategy that filters illegal users using preset list attributes, thereby playing a role in data protection. The data transmission of edge network equipment uses clear and trusted network information, such as an IP address, port number, and transmission protocol. Therefore, this article presents an access control list, including data frame filtering attributes, such as the source media access control (MAC) address, destination MAC address, source IP address, destination IP address, source port number, and destination port number. When a data frame is transmitted to FPGA, the data frame is parsed and filtered according to frame information and preconfigured ACL. The implementation structure is shown in Figure 8.

The network data frame is transmitted to FPGA. Firstly, the data frame is decapsulated, and the frame information and frame data are buffered in the FIFO buffer. Then, the ACL module reads the data frame information and static access control attribute information to filter, authorize, and divide the data. There are three kinds of processing: (1) discard: discard the frame information, and read the corresponding data from the data FIFO buffer to discard them, (2) forwarding: buffer the frame information, read the data from the data FIFO buffer, and send them to the data frame encapsulation module to process and output them using the network sending port, and (3) encryption: buffer the frame information, read the data in the data FIFO buffer, cache them in the DDR using the high-speed interface, process the data according to the encryption mechanism, send the processed ciphertext and re-encapsulate, and send the frame information.

Using ACL for access control can directly filter illegal data and reduce data transmission. Legal data are processed in two ways, namely forwarding and encryption, which can

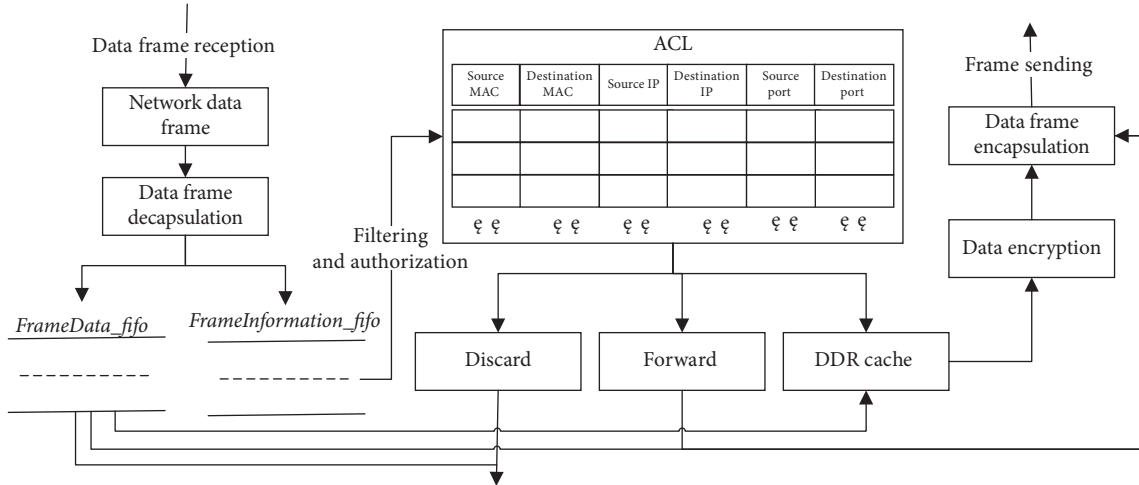


FIGURE 8: Data access control structure.

reduce the amount of calculation needed for data processing, thereby reducing the energy consumption of the device and simultaneously ensuring the privacy and security of important data.

4. High-Performance Core Algorithm Implementation

Encryption algorithms and compression algorithms consume the most computing resources and the longest computing time in the entire framework. FPGA is the main computing component. High-performance cryptographic algorithms and data compression algorithms are essential for improving edge network data protection and reducing network latency. Therefore, one of the key research objects of this article is the parallelization of cryptographic algorithms and data compression algorithms on FPGAs based on pipeline technology, storage optimization, prime domain computing optimization, collaborative computing, multi-channel parallelism, and other methods to obtain high-performance, low-energy algorithms.

4.1. SM4 Parallel Implementation. The SM4 cipher algorithm is a block encryption algorithm. The input data and key are 128 bits, and the encryption operation adopts 32 rounds of nonlinear iterative structure, which can be guaranteed in terms of security, as there is still no effective method of attacking it in a limited time [40]. The SM4 encryption algorithm includes two parts: key expansion and round function encryption. The specific algorithm flow is shown in Algorithm 1.

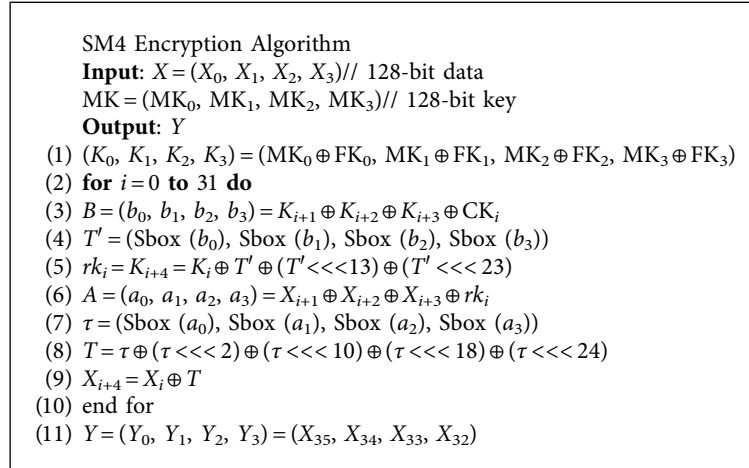
Step 1 of the encryption algorithm sets the initialization parameter, and the initial key is obtained using the system parameter. Steps 2 to 10 are 32 rounds of loop iterations, in which steps 3 to 5 and 6 to 9 generate each round of the subkey rk_i and data encryption using exclusive OR operations, S-box permutations, and linear transformations. These steps encrypt and scramble the data, thereby improving the resistance to attack. Finally, Step 11 obtains the final output

using the reverse-sequence operation. The operation and symbol descriptions for the algorithm are shown in Table 1.

The SM4 encryption algorithm has a small amount of calculation and low complexity in the initialization key and reverse-sequence output generation stages and requires only one calculation clock. Both subkey generation and data encryption require round function calculations, including XOR operations with four operands, four S-box lookups, linear transformations, and XOR operations, where the S-box lookups need 256 data points, i.e., obtaining an 8-bit input requires 256 corresponding 8-bit data points, and its complexity will affect the timing implemented on FPGA, which will make it difficult to improve the performance of the algorithm. Therefore, it is necessary to optimize the round function and S-box.

The round function is the key path of the SM4 algorithm. The main computing resources in FPGAs include look-up tables (LUTs), flip-flop (FF) registers, and random access memory (RAM). If the critical path is implemented in one clock, a combinational logic method is required, which will consume a large number of LUTs and calculations at the same time. The frequency will also drop, and the relationship between LUT and FF resources is 1:2. When implementing FPGAs, it is necessary to ensure the balanced utilization of resources and maximize the calculation frequency. We separate the critical path and use sequential logic to implement A and X_{i+4} , which consumes 2 clock cycles. Four S-box operations can be processed in one clock cycle in parallel. Because of the need to implement a variety of algorithms in this solution and the fact that the RAM resource occupancy is small, the S-box data are stored in RAM to reduce the use of LUTs. When operating, only the searched position needs to be input as an address, which can be completed in one clock. The round function calculation structure of the optimized conversion is shown in Figure 9.

The key to maximizing the performance of the SM4 algorithm is to improve the algorithm throughput and realize the SM4 algorithm for the full pipeline. The SM4 algorithm contains 32 rounds of iterative operations. The critical path of each round of operation is split into 3 clock



ALGORITHM 1: SM4 encryption algorithm.

TABLE 1: SM4 algorithm parameter description.

Operator	Description
\oplus	32-bit XOR
$\lll i$	32-bit circular shift left i -bit
FK_i	System parameters
CK_i	Fixed parameters
$\text{Sbox}()$	S-box replacement, 8-bit input, 8-bit output

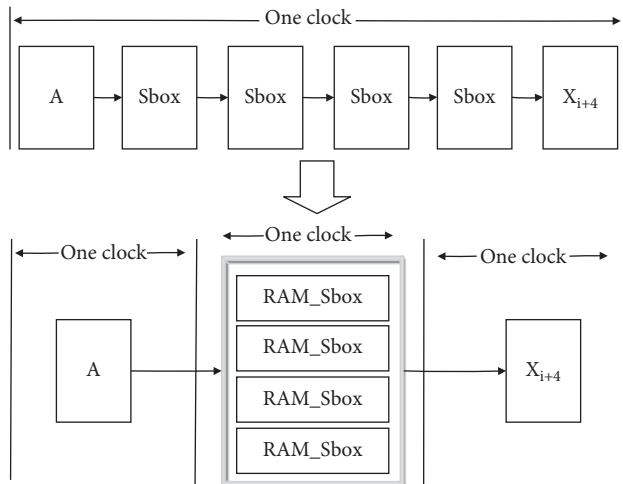


FIGURE 9: Round function optimization structure.

cycles, i.e., key generation and data encryption require 3 clocks, and a total of 6 clock cycles are required for one round of calculation. The transfer of data follows a similar process. Therefore, in a single round of key generation and data encryption, a three-stage pipeline is used to obtain 98-stage pipelines, including the two-stage operations of pre-processing and reverse-sequence output. The structure of SM4 algorithm is shown in Figure 10.

When calculating the data to be encrypted, the continuous data to be encrypted are first input into *Round0*, the first sub-key is calculated after three clock cycles, and the value of A_0 is calculated from the output. At the same time, the second group of data outputs the first sub-key using

parallel calculations. After two more clock cycles, key expansion and round encryption enter the parallel calculation state. After the 99th clock cycle, the first group of data is encrypted and output. The computing module occupied by the 96-stage pipeline runs at full load. The edge network needs to encrypt a large amount of data. The continuous data are input into the encrypted data stream. After 99 clock cycles, each clock has an output that can ensure the continuity of the ciphertext data and meet the network delay requirements, and throughput reaches its maximum.

4.2. SM3 Parallel Implementation. The hash algorithm has a wide range of applications in cryptography and data encryption and decryption [41–43]. SM3 is a hash algorithm proposed in China. It is suitable for digital signatures and verification in commercial cryptographic applications, message authentication code generation, verification, and randomization. The generation of numbers has the ability to resist currently known attacks more than the secure hash algorithm 256 (SHA-256) [44]. The SM3 algorithm inputs arbitrary-length data. After filling and iterative compression, it produces fixed-length 256-bit data.

Data padding adds input data m to data m' with a length of 512 bits according to the rule and divides the data into blocks of 16 words with a length of 32 bits: $W_0 \sim W_{15}$. The core of the algorithm is 64 rounds of iterative compression operations, and the compression function operation in each round is shown in Figure 11(a). The initial values of A through H in Figure 11 are the system vector V , and t represents the number of calculation rounds. After 64 rounds of calculation, the results $A_{63} \sim H_{63}$ and the initial vector V are XORed to obtain the final result. The SM3 algorithm parameter description is shown in Table 2.

FPGA is mainly composed of logic gates. Operations, such as AND, OR, NOT, and shifting have greater advantages, however, the delay of addition operations is relatively high. The longest path of the compression function in the SM3 algorithm is to calculate the values of A and E , which requires 5 addition operations. In the algorithm, SS1 is shared by A and E , and SS2 requires only one step of an

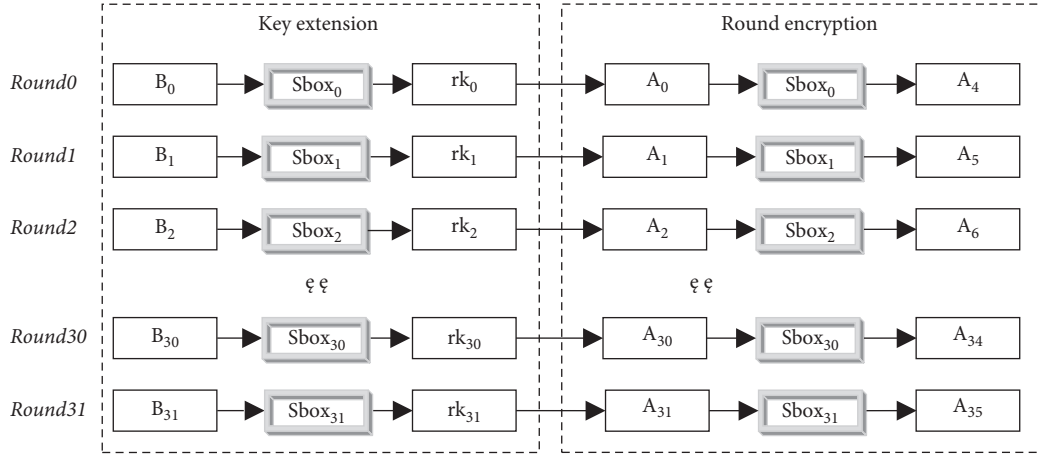


FIGURE 10: Structure of SM4 algorithm rounds.

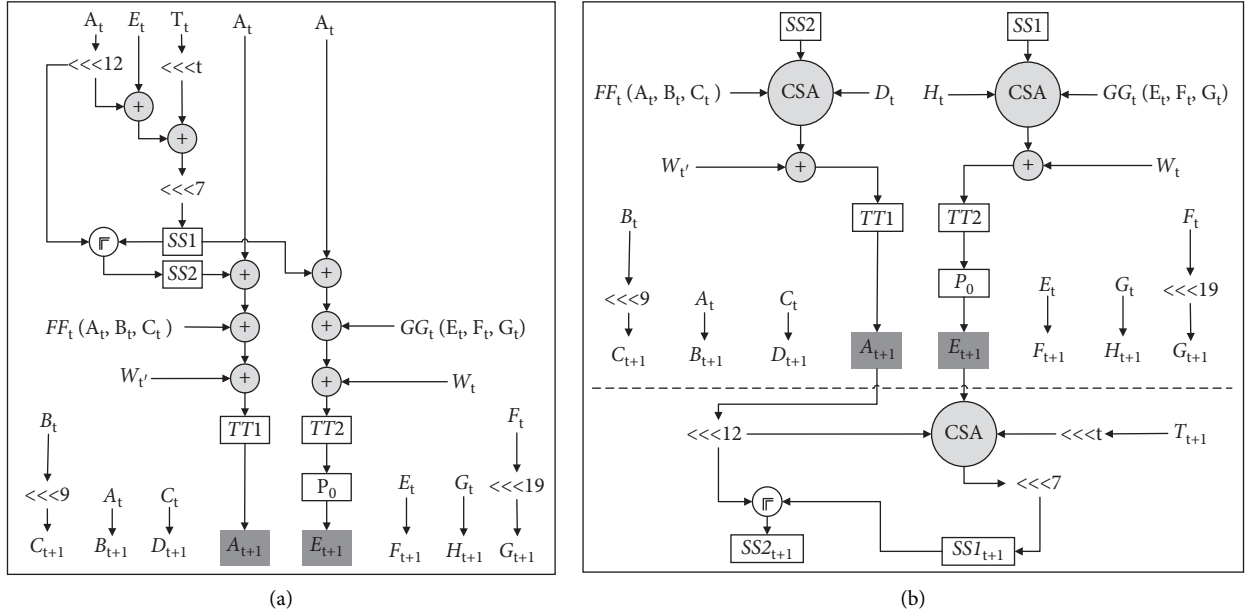


FIGURE 11: SM3 compression function structure. (a) Initial structure. (b) Optimized structure.

exclusive OR operation on SS1 and the value of the operation. There is no coupling with subsequent operations. Therefore, the critical path needs to be truncated. SS1 and SS2 are precalculated using a clock, and the critical path is reduced to 3 addition operations, which can reduce the algorithm delay.

Carry-save address (CSAs) can convert the addition of three operands into one addition operation and 8-bit operations using logical bit operations. The CSA operation is defined as $CSA(x, y, z) = (x \hat{\ } y \hat{\ } z) + (((x \& y) | (x \& z) | (y \& z)) \ll 1)$. There are multiple addition operations in the SM3 algorithm. Hence, CSAs can be used for conversion. The conversion calculation process is as follows:

$$\begin{aligned}
 (A_t \lll 12) + E_t + (T_t \lll t) &= CSA((A_t \lll 12), E_t, (T_t \lll t)), \\
 FF_t(A_t, B_t, C_t) + D_t + SS2 &= CSA(FF_t(A_t, B_t, C_t), D_t, SS2), \\
 GG_t(E_t, F_t, G_t) + H_t + SS1 &= CSA(GG_t(E_t, F_t, G_t), H_t, SS1).
 \end{aligned}
 \tag{3}$$

By precalculation and CSA conversion, the key path of the SM3 algorithm changes from 5 addition delays to 2 addition delays, and the calculation delay per unit time is greatly reduced.

Through precalculation, the critical path is split into two parts, and SS1 and SS2 need the values of A and E in the current round to participate in the calculation. If the single-round internal compression function is divided into a two-stage pipeline calculation, at least a 128-stage pipeline is required. A pipeline with more than 100 stages will have a greater timing impact on FPGA chips with a lower process level. Therefore, the calculation of SS1 and SS2 in round $t + 1$ is performed after the compression function of round t , and they are in the same clock. It can reduce the impact of timing without increasing the delay of the critical path. After precalculation and CSA optimization, the single-round processing structure is shown in Figure 11(b). The value of

TABLE 2: SM3 algorithm parameter description.

Operator	Description	Calculation
T_t	Constant	0x79cc4519 $0 \leq t \leq 15$ 0x7a879d8a $16 \leq t \leq 63$
$FF_t(X, Y, Z)$	Boolean function	$X \oplus Y \oplus Z$ $0 \leq t \leq 15$ $(X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z)$ $16 \leq t \leq 63$
$GG_t(X, Y, Z)$	Boolean function	$X \oplus Y \oplus Z$ $0 \leq t \leq 15$ $(X \wedge Y) \vee (\neg X \wedge Z)$ $16 \leq t \leq 63$
$P_0(X)$	Permutation function	$X \oplus (X \lll 9) \oplus (X \lll 17)$
$P_1(X)$	Permutation function	$X \oplus (X \lll 15) \oplus (X \lll 23)$
W_t	Extended word	$P_1(W_{t-16} \oplus W_{t-9} \oplus (W_{t-3} \lll 15)) \oplus (W_{t-13} \lll 7) \oplus W_{t-6}$ $16 \leq t \leq 67$
W'_t	Extended word	$W_t \oplus W_{t+4}$

W involved in the calculation includes the values generated by the different iteration rounds, and multiple W values need to be stored. There is only one-way data transmission with the compression function, which can be used as a separate first-stage pipeline. The SM3 compression function requires 64 iterations. Therefore, a 65-stage full pipeline is used for implementation.

4.3. High-Speed SM2 Algorithm Implementation. The SM2 algorithm is a public key encryption algorithm based on the elliptic curve discrete logarithm problem. In the prime domain, an elliptic curve $E(F_p)$ is described as [45] $y^2 = x^3 + ax + b \pmod{p}$. The security of an elliptic curve cryptosystem is mainly based on the difficulty of finding the inverse of the point multiplication. Point multiplication, also called a multiple-point operation, refers to the multiplication operation of a base point P on a curve with an integer k , i.e.,

$$kp(x) = \sum_1^k p = p + p + p + \dots + p. \quad (4)$$

The point multiplication process includes point doubling and point addition operations. Hence, the optimization of point addition, point doubling, and point multiplication is an important means of improving the efficiency of elliptic curve calculation.

The SM2 algorithm uses the reconfigurable features of FPGA, combined with Karatsuba-Ofman algorithm (KOA) multiplication, fast modular reduction, radix-4 modular inversion, Montgomery point multiplication, point addition, point doubling, and other optimization methods, to achieve high energy efficiency and resistance to attacks. By the bottom-up design method, the most basic operations at the bottom are realized with modular addition and subtraction, modular reduction, modular inversion, and modular multiplication. Then, the multiplication operation is optimized by point doubling and point addition, and finally, the SM2 encryption function is realized. The overall structure is shown in Figure 12.

When calculating the point multiplication, the point addition and point doubling operations are called multiple times, and the coordinate conversion is calculated only once at the end. Therefore, the point addition and point doubling operations are optimized for the best performance, and coordinate conversion is optimized for resource use. Secondly, the master control state machine performs scheduling

and management of the dot product module to meet the calculation requirements of different functions. Finally, coordinate conversion shares the modular addition and subtraction module to reuse resources to reduce the consumption of FPGA resources.

4.3.1. KOA Fast Multiplication. The core idea of the KOA [46] algorithm is to “divide and conquer.” It uses a recursive method to decompose a complex multiplication operation into multiple simple multiplication operations, which is faster and more efficient than traditional calculations. If two numbers of length n are directly multiplied, the complexity is $O(n^2)$. Using the KOA algorithm can reduce the complexity to $O(n^{\log_2 3})$.

For SM2, the parameter is 256 bits, and the FPGA digital signal processor (DSP) supports multiplication operations with a maximum width of 64 bits. Then, 256 bits can be divided into 128 bits, and 128 bits can be divided into 64 bits. After two recursive operations, the final result is obtained, as shown in Algorithm 2.

To further optimize the implementation of the KOA algorithm on FPGA, the 64-bit DSP multiplication clock cycle is set to 0, and the various modules are interconnected using wire type variables. When 256-bit data are input, the result can be calculated immediately and output by the register buffer. The whole calculation process takes 1 clock cycle.

4.3.2. Fast Modular Reduction. For fast modular reduction, several addition and subtraction operations can be used to obtain the modular reduction result. Compared with the currently universal Montgomery algorithm, fast modular reduction saves several 256-bit multiplication operations, and the performance can be significantly improved. If

$$p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1, \quad (5)$$

then for a large number A , we have the following:

$$A = A_{15} \times 2^{480} + A_{14} \times 2^{448} + \dots + A_1 \times 2^{32} + A_0. \quad (6)$$

Each A_i is a 32-bit integer. Then, A can be expressed as follows:

$$A = A_{15} \parallel A_{14} \parallel \dots \parallel A_1 \parallel A_0. \quad (7)$$

Then,

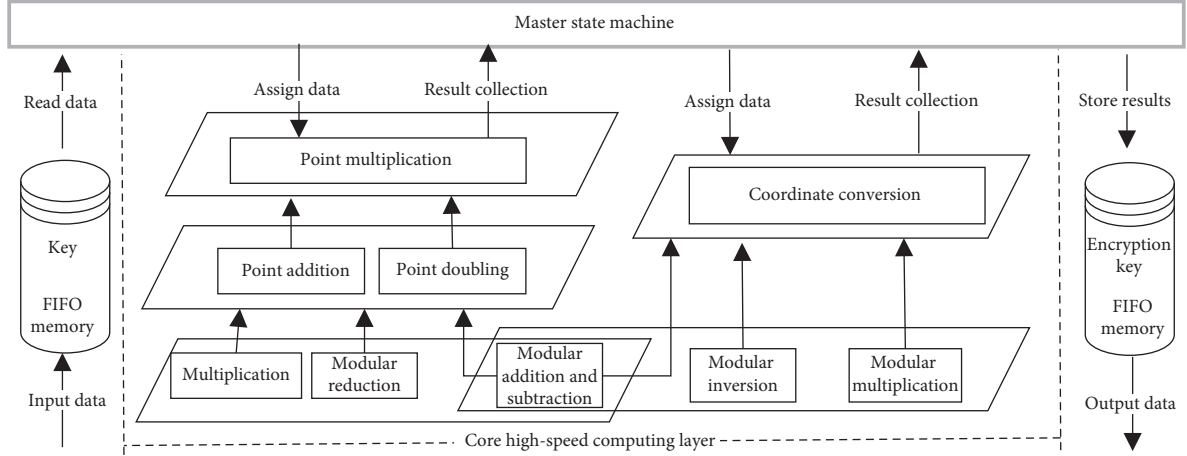


FIGURE 12: Overall architecture of the SM2 algorithm.

$$B = A \bmod p = (2S_0 + 2S_1 + 2S_2 + 2S_3 + 2S_4 + S_5 + S_6 + S_7 + S_8 + S_9 - D_1 - D_2 - D_3 - D_4) \bmod p, \quad (8)$$

where each 256-bit operand is represented as shown in Table 3.

4.3.3. Extended Euclidean Modular Inverse. The extended Euclidean algorithm uses the toss and turns division method to obtain the modular inverse. According to the nature of the common divisor, all divisions can be changed to addition and subtraction operations, and the division-by-2 operation is completed by binary shift, which is conducive to hardware implementation. Here, the algorithm is expressed in a

quaternary system using state machine cycle control to optimize the extended Euclidean algorithm, and the value of $b/a \bmod p$ can be obtained directly. The specific process is shown in Algorithm 3.

In Algorithm 3, the first line is the initialization state. The second line is the loop judgment state. Lines 3–27 are for various judgments and calculations. The last line is the output. Secondly, the calculation of u and v always ensures that the result value is less than p , and no additional processing is required. The addition and subtraction of x_1 and x_2 may be greater than p or may overflow, and division by 2 and division by 4 require additional judgment and calls of modulo addition and subtraction for processing. The specific calculation formula is as follows:

$$\frac{x}{2} \bmod p = \begin{cases} x \gg 1, & \text{if } x[0] == 1'b0, \\ x \gg 1 + p \gg 1 + 1, & \text{if } x[0] == 1'b1, \end{cases}$$

$$\frac{x}{2} \bmod p = \begin{cases} x \gg 2, & \text{if } x[1:0] == 2'b00, \\ (x \gg 1 + p \gg 1 + 1) \gg 1, & \text{if } x[1:0] == 2'b01, \\ x \gg 2 + p \gg 1 + 1, & \text{if } x[1:0] == 2'b10, \\ (x \gg 1 + p \gg 1 + 1) \gg 1 + p \gg 1 + 1, & \text{if } x[1:0] == 2'b11. \end{cases} \quad (9)$$

4.3.4. Point Multiplication Optimization. At present, the Montgomery point multiplication algorithm is the most efficient and widely used algorithm [47, 48]. The specific operation process is shown in Algorithm 4.

As shown in Algorithm 4, regardless of the value of k , the point addition and point doubling operations will be calculated during each cycle, and the two are independent of each other and can be executed in parallel. At the same time, because of the simultaneous calculation of point addition

and point doubling, the power consumption information leaked during the point multiplication operation is unruly, which can effectively resist a simple power consumption attack (SPA).

To improve the calculation efficiency of point addition and point doubling, Montgomery point multiplication needs only the x coordinate to participate in the calculation and calculate the y coordinate in the last step, which greatly simplifies the calculation process.

KOA multiplication
Input: A, B, n
Output: C

- (1) **if** ($n == 64$) **return** $C = A \times B$;
- (2) $A = A^H \times 2^{n/2} + A^L$
- (3) $B = B^H \times 2^{n/2} + B^L$
- (4) $C_1 = \text{KOA}(A^H, B^H, n/2)$
- (5) $C_2 = \text{KOA}(A^L, B^L, n/2)$
- (6) $C_3 = \text{KOA}(A^H + A^L, B^H + B^L, n/2)$
- (7) $C = C_1 \ll n + (C_3 - C_2 - C_1) \ll (n/2) + C_2$

ALGORITHM 2: KOA multiplication.

TABLE 3: Fast modulus reduction of various parameters.

	255–224	223–192	191–160	159–128	127–96	95–64	63–32	31–0
S_0	A_{15}	0	A_{15}	A_{14}	A_{13}	0	A_{15}	A_{14}
S_1	A_{14}	0	0	0	0	0	A_{14}	A_{13}
S_2	A_{13}	0	0	0	0	0	0	A_{15}
S_3	A_{12}	0	0	0	0	0	0	0
S_4	A_{15}	A_{15}	A_{14}	A_{13}	A_{12}	0	A_{11}	A_{10}
S_5	A_{11}	A_{14}	A_{13}	A_{12}	A_{11}	0	A_{10}	A_9
S_6	A_{10}	A_{11}	A_{10}	A_9	A_8	0	A_{13}	A_{12}
S_7	A_9	0	0	A_{15}	A_{14}	0	A_9	A_8
S_8	A_8	0	0	0	A_{15}	0	A_{12}	A_{11}
S_9	A_7	A_6	A_5	A_4	A_3	A_2	A_1	A_0
D_1	0	0	0	0	0	A_8	0	0
D_2	0	0	0	0	0	A_9	0	0
D_3	0	0	0	0	0	A_{15}	0	0
D_4	0	0	0	0	0	A_{14}	0	0

In the standard projective coordinate system, for points $P(X_1, Y_1, Z_1)$ and $Q(X_2, Y_2, Z_2)$, the calculation formulas for point addition and point doubling are as follows:

$$\begin{cases}
 X(P+Q) = (X_1X_2 - aZ_1Z_2)^2 - 4bZ_1Z_2(X_1Z_2 + X_2Z_1), \\
 Z(P+Q) = x_G(X_1Z_2 - X_2Z_1)^2, \\
 X(2P) = (X_1^2 - aZ_1^2)^2 - 8bX_1Z_1^3, \\
 Z(2P) = 4Z_1(X_1^3 + aX_1Z_1^2 + bZ_1^3)(X_1Z_2 - X_2Z_1)^2.
 \end{cases} \quad (10)$$

Upon converting the result to affine coordinates, we have the following:

$$\begin{cases}
 x_1 = \frac{X_1}{Z_1}, \\
 x_2 = \frac{X_2}{Z_2}, \\
 y_1 = \frac{2b + (a + x_Gx_1)(x_G + x_1) - x_2(x_G - x_1)^2}{2y_G}.
 \end{cases} \quad (11)$$

Then, the point (x_1, y_1) is the result. Here, (x_G, y_G) are the coordinates of the base point G .

Under standard projection coordinates, the projection point and the affine point will be mapped one by one. At the beginning of the operation, the affine coordinates will be transformed to projection coordinates, and they will be

mapped back to affine coordinates at the end of the operation. Therefore, in the entire calculation process, only one modular inverse operation is used at the end, and there is no modular inversion in the intermediate iteration process.

Finally, to further optimize the calculation efficiency of point addition and point doubling, the data flow is deeply optimized so that the calculation can be completed in the shortest time. Since fast modular multiplication consists of two modules, namely KOA multiplication and fast modular reduction, and both can calculate the result within one clock cycle, part of the calculation process of adjusting point addition and point doubling alternately calls KOA multiplication and fast modular reduction modules, taking full advantage of computational efficiency. After optimization, the calculation of point addition and point doubling can be completed in 12 clock cycles, indicating very high efficiency.

4.4. Parallel LZ4 Algorithm Implementation. One of the fastest compression algorithms is the LZ4 algorithm proposed by Yann Collet in 2012 [49], which is appropriate for data compression applications of lightweight hardware devices. The LZ4 algorithm inputs 1 byte of data *char* each time. After data compression and LZ4 encoding processing, the compression stage is subdivided into four parts: dictionary matching, optimal matching filtering, discarding of matching data, and data separation. The flow of the LZ4 algorithm is shown in Figure 13.

```

Extended Euclidean modular inverse
Input:  $a, b, p$ 
Output:  $c = b/a \pmod p$ 
(1)  $u = a; v = p; x_1 = b; x_2 = 0$ 
(2) while ( $v > 0$ )
(3) if ( $(u[1:0] == 2'b00)$ )
(4)  $u = u \gg 2, x_1 = x_1/4 \pmod p$ 
(5) else if ( $(v[1:0] == 2'b00)$ )
(6)  $v = v \gg 2, x_2 = x_2/4 \pmod p$ 
(7) else if ( $(u[1:0] == v[1:0])$ )
(8) if ( $(u > v) \ u = (u - v) \ \&Gt; 2$ )
(9)  $x_1 = (x_1 - x_2)/4 \pmod p$ 
(10) else  $v = (v - u) \ \&Gt; 2$ 
(11)  $x_2 = (x_2 - x_1)/4 \pmod p$ 
(12) else if ( $(u[1:0] == 2'b10)$ )
(13) if ( $((u \gg 1) > v) \ u = ((u \ \&Gt; 1) - v) \ \&Gt; 1$ )
(14)  $x_1 = (x_1/2 - x_2)/2 \pmod p$ 
(15) else  $u = u \gg 1, x_1 = x_1/2 \pmod p$ 
(16)  $v = (v - (u \gg 1)) \ \&Gt; 1$ 
(17)  $x_2 = (x_2 - x_1/2)/2 \pmod p$ 
(18) else if ( $(v[1:0] == 2'b10)$ )
(19) if ( $(u > (v \gg 1)) \ u = (u - (v \ \&Gt; 1)) \ \&Gt; 1$ )
(20)  $x_1 = (x_1 - x_2/2)/2 \pmod p$ 
(21)  $v = v \gg 1, x_2 = x_2/2 \pmod p$ 
(22) else  $v = ((v \gg 1) - u) \ \&Gt; 1$ 
(23)  $x_2 = (x_2/2 - x_1)/2 \pmod p$ 
(24) else if ( $(u \geq v)$ )
(25)  $u = (u - v) \ \&Gt; 1, x_1 = (x_1 - x_2)/2 \pmod p$ 
(26) else
(27)  $v = (v - u) \ \&Gt; 1, x_2 = (x_2 - x_1)/2 \pmod p$ 
(28) end while
(29) return  $c = x_1$ 

```

ALGORITHM 3: Extended Euclidean modular inverse.

```

Montgomery point multiplication
Input:  $k = (k_{l-1}, \dots, k_0)$ , point  $G$ 
Output:  $Q = kG$ 
(1)  $R_0 = G, R_1 = 2G, i = l - 2$ 
(2) while ()
(3) if ( $(k_i == 0)$ )
(4)  $R_1 = R_0 + R_1, R_0 = 2R_0$ 
(5) else if ( $(k_i == 1)$ )
(6)  $R_0 = R_0 + R_1, R_1 = 2R_1$ 
(7)  $i = i - 1$ 
(8) end while
(9)  $Q = R_0$ 

```

ALGORITHM 4: Montgomery point multiplication.

In the data compression stage, dictionary matching stores the input *char* in the matching *window*, calculates the *hash* value according to the formula, reads the data from the hash index of the matching dictionary for short matching, and obtains the matching *length* and *offset*. The lengths are

1 byte and 2 bytes, respectively, and the matching window data are updated to the matching dictionary at the same time. This process is the data expansion stage. The data length changes from 1 byte to 4 bytes, and the *hash* calculation is as follows:

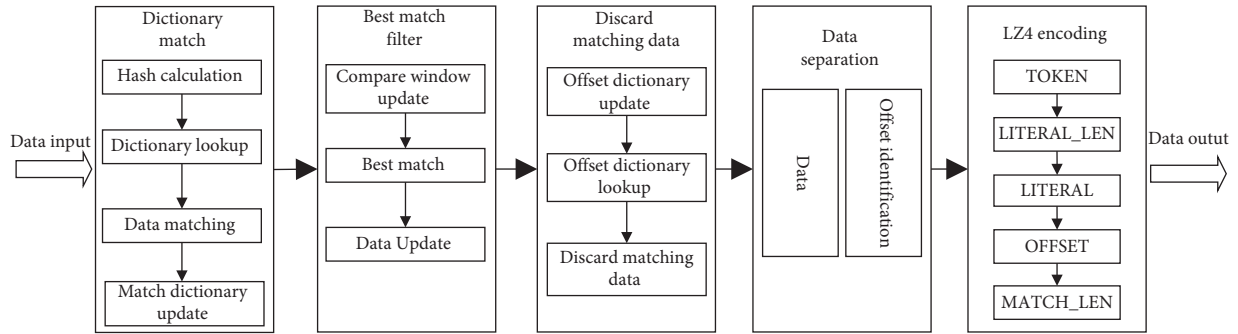


FIGURE 13: LZ4 algorithm processing structure.

$$hash = (window[0] \ll 4) \wedge (window[1] \ll 3) \wedge (window[2] \ll 3) \wedge window[3]. \quad (12)$$

Optimal matching filtering processes the current data and neighboring data according to the optimal matching strategy and outputs them if they meet the conditions. Otherwise, it resets *length* and *offset* to 0, reducing the subsequent long matching operations. In the process of discarding matching data, firstly, the input data are stored in the offset dictionary. Then, the offset dictionary is matched according to the matching length. A maximum of 255 data points can be matched, and the matched data will be jumped to perform matching and discarding. Data separation divides the data into plaintext data *char* and offset identification according to the matching length. Offset identification includes the matching length, the matching offset, and the amount of plaintext data, which is also the basis for decompression.

The LZ4 encoding format jumps between the five states of token, literal length, literals, offset, and match length according to the offset identifier, and it outputs the final LZ4 data. The encoding structure is shown in Figure 14.

The LZ4 algorithm is a streaming algorithm that is used for storage-intensive, matching-intensive, and communication-intensive tasks. It needs to meet the requirements of calculation, storage, and communication at the same time. The data are transmitted in one direction in the data compression stage. Therefore, the algorithm is implemented in a pipelined computing mode. Data compression is divided into 11 subtasks. The same clock frequency is used in FPGA implementation. Under the *clk* trigger, 11 subtasks are calculated in parallel, and the data are transferred in sequence to form an 11-stage pipeline. The FPGA implementation of the LZ4 algorithm structure is shown below in Figure 15.

In the LZ4 encoding stage, the repeated data are removed, and this operation requires only a serial state machine. Even in the worst case, there is no data compression, however, only a few states are added for jumping, and the most time is still spent in the LITERAL state. One clock cycle processes one input. Therefore, the LZ4 algorithm uses an 11-stage pipeline to implement parallel calculations and uses serial calculations for encoding. The pipeline arithmetic module and the encoding module use FIFO to store

communication data, preventing overflow and discarding the data generated by parallel calculations, which would result in incomplete data.

Multimodule parallelism is the simultaneous calculation of the same module in the same clock cycle using the control logic, and the performance can be doubled according to the number of parallel modules. Although the calculation logic of the LZ4 algorithm is complex, it occupies fewer resources. Therefore, according to the chip resources of FPGA, the data are distributed and recovered using the control of the state machine to realize multipath parallelism. The structure is shown in Figure 16.

The compressed data are transferred from the memory to the *data_fifo* inside the FPGA by the AXI bus protocol. The data are 256 bits wide, and the compressed data are 8 bits wide. Therefore, the data conversion module is added, the data are converted and stored in the FIFO buffer again, and the returned data still needs to be converted.

5. Experimental Results and Analysis

5.1. Experimental Environment. The main hardware computing component used in the scheme is the Zynq-XC7Z035 chip, which integrates a dual-core ARM A9 and a 275 K programmable logic unit and has hardware programming and software programming capabilities. The memory used is Micron's DDR3, with 1 GB of storage. There are Gigabit Ethernet ports on the ARM side and 10-Gigabit Ethernet ports and Gigabit Ethernet ports on the FPGA side. Flash is also included in the entire system. Writing *Bitstream* into Flash can complete the automatic loading and reconstruction of FPGA and provide detailed information about the main component configuration, as shown in Table 4.

The software environment for development is Vivado v2019.2, which is the supporting software of Xilinx and is used to perform the complete code writing, code simulation, compilation, placement and routing, downloading of bit-stream files, and other operations.

The data protection scheme in this article is mainly for edge network equipment. Network video surveillance equipment plays an important role in public security, smart homes, smart cities, and other fields. The protection of data

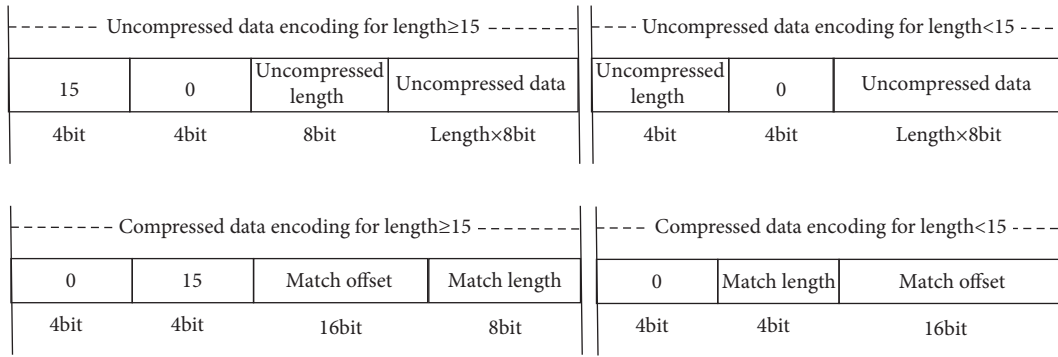


FIGURE 14: LZ4 coding structure.

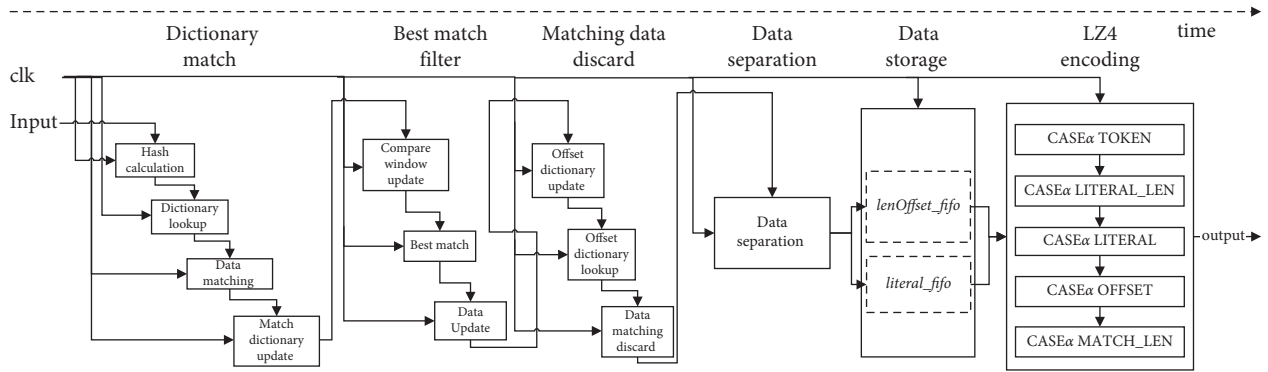


FIGURE 15: LZ4 algorithm FPGA implementation structure.

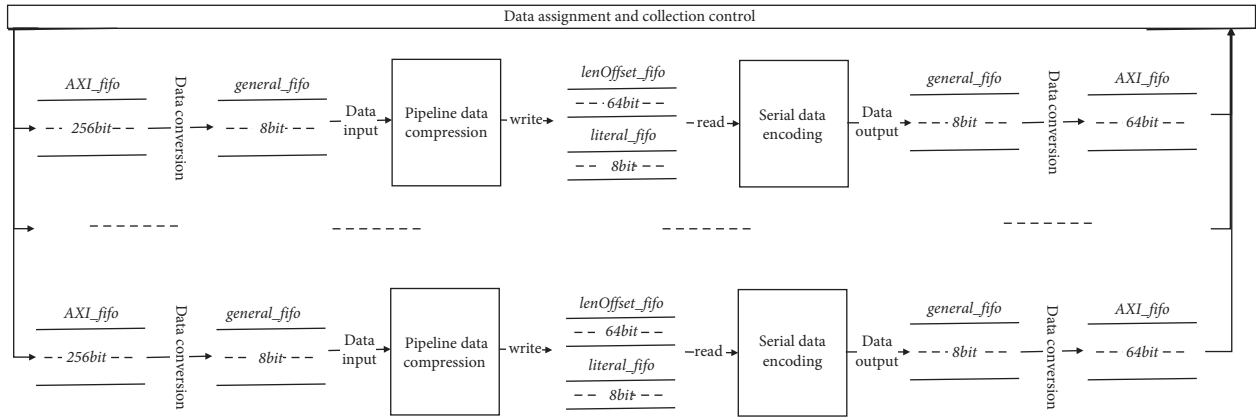


FIGURE 16: LZ4 multichannel parallel structure.

privacy is of great significance to safeguard people’s lives and property. Therefore, we take video surveillance as an example to build a simulated test environment, and the real test example structure is shown in Figure 17.

The network monitoring device in Figure 17 has assigned IP addresses, which are 172.26.11.6 and 172.26.11.4, respectively. When the test is not performed, the terminal device can log in remotely to view the monitoring information. During the overall program performance test, the connection is made for the network monitor, router, Zynq, and terminal to initialize the protection program, including the initialization of the key and the initialization of the access control module. The

protection equipment receives and processes the monitored real-time data from the network to verify whether the proposed solution meets the high-speed network data transmission requirements. In terms of security testing, simulated attackers are inserted into the front and back ends of the protection equipment, and real-time video surveillance information is obtained using network stealing methods. Based on the information obtained by the attackers, the security of the protection scheme is verified.

In this paper, the encryption algorithms SM3 and SM4 are deeply optimized. To verify the real performance, in the actual test, only the FPGA in Figure 17 needs to be statically reconstructed. The encryption algorithm is run on FPGA,

TABLE 4: Main component configuration information.

Component	Name	Configuration information
ARM	Model	Cortex-A9
	Architecture	ARMv7
	Frequency	800 M
FPGA	Logic cells	270 K
	Look up table (LUT)	171,900
	DSP slices	900
	Flip-flops	343,800
	GTP Transceiver	8 pairs of GTX, 10.315 Gbps, support PCIE Gen2
DDR	Memory size	1 G
	Main frequency	1600 MHz
	Maximum bandwidth	50 Gbps
Flash	Storage size	256 Mbit
	Maximum frequency	104 M

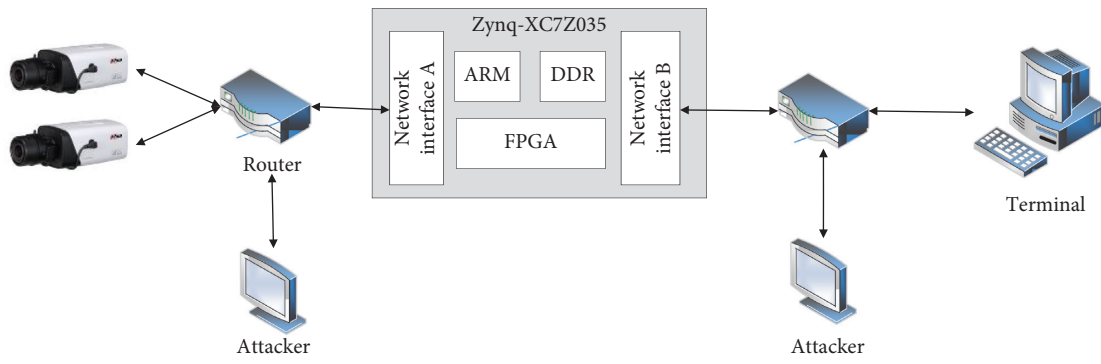


FIGURE 17: Real test environment structure.

and SM3 and SM4 are tested. The content is the real-time data of the monitoring equipment.

Encrypted data have no effect on the performance of the encryption algorithm, and the LZ4 compression algorithm is different. Therefore, in the actual test, not only the video content but also different content tests, including the text, data tables, pictures, and network mixed data packets, need to be tested. Thus, during FPGA testing, we transmit different data to Zynq through the network and perform multiple real tests on different content.

5.2. Experimental Results and Performance Analysis

5.2.1. Encryption Algorithm Implementation. The algorithm performance is based on throughput, and the calculation formula is as follows:

$$T = \frac{B \times f_{\max} \times N}{d}, \quad (13)$$

where T is the throughput, B is the data block size, f_{\max} is the maximum clock frequency of each scheme, N is the number of pipeline stages, and d is the calculation delay.

Three encryption algorithms are implemented on FPGA, among which the SM3 and SM4 algorithms are implemented using a full pipeline. Detailed information on the experimental results is shown in Table 5.

As the S-box in the SM4 algorithm uses block random access memory (BRAM), it occupies more BRAM. Many researchers have implemented parallel SM3 and SM4 algorithms on FPGAs, and the results are shown in Table 6.

Table 6 shows that after precomputation, pipeline technology, critical path optimization, and other methods are used to optimize the implementation, the performance of the SM3 and SM4 algorithms is improved by 43.2% and 36.1%, respectively, compared with other solutions, which has great advantages.

For the SM2 algorithm, the specific conditions of each mode's clock frequency, resource occupation, and calculation period are shown in Table 7.

Table 7 shows that when the point multiplication frequency is 29 MHz, the calculation can be completed after 3064 clock cycles, which is a very high calculation speed.

5.2.2. LZ4 Algorithm Implementation. The LZ4 algorithm reduces the amount of data transmitted on the network by compressing the network data. The single-module LZ4 and the two-way parallel LZ4 are implemented on FPGA. The results are shown in Table 8.

Table 8 shows that although the frequency of the implemented dual-channel LZ4 algorithm decreases, its performance increases by 1.84 times. According to different needs, the multichannel parallel LZ4 algorithm can be

TABLE 5: SM3 and SM4 algorithm implementation.

Algorithm	Algorithm structure	Frequency (MHz)	LUTs	FF	BRAM	Throughput (Gbps)
SM3	65-stage pipeline	240	24774	33189	0	115.2
SM4	98-stage pipeline	335	8284	10627	128	42.88

TABLE 6: Algorithm implementation comparison.

Algorithm	Implementation	Frequency (MHz)	Throughput
SM3	Ours	240	115.2 Gbps
	Zheng et al. [50]	36	263 Mbps
	Zang et al. [51]	415	6.4 Gbps
SM4	Ours	335	42.88 Gbps
	Fan et al. [34]	250	528 Mbps
	Yang et al. [35]	250	31.5 Gbps

TABLE 7: Implementation of SM2 modules.

Module	Frequency (MHz)	LUT	FF	DSP	Calculation period
Point addition	29	8911	4442	144	12
Point doubling	29	10056	3824	144	12
Point multiplication Control	29	1499	7251	0	3064
Coordinate transformation	29	16927	4356	144	225

TABLE 8: LZ4 algorithm implementation results.

Algorithm	Frequency (MHz)	LUT	FF	BRAM	Throughput (Mbps)
Single-module LZ4	110	8583	8072	98	880
Dual parallel LZ4	101	17481	16,632	196	1616

configured and transplanted to different application scenarios.

Different types of data are tested to verify the actual performance of the LZ4 algorithm. The results are shown in Table 9.

Table 9 shows that the LZ4 algorithm has the highest compression rate for pictures, i.e., the worst effect. It is because the LZ4 algorithm is a general-purpose compression algorithm, and an image requires a dedicated compression algorithm to reduce the compression rate. LZ4 has a better compression effect for other types of data.

The LZ4 algorithm is a solution proposed in this paper to reduce the network load. Different types and sizes of data are input for processing within a period of time, and the output data volume is determined. The test results are shown in Figure 18.

The experimental results in Figure 18 show that the compression performance of the LZ4 compression algorithm is related to the compressed data. By calculating the average compression ratio, it can be concluded that the LZ4 algorithm reduces the amount of original network data by 10%, which shows that the scheme proposed in this paper is effective.

5.2.3. Implementation of FPGA Underlying the Related Modules. The encryption algorithm and data compression algorithm are the core parts of the scheme of this article. To realize a complete data processing scheme, 10-Gigabit network interfaces, Gigabit network interfaces, data packet analysis and encapsulation, and key generation modules

implemented on FPGA are needed. The realization of each functional module is shown in Table 10.

The processing flows of the Gigabit and 10-Gigabit networks are basically the same, except that the working frequencies are different, and the bit widths of the processed data are 1 byte and 8 bytes, respectively. Therefore, bit width conversion is required before a data packet is encrypted or decrypted.

5.2.4. Network Performance Test. In a Gigabit network, since the LZ4 algorithm processes only the data filtered by ACL, a single-channel LZ4 algorithm can meet the requirements. Among the modules implemented, the lowest frequency of the LZ4 algorithm is 110 MHz, which gives the lowest throughput. Therefore, when implemented, the SM3 and SM4 algorithms also work at 110 MHz, which can meet the performance requirements. The network data of different sizes are encrypted, and the network performance is shown in Table 11.

Table 11 also shows that the data delay gap of different data sizes is relatively small, i.e., approximately 480. It is because the key agreement and key encryption calculation are first carried out in the entire system, which consumes some of the time. When the data start entering the compression and encryption stage, the data are processed continuously, which is independent of the size of the data. The processing time is from the beginning of data input to the time at which the output is complete. The greater the data length, the longer the processing time. As the data length

TABLE 9: LZ4 compression rate and compression speed.

Type of data	Before compression	After compression	Compression rate (%)	Compression speed (MB/s)
Network packet	1,536,000	1,406,664	91.58	107
Image	430,080	423,154	98.39	106
Text	147,456	680,686	46.16	109
Data sheet	16,461	13,379	81.28	108.4

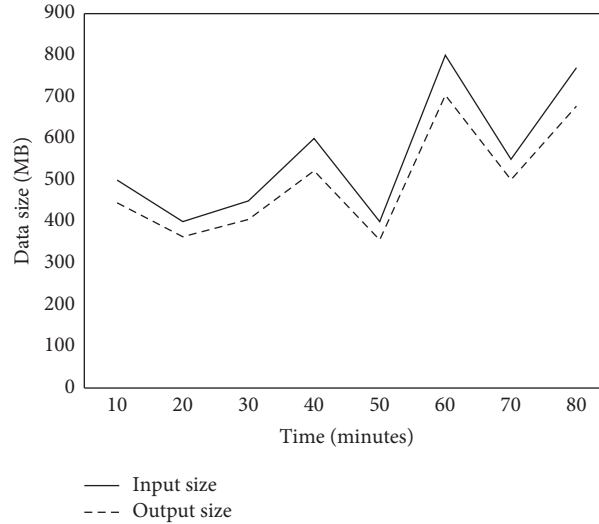


FIGURE 18: Network load changes.

TABLE 10: FPGA-related module implementation.

Functional module	Description	Frequency (MHz)	LUT	FF
ARM	ARM communication module	100	6487	8296
SFP_10GE_MAC	10-Gigabit network interface	156.25	4816	5457
Tri_Mode_Ethernet_MAC	Gigabit network interface	125	637	879
DDR_WR	Memory read-write interface	666.67	9321	7549
Frame_Parse	Data frame analysis	158	900	2336
Frame_Filter	Data frame filtering	158	1026	2673
Frame_Package	Data frame encapsulation	158	274	476
Key_LFSR	Key generation and update	158	517	1016
DataTransmission	High-speed data transmission	158	735	2037

TABLE 11: Gigabit network performance test.

Data length (MB)	Output delay (μ s)	Processing time (s)
100	480	1.7
200	478	2.3
300	484	3.05
400	481	3.78
500	484	4.17
600	483	5.15
700	476	6.11
800	488	6.504

increases, the processing performance of network data is closer to 1000 Mb/s, reaching 987 Mb/s. It indicates that when data protection is added, there is no additional delay in network transmission, which meets the network requirement of a low delay.

In the 10-Gigabit network, the data input speed is 10 Gb/s, and the 4-channel parallel LZ4 algorithm is implemented on FPGA with a frequency of 100 MHz. The network

performance test is shown in Table 12, and the network performance can be calculated as reaching 9302 Mb/s.

The network performance of the Gigabit network and the 10-Gigabit network reached 987 Mb/s and 9302 Mb/s, respectively, fulfilling the data processing requirements of Gigabit and 10-Gigabit networks in the overall design scheme. The encryption of the network data guarantees the privacy of the data, the effectiveness of the network load, and little network delay.

5.2.5. Computational Time Complexity Analysis. In the data protection scheme designed in this paper, the main calculation modules are key generation, high-speed data transmission, access control, the symmetric encryption algorithm SM4, the hash algorithm SM3, the key agreement algorithm SM2, and the data compression algorithm.

Key generation includes two parts: LFSR pseudo-random number generation and scrambling factor generation.

TABLE 12: 10 Gb network performance test.

Data length (MB)	Output delay (μ s)	Processing time (s)
10,000	482	9.8
20,000	484	17.1
30,000	477	25
40,000	483	33.4
50,000	482	43

LFSR generates 128-bit data. Hence, 128-level LFSR is required, which consumes 128 clock cycles. The scrambling factors FID, temperature, and RS are calculated at the same time during the initial configuration of the key. After the pseudo-random sequence is generated, the key generation is completed by one clock consumption. The calculation time T_{Key} for key generation is 129 clocks consumed.

High-speed data transmission is mainly used for data transmission between DDR and FPGA. It adopts burst data transmission and is actually tested on FPGA. When the frequency is 158 MHz, the maximum throughput is 4157 MB/s. When the size of the transmitted data is $Size_{Data}$, the transmission time is $Size_{Data}/4157$.

Access control includes data frame analysis, filtering, and encapsulation. When implementing, the corresponding data are extracted from a clock using the state selector and filtered through multicondition matching, and the corresponding operations are performed. Finally, the corresponding data are filled into the fixed position of the data frame. The computational complexity is mainly the realization of the state selector, the final frequency of the hardware realization is 158 MHz, and each data frame only needs to consume 1 clock.

SM4, SM3, and LZ4 are the most computationally complex parts of the data protection scheme. This article adopts a variety of optimization schemes to focus on implementation. A set of data can be calculated on each clock. Therefore, SM4, SM3, and LZ4 calculate one set for each clock. The data sizes are 128 bits, 480 bits, and 8 bits.

SM2 encrypts the key. It is calculated only once in a period of time, and the amount of calculation is small. Hence, the area is optimized. The time for one calculation is mainly point multiplication, and the time consumed by T_{SM2} is 3064 clock cycles.

In the data protection scheme, using the implementation and testing of each module, the calculation time complexity of the key factor in the LZ4 algorithm performance scheme is the key factor in the calculation time complexity. Therefore, when N groups of data need to be protected and the size of each group of data is M bytes, the total calculation time T_{all} is given by the following equation:

$$T_{all} = T_{Key} + T_{SM2} + (T_{Delay_LZ4} + N \times M) + T_{Delay_SM4} + T_{Delay_SM3}. \quad (14)$$

T_{Delay_LZ4} , T_{Delay_SM4} , and T_{Delay_SM3} are the output delays of LZ4, SM4, and SM3, respectively, and the specific values are 13, 99, and 66. LZ4 processes 1 byte of data each time and takes a total of $N \times M$. As SM4, SM3, and LZ4 are calculated in parallel, when the last set of data is compressed,

there is only one set of data to be encrypted, and the processing of N sets of data is completed after the encryption is delayed and output. The ACL and the data transmission module have small delays and are parallel modules. Therefore, the calculation time complexity is mainly based on data compression and encryption. When the data size is 1510, the time consumed can be calculated as shown in the following formula:

$$T_{all} = 129 + 3064 + (13 + N \times 1510) + 99 + 66. \quad (15)$$

5.3. Safety Analysis

5.3.1. Key Randomness Analysis. Encryption keys are the key to ensuring data security. In this paper, while incorporating the idea of mimic defense, three kinds of LFSR, DF , and time t are used as variable factors to generate keys. The initial key generated at time t is $Key(t) = LFSR \oplus DF$, $LFSR \in \{LFSR_1, LFSR_2, LFSR_3\}$, $DF \in \{FID, temperature, RS\}$.

According to different configuration attributes, the initial key has 9 different configuration combinations, and the LFSR and the scrambling factor are dynamically variable and related to the operating state of the system at the time. Therefore, the probability of generating the same initial key is low, ensuring the initial unpredictability of the key, and the encryption key of different frame data $fdata$ implements the idea of "one frame, one key." The calculation of the key within time t is as follows:

$$key_{FID} = \begin{cases} Key(t), & FID = 1, \\ key_{FID-1} \oplus SM3(fdata), & FID > 1. \end{cases} \quad (16)$$

The edge network and the server agree to generate an initial key at different time intervals using key agreement, and the minimum value of the time interval must meet the calculation time of the SM2 encryption key. The key is constantly changing, and the value at a certain moment is different from that at other moments, i.e., $Key(t_1) \neq Key(t_2) \neq \dots \neq Key(t_1)$, to ensure the dynamic nature of the key transformation. Different LFSRs have different rules for generating keys, which increases the attack disturbance, making it difficult for an attacker to crack the key in a short time, and the diversity of disturbance factors increases the difficulty of the attack. The pseudo-random number generator itself has a certain degree of randomness. The multiple initial keys generated in a certain period of time are again randomly selected as the final key, which is the second random selection, thereby further increasing the encryption key randomness.

5.3.2. Security Analysis of the Data Protection Scheme. The cryptographic standards proposed in China have high complexity and security, which makes the cost of deciphering by attackers exceed the possible benefits.

The encryption key uses the 256-bit SM2 algorithm to complete key negotiation between the two parties. It is based on the problem of discrete logarithms and has relatively high security and resistance to attacks. According to the

TABLE 13: Comparison of the security solutions.

Scheme	Year	Technology/method	Computing platform	Goals
Dar et al. [25]	2020	Context-Aware, RSA, ECC, DSA, AES, Blowfish, RC6	CPU	Protect IoT data security and reduce execution time and energy consumption
Zhao et al. [28]	2020	Data aggregation, bilinear pairing, Paillier homomorphic encryption	CPU	Solve the problem of limited bandwidth and data privacy protection of a single device
Soliman et al. [30]	2019	AES, LFSR, COLM, OCB	ARM + FPGA	Add a new security dimension to IoT devices and reduce area utilization and power consumption
Yang et al. [35]	2019	SM4-XTS, SM2, modular exponentiation	FPGA	Meet high-concurrency big data security requirements
Wang et al. [36]	2021	Double colour images encryption, compressive sensing	CPU	Reduce data volume and improve the efficiency of transmitting data
Fouad et al. [37]	2021	RSA, hybrid compression	CPU/ARM	Reduce the physical footprint and protect encrypted hidden data
Our System	—	Access control list One frame, one key SM4, SM3, SM2, LZ4	ARM + FPGA	Protect the privacy of edge network data, and increase the amount of data transmission

published $E(Fp(a, b))$, base point G , and order n , $2G$, $3G$, \dots , nG can be calculated, and $nG = O$. When a large number k is given, $P = kG$ can be easily calculated. However, given P and G , it is very difficult to infer k .

The SM3 algorithm is irreversible, and the hash values obtained differ for different content. Any change in the input information will cause a significant change in the hash result. It ensures that the key parameters of different data frames are very different, thereby protecting the frame data and preventing attackers from inverting the key based on the content of the frame. The SM3 operation is anticollision, and the collision threshold is on the order of 2^{256} . It is difficult to find two pieces of information with the same hash result, which can effectively prevent differential attacks.

Similarly, the SM4 algorithm uses brute-force cracking that requires an order of magnitude of 2^{128} . At the same time, data encryption uses the “one frame, one password” scheme. Even if a key replay attack or a ciphertext attack is used to crack a set of data frames, it is necessary to re-establish the attack chain and crack other groups of data.

The LZ4 algorithm provides data compression, which not only increases the network data load but also plays a role in data protection. Assume that when an attacker intercepts all encrypted data, he or she obtains a certain frame of plaintext data through key exhaustion attacks, ciphertext-only attacks, and differential attacks. The time required is t . If the key information required by the attacker is in the last frame of the data and the total data frame is m , when the data are not compressed, it takes only time t to crack, and after data compression is added, all the data need to be decrypted. The time is mt , and decrypting only the current frame data may result in garbled information i.e., passing the first SM4 encryption line of defense and the second line of defense brought by data compression so that the attacker’s attack chain is expanded from part to all of the data increases the cost of the attack, thereby further ensuring the privacy of all data.

This article uses video surveillance to test and add an attacker before and after the protection scheme equipment. At the front end without protection, the surveillance video can be obtained directly. At the back end of the protection

equipment, the data obtained by the attacker are worthless garbled data because of encryption, and only after the terminal is decrypted can the correct data be obtained. Therefore, applying the solution proposed in this article to edge network equipment can protect the confidentiality of data and achieve a higher security algorithm, which increases the attack difficulty.

5.3.3. Comparison with Other Security Solutions. The lightweight data protection scheme designed in this paper is oriented toward edge networks, and mobile networks and edge sensor networks are important components of edge networks. Therefore, the design scheme in this paper is compared with related security mechanisms, as shown in Table 13:

In terms of computing platforms, CPUs are used for implementation in the literature [25, 28, 36, 37]. Even if the calculation is performed using parallel technology, such as multithreading, it is still difficult for the computing efficiency to meet high-speed network data processing requirements, and FPGA using register transfer-level pipeline technology can achieve higher performance and has a larger performance advantage compared with CPU. In previous work [28, 30] using an FPGA for implementation in high-performance network applications, the encryption scheme does not consider the key factor, and the completeness of the system does not consider the changeable network environment. In terms of the core algorithm, the RSA algorithm is used for encryption in the literature [25, 37]. Under the same encryption length, the security of SM2 is much higher than that of RSA. At the same time, the calculation of multiple algorithms of the same type will increase the complexity of the algorithm and consume calculation resources. Encryption and compression are used to protect the security of image data in the literature [36, 37], however, computational efficiency and applicability are lacking for other types of data.

Table 13 shows that this article combines 4 security strategies to achieve data security in the edge network. Compared with other solutions, the proposed approach

provides more comprehensive data protection. The first strategy is the access control list, which is used to filter illegal data and reduce the recurrence of illegal data. The transmission and direct forwarding of unimportant data reduce processing, thereby reducing the energy consumption of system operations. Secondly, the use of a “one frame, one key” security key strategy resists ciphertext-only attacks and destroys the construction of the attack chain. Then, data compression not only reduces the space occupied by the data but also plays an important role in data security. Finally, the data encryption algorithm contains different types of operations that can perform key encryption, data encryption, and key update functions to meet different needs.

The design scheme of this article uses ARM and FPGA to realize the security mechanism together and implements a high-performance encryption algorithm and data compression algorithm on FPGA. FPGA is resistant to interference, and it is difficult for outsiders to obtain authorization to make internal changes. The security of the system is protected on the hardware. ARM can detect the operating state of FPGA using the feedback of FPGA, thereby changing the operating state of FPGA in real time and flexibly performing configuration and calculations. The algorithm implemented in this paper occupies fewer FPGA resources and has low operating power consumption. ARM is mainly used for mobile devices. It has the characteristics of a small structural area and high operational flexibility. Therefore, the combination of ARM and FPGA in an edge network device can satisfy the lightweight edge data protection requirements of the network.

6. Conclusions

The edge of the network is the first line of defense against malicious attacks. The lightweight edge network data protection scheme proposed in this paper is mainly composed of encryption algorithms and data compression algorithms. It uses LFSR and disturbance factors to generate a random, dynamic, and diverse initial key. The key is updated with the hash value of the data frame to realize the encryption method of “one frame, one key,” and the whole system is constructed using the heterogeneous calculation method of ARM-FPGA. The experimental results and analysis show that the encryption system has not only higher encryption throughput but also higher security. It can effectively prevent data leakage and resist key exhaustive attacks and ciphertext attacks. At the same time, the added data compression module not only reduces the amount of network data but also displays compressed, garbled information when the attacker obtains part of the data. It also provides data privacy protection to a certain extent. The lightweight data compression algorithm LZ4 can increase the network load by 10%.

The security protection mechanism proposed in this article includes access control, random key generation, data compression, and data encryption modules. Different modules can be dynamically transformed according to actual needs. For example, the efficient optimization method of the encryption algorithm on FPGA in this article is also

applicable to the advanced encryption standard (AES), elliptic curve cryptography (ECC), and SHA-256, which are equivalent algorithms. Hence, they can be replaced flexibly as needed. On the other hand, with the rapid development of chip technology, mobile devices integrate ARMs, GPUs, FPGAs, etc., to form a heterogeneous computing platform. As part of the edge network, the lightweight data security solution in this article is also applicable to mobile devices. It protects the data security of mobile devices and improves the data transmission speed through data compression.

In future work, we will conduct more in-depth research on edge network security mechanisms. The first objective is the division of data security levels. There are differences in the security level and implementation complexity of different encryption algorithms. Achieving the most reconfigurable security protection for optimal planning of different data guarantees maximum utilization of resources and energy consumption. The second goal is to further establish the security mechanism of the edge network using reliability theory, network coding, combination design, etc., develop the theoretical model of the edge network, and evaluate the security of the data protection mechanism based on theoretical simulations. Finally, the edge node and the server establish a dedicated and lighter-weight secure communication protocol. Therefore, it is important to ensure that when an FPGA-based edge device is attacked, it can actively discover, dynamically reconfigure, and improve the device's antiattack ability.

Data Availability

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

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant 61702518 and in part by the National Key R&D Program Key Special Project of China under Grant 2018XXXXXXXX01.

References

- [1] J. Zhou, H. J. Shen, Z. Y. Lin, Z. F. Cao, and X. L. Dong, “Research advances on privacy preserving in edge computing,” *Journal of Computer Research and Development*, vol. 57, no. 10, pp. 2027–2051, 2020.
- [2] A. Paul, *2020 Internet Crime Report*, Internet Crime Complaint Center, USA, 2020.
- [3] W. House, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program. Report of the National Science and Technology Council*, Executive Office of the President, 2011.
- [4] S. Tennina, O. Gaddour, A. Koubâa, F. Royo, M. Alves, and M. Abid, “Z-Monitor: a protocol analyzer for IEEE 802.15.4-

- based low-power wireless networks,” *Computer Networks*, vol. 95, pp. 77–96, 2016.
- [5] Y. Zou and G. Wang, “Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack,” *IEEE Transactions on Industrial Informatics*, vol. 12, no. 2, pp. 780–787, 2016.
 - [6] M. Albanese, S. Jajodia, and S. Venkatesan, “Defending from stealthy botnets using moving target defenses,” *IEEE Security & Privacy*, vol. 16, no. 1, pp. 92–97, 2018.
 - [7] S. Venkatesan, M. Albanese, and K. Amin, “A moving target defense approach to mitigate DDoS attacks against proxy-based architectures,” in *Proceedings of the 2016 IEEE Conference on Communications and Network Security (CNS)*, pp. 198–206, IEEE, Philadelphia, PA, USA, October 2016.
 - [8] H. Almohri, L. T. Watson, and D. Evans, “Predictability of IP address allocations for cloud computing platforms,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 500–511, 2019.
 - [9] J. H. Jafarian, E. Al-Shaer, and Q. Duan, “An effective address mutation approach for disrupting reconnaissance attacks,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2562–2577, 2015.
 - [10] J. H. Jafarian, E. Al-Shaer, and Q. Duan, “Adversary-aware IP address randomization for proactive agility against sophisticated attackers,” in *Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 738–746, IEEE, Kowloon, Hong Kong, April 2015.
 - [11] F. Song, Y. T. Zhou, Y. Wang, T. Zhao, I. You, and H. K. Zhang, “Smart collaborative distribution for privacy enhancement in moving target defense,” *Information Sciences*, vol. 479, pp. 593–606, 2018.
 - [12] H. Tang, Q. T. Sun, X. Yang, and K. Long, “A network coding and DES based dynamic encryption scheme for moving target defense,” *IEEE Access*, p. 1, 2018.
 - [13] D. Ma, L. Wang, and L. Cheng, “Thwart eavesdropping attacks on network communication based on moving target defense,” in *Proceedings of the 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, pp. 1–2, IEEE, Las Vegas, NV, USA, December 2016.
 - [14] G. Lin, M. Dong, and K. Ota, “Security function virtualization based moving target defense of SDN-enabled smart grid,” in *Proceedings of the 2019 IEEE International Conference on Communications (ICC) (ICC 2019)*, IEEE, Shanghai, China, May 2019.
 - [15] S. Wang, Y. Zhou, and R. Guo, “A novel route randomization approach for moving target defense,” in *Proceedings of the 2018 IEEE 18th International Conference on Communication Technology (ICCT)*, IEEE, Chongqing, China, October 2018.
 - [16] E. M. Ghourab and M. Azab, “Benign false-data injection as a moving-target defense to secure mobile wireless communications,” *Ad Hoc Networks*, vol. 102, no. 9, Article ID 102064, 2020.
 - [17] H. Hu, J. Wu, Z. Wang, and G. Cheng, “Mimic defense: a designed-in cybersecurity defense framework,” *IET Information Security*, vol. 12, no. 3, pp. 226–237, 2018.
 - [18] Y. Ming and E. Wang, “Identity-based encryption with filtered equality test for smart city applications,” *Sensors*, vol. 19, no. 14, p. 3046, 2019.
 - [19] X. Zhou, B. Li, Y. Qi, and W. Dong, “Mimic encryption box for network multimedia data security,” *Security and Communication Networks*, vol. 2020, no. 2, pp. 1–24, Article ID 8868672, 2020.
 - [20] N. M. Truong, M. Aoki, Y. Igarashi, M. Saito, and K. Yamamoto, “Real-time lossless compression of waveforms using an FPGA,” *IEEE Transactions on Nuclear Science*, vol. 65, no. 9, pp. 2650–2656, 2018.
 - [21] C. Wang, D. Wang, Y. Tu, G. Xu, and H. Wang, “Understanding node capture attacks in user authentication schemes for wireless sensor networks,” *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 507–523, 2020.
 - [22] Q. Tong, Z. Zhang, W. Zhang, and J. Wu, “Design and implementation of mimic defense web server,” *Journal of Software*, vol. 28, no. 4, pp. 883–897, 2017.
 - [23] P. Pavithran, S. Mathew, S. Namasudra, and P. Lorenz, “A novel cryptosystem based on DNA cryptography and randomly generated mealy machine,” *Computers & Security*, vol. 104, 2020.
 - [24] P. Zhang, C. Lin, Y. Jiang, Y. Fan, and X. Shen, “A lightweight encryption scheme for network-coded mobile ad hoc networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2211–2221, 2014.
 - [25] Z. Dar, A. Ahmad, F. A. Khan et al., “A context-aware encryption protocol suite for edge computing-based IoT devices,” *The Journal of Supercomputing*, vol. 76, no. 4, pp. 2548–2567, 2020.
 - [26] S. Qiu, D. Wang, G. Xu, and S. Kumari, “Practical and provably secure three-factor Authentication protocol based on extended chaotic-maps for mobile lightweight devices,” *IEEE Transactions on Dependable and Secure Computing*, 2020.
 - [27] C. Y. Wang, D. Wang, G. A. Xu, and D. B. He, “Efficient privacy-preserving user authentication scheme with forward secrecy for Industry 4.0,” *Science China Information Sciences*, 2020.
 - [28] O. Zhao, X. Liu, X. Li, P. Singh, and F. Wu, “Privacy-preserving data aggregation scheme for edge computing supported vehicular ad hoc networks,” *Transactions on Emerging Telecommunications Technologies*, 2020.
 - [29] A. L. P. de França, R. P. Jasinski, and V. A. Pedroni, “Moving network protection from software to hardware: an energy efficiency analysis,” in *Proceedings of the 2014 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, IEEE, Tampa, FL, USA, pp. 456–461, 2014.
 - [30] S. Soliman, M. A. Jaela, A. M. Abotaleb et al., “FPGA implementation of dynamically reconfigurable IoT security module using algorithm hopping,” *Integration*, vol. 68, pp. 108–121, 2019.
 - [31] S. Pontarelli, C. Greco, E. Nobile, and S. Teofili, “Exploiting dynamic reconfiguration for FPGA based network intrusion detection systems,” in *Proceedings of the 2010 International Conference on Field Programmable Logic and Applications (FPL)*, pp. 10–14, IEEE, Milano, Italy, August 2010.
 - [32] S. Pontarelli, G. Bianchi, and S. Teofili, “Traffic-aware design of a high-speed FPGA network intrusion detection system,” *IEEE Transactions on Computers*, vol. 62, no. 11, pp. 2322–2334, 2013.
 - [33] Y. Zhang, D. He, M. Zhang, and K.-K. Raymond Choo, “A provable-secure and practical two-party distributed signing protocol for SM2 signature algorithm,” *Frontiers of Computer Science*, vol. 14, no. 3, 2019.
 - [34] L. Y. Fan, M. Zhou, J. J. Luo, and H. L. Liu, “IC design with multiple engines running CBC mode SM4 algorithm,” *Journal of Computer Research and Development*, vol. 55, no. 6, pp. 1247–1253, 2018.
 - [35] G. Q. Yang, H. C. Ding, J. Zou, H. Jiang, and Y. Q. Chen, “A big data security scheme based on high-performance cryptography implementation,” *Journal of Computer Research and Development*, vol. 33, pp. 12755–12776, 2019.

- [36] K. Wang, X. Wu, and T. Gao, "Double color images compression-encryption via compressive sensing," *Neural Computing and Applications*, pp. 1–22, 2021.
- [37] O. Fouad, A. Khalaf, A. I. Hussein, and H. F. A. Hamed, "Hiding data using efficient combination of RSA cryptography, and compression steganography techniques," *IEEE Access*, vol. 9, pp. 31805–31815, 2021.
- [38] Z. Zhang, X. Q. Zhang, D. C. Zuo, and G. D. Fu, "Research on target tracking application deployment strategy for edge computing," *Journal of Software*, vol. 31, no. 9, pp. 2691–2708, 2020.
- [39] A. K. Panda, P. Rajput, and B. Shukla, "Design of multi bit LFSR PNRG and performance comparison on FPGA using VHDL," *International Journal of Advances in Engineering & Technology*, vol. 3, no. 1, pp. 566–571, 2012.
- [40] Y. Liu, H. Liang, W. Wang, M. Wang, and J. Díaz-Verdejo, "New linear cryptanalysis of Chinese commercial block cipher standard SM4," *Security and Communication Networks*, vol. 2017, Article ID 1461520, 2017.
- [41] A. P. Kakarountas, H. Michail, A. Milidonis, C. E. Goutis, and G. Theodoridis, "High-speed FPGA implementation of secure hash algorithm for IPsec and VPN applications," *The Journal of Supercomputing*, vol. 37, no. 2, pp. 179–195, 2006.
- [42] B. S. Jangareddi and G. Sridevi, "A cryptographic based implementation of secure hash algorithm by using microblaze processor," *International Journal of Research in Computer and Communication Technology*, vol. 3, no. 10, pp. 1379–1383, 2014.
- [43] D. Ravilla and C. S. R. Putta, "Enhancing the security of MANETs using hash algorithms," *Procedia Computer Science*, vol. 54, pp. 196–206, 2015.
- [44] J. Zou and L. Dong, "Improved preimage and pseudo-collision attacks on SM3 hash function," *Journal on Communications (in Chinese)*, vol. 39, no. 1, pp. 46–55, 2018.
- [45] M. S. Hossain, Y. Kong, E. Saeedi, and N. C. Vayalil, "High-performance elliptic curve cryptography processor over NIST prime fields," *IET Computers & Digital Techniques*, vol. 11, no. 1, pp. 33–42, 2016.
- [46] S. Khan, K. Javeed, and Y. A. Shah, "High-speed FPGA implementation of full-word Montgomery multiplier for ECC applications," *Microprocessors and Microsystems*, vol. 62, pp. 91–101, 2018.
- [47] W. Yu, K. Wang, B. Li, and S. Tian, "Montgomery algorithm over a prime field," *Chinese Journal of Electronics*, vol. 28, no. 1, pp. 43–48, 2019.
- [48] K. Javeed and X. Wang, "FPGA based high speed SPA resistant elliptic curve scalar multiplier architecture," *International Journal of Reconfigurable Computing*, vol. 2016, Article ID 6371403, 10 pages, 2016.
- [49] J. Kim and J. Cho, "Hardware-accelerated fast lossless compression based on LZ4 algorithm, International academy of computing technology (IACT)," in *Proceedings of the 2019 3rd International Conference on Digital Signal Processing (ICDSP 2019)*, pp. 67–70, Jeju Island, Republic of Korea, February 2019.
- [50] X. Zheng, X. Hu, J. Zhang, J. Yang, S. Cai, and X. Xiong, "An efficient and low-power design of the SM3 hash algorithm for IoT," *Electronics*, vol. 8, no. 9, p. 1033, 2019.
- [51] S. Zang, D. Zhao, Y. Hu et al., "A high speed SM3 algorithm implementation for security chip," in *Proceedings of the 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, pp. 915–919, Chongqing, China, March 2021.

Research Article

Adaptive Weight Adjustment and Searching Perception Strategy for Multivariate Complex Environments

Wenshan Wang ¹, Jianguo Sun ¹, Sizhao Li ^{1,2}, Junpeng Wu ¹ and Qingan Da ¹

¹Department of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China

²Department of Information Engineering, The Chinese University of Hong Kong, Hong Kong, 999077, China

Correspondence should be addressed to Sizhao Li; sizhao.li@hrbeu.edu.cn

Received 9 July 2021; Revised 23 November 2021; Accepted 23 December 2021; Published 24 January 2022

Academic Editor: Weizhi Meng

Copyright © 2022 Wenshan Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Affected by the complex environment and the destruction of communication infrastructure in the disaster-stricken area, it has brought great challenges to the search and rescue team. The use of small unmanned aerial vehicles (UAVs) for search tasks can minimize casualties. Therefore, in order to avoid any possible collision and search for unknown targets in the shortest time, it is necessary to design a multi-UAV cooperative target search strategy. In this paper, we analyze the unknown target search problem of multi-UAVs under random dynamic topology and propose an adaptive target search strategy based on the whale algorithm. First of all, each UAV detects the environmental information of its current area and uses the probability map search algorithm to gain the target existence probability map in the task area. Then, the whale optimization search method of shrinking circle or spiral is selected to update the position of the UAV to continuously approach the target. Finally, the obstacle avoidance strategy based on artificial potential field is designed to solve any collision problems that may be encountered during the flight of UAVs. Simulations on multi-UAVs target search in different scenarios show that compared with the whale optimization algorithm, the proposed algorithm can reduce the search time by 43.1% and the total path cost by 18.1%, and it is also superior to the advanced metaheuristic optimization algorithms such as PSO and GWO.

1. Introduction

Due to its high flexibility and autonomy, UAVs can perform surveillance and search tasks in complex environments, especially in postdisaster search and rescue scenarios [1]. In search and rescue missions, to locate the missing target is usually unclear, and it is important to complete the rescue mission 72 hours after the disaster [2]. In the traditional search method, rescuers are scattered in all mission areas, which is inefficient and dangerous. Compared with traditional search methods, a postdisaster rescue based on multi-UAV search is an effective method. However, the former is more challenging. Due to the complexity and unknowability of the environment, solving the problem of crashes between UAV and UAV and UAV and obstacles during the flight has also become the key to the safe execution of multi-UAVs.

UAV path optimization is a global optimization problem [3], which aims to increase the performance indicators during the entire mission execution, including search likelihood and search time. At present, there are many methods to solve the problem of multi-UAV collaborative search, which are mainly divided into two categories. One is the graph search method based on sampling. The second is the metaheuristic optimization method based on swarm intelligence.

First, the graph search method based on sampling divides the search space into grids or hash points and expands feasible planning paths through different search mechanisms. For example, A star algorithm, Probabilistic Road Map (PRM), and Voronoi diagram search algorithm, Song et al. [4] proposed a sparse A* search algorithm, which can be applied to the obstacle avoidance scenarios in a complex environment and can effectively avoid threats and realize the search and monitoring of targets in the task area. In

order to make up for the disadvantages of traditional UAVs that take a long time to perform tasks and poor stability, Cai et al. [5] proposed a path planning strategy based on the improved A* algorithm, which improved the efficiency of UAV missions. Probabilistic Road Map (PRM) is a path planning algorithm based on random sampling strategy [6], which can solve the problem of difficulty in constructing effective paths in high-dimensional space. However, this algorithm requires a large amount of sampling data, which leads to increased calculation time and reduced efficiency. Farooq et al. [7] proposed a collision-avoidance UAV formation reconstruction and probabilistic roadmap navigation algorithm which complete UAV path planning with obstacle avoidance function. Xu et al. [8] proposed a dynamic exploration planner (DEP) based on incremental sampling and PRM to explore unknown environments. PRM allows DEP to quickly search for paths and avoid obstacles for safe exploration. In order to solve the path planning problem of multi-UAV searching for multiobjective, Chen et al. [9] used the Voronoi diagram to create the task area scene, preliminarily determined the cost of total path, and then planned the optimal path of multi-UAVs by setting up a path solving framework. To reduce the energy consumption of UAV and prolong its service life, Baek et al. [10] proposed a UAV route algorithm based on Voronoi diagram to provide a hovering position for UAV with low computational complexity. Then, the hovering position of each UAV was adjusted in turn according to the sensor energy state to obtain the optimal UAV route.

These algorithms mentioned above can solve the conventional path planning problem well. However, with the increasing complexity of the task environment in which UAVs are found, the requirements for the calculation and execution time of the algorithm are also getting higher and higher.

Second, the metaheuristic optimization method is a commonly used method in solving path planning problems, because these algorithms not only have strong robustness and good generalization but also can find possible solutions that meet the requirements in a short time. In these algorithms, the path planning task is regarded as a complex optimization problem, which is solved by intelligent algorithms such as particle swarm optimization (PSO) algorithm, ant colony optimization (ACO) algorithm, and gray wolf optimization (GWO) algorithm. PSO is one of the commonly used heuristic optimization algorithms in path planning, but it is easy to fall into local optimization. To solve this problem, Gou and Li [11] proposed a PSO algorithm based on inertia weight of logistic function. This algorithm has fast execution speed and good global optimization ability. But as the number of UAVs increases, its search accuracy will decrease accordingly. Therefore, Sánchez-García et al. [12] proposed a path planning algorithm based on Distributed Particle Swarm Optimization (DPSO) to achieve the needs of fast convergence and precise search. However, this algorithm cannot achieve a satisfactory result when the target location is unclear and there are too many obstacles in the disaster area. Zhen et al. [13] used a hybrid artificial potential field and ant colony optimization (HAPF-ACO) method to search for targets in an uncertain environment and

constructed the target attraction field and threat repulsive field, which improved the global search ability of UAVs. This scheme has advantages in task execution efficiency and collision avoidance performance, but it is not suitable for emergency environment because of high time cost. Liu et al. [14] improved the ant colony algorithm and designed a multi-UAV path planning algorithm to avoid the problem of slow optimization. But the algorithm ignores the energy waste problem when multiple drones repeatedly search the same area. Jarray and Bouallègue [15] proposed a method based on GWO for flight path planning of UAVs to ensure destination arrival and obstacle avoidance, whereas this method has slow convergence speed and high overhead. For this reason, Liu et al. [16] proposed a whale optimization algorithm, which improved the global search ability of WOA by introducing adaptive weights and nonlinear convergence factors. This method improves the ability of UAV to adapt to complex map and provides a new idea for solving the problem of UAV path planning. But this method is aimed at the known target search problem and does not consider the case of unknown target search. In recent years, deep reinforcement learning has been widely used in path planning scenarios. For single UAV path planning problem, Li et al. [17] proposed a trajectory planning algorithm based on deep reinforcement learning (DRLTP), which gradually learns the best value by training a deep neural network on the UAV to optimize the flight trajectory in real time. For multi-UAV path planning problem, Yu et al. [18] proposed an extended deep deterministic policy gradient (DDPG) algorithm to learn the control strategy of UAV in target search, which solved the problem of target assignment and path planning for multi-UAVs in complex environments. Nevertheless, the data sampling efficiency of the DRL algorithm is not ideal, and it is difficult to be competent for rescue tasks in emergency scenarios.

Motivated by this, we propose an adaptive search strategy based on a whale optimization algorithm (ASWOA) for multi-UAVs to quickly find lost persons in disaster scenarios with less energy consumption. Figure 1 clearly shows how the ASWOA is related to path planning. In particular, in the first stage, we establish the whale optimization algorithm (WOA) and add the obstacle avoidance strategy. If the position of a UAV updated by the whale algorithm is within an obstacle area, the obstacle avoidance strategy will be executed to ensure that the UAV will not collide with the obstacle. Since the target position is unknown, the traditional method of using the distance between the current position of the UAV and the target position as the fitness function is not appropriate. Therefore, in the second stage, we introduce the target probability strategy. Since the UAV flying over the task area has a certain range of sight, the closer it is to the target, the greater the target existence rate. Otherwise, the smaller the target presence rate. We restrict the flight direction of multi-UAVs in the third stage to avoid invalid search. When there is no target in an area unit searched by a UAV, the area unit is marked. The more times the target is marked, the lower the probability of the target appearing in this area unit. Since multi-UAVs are interconnected, other UAVs will no longer fly towards this area unit.

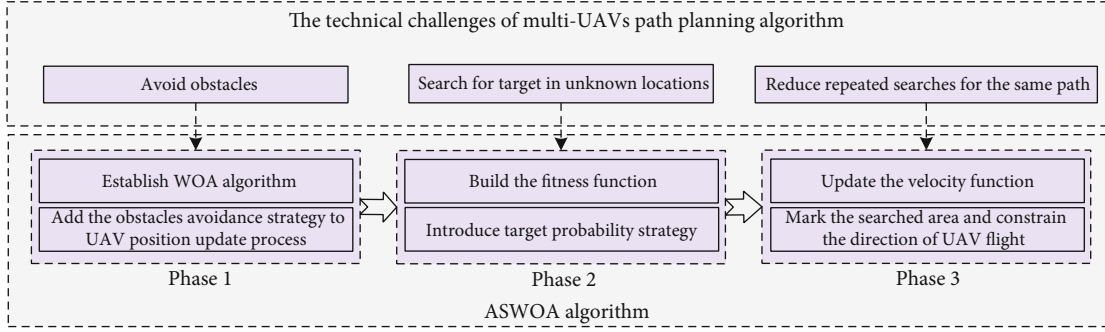


FIGURE 1: Proposed ASWOA model process.

Based on the above discussion, we consider the comprehensive design factors (e.g., the success rate of target searching, the search time, and the cost of repeated search paths) and propose the ASWOA of multi-UAVs for unknown target searching. Through our algorithm, the success rate of multi-UAVs for searching the unknown target has been significantly improved. The contributions of this work are as follows:

- (i) The obstacle avoidance strategy based on virtual forces is used to improve the flight safety of multi-UAVs and reduce repeated paths and energy consumption
- (ii) The probability map search strategy is used to update the probability of the target existence in the task area to improve the search ability of the population
- (iii) Adaptive inertia weight is introduced to balance the convergence speed of the algorithm
- (iv) The position adjacent to the UAV with the highest target existence rate is selected as the optimal solution to improve the convergence speed of the algorithm

The rest of the paper is organized as follows. Section 2 is the description and modeling of the target searching problem by multi-UAVs and discusses the path planning strategy based on the whale algorithm. Section 3 presents numerical simulation results and performance comparison with other algorithms and verifies the effectiveness of the proposed algorithm. Lastly, the conclusion and future work are drawn in Section 4 to close our paper.

2. Optimal Deployment of Multi-UAVs

2.1. System Model and Problem Formulation. In this paper, N highly manoeuvrable UAVs are used to search for lost target in an unknown environment. The specific mission requirements are as follows: in a complex mission environment, multi-UAVs need to avoid environmental obstacles, form a reasonable formation, and find the lost target as soon as possible to ensure the rescue team has enough time to carry out a rescue mission. Each UAV is regarded as a particle moving in a three-dimensional space, which make new action decision and find the target at every moment. As shown in Figure 2, each quadrotor UAV can move in

eight directions, that is, it can move from the current cell to the adjacent cell.

The mechanism of UAV for detection and data collection uses wireless communication technology [19, 20] or artificial vision technology [21, 22] and transmits monitoring information in a multihop manner [23]. The channel is determined by the line-of-sight (LOS) link and non-line-of-sight (NLOS) link [24]. Whenever a communication link can be established between two UAVs, they will exchange information about the best candidate. Lost in personnel can help themselves to be found by sending out distress signals via smart devices such as phone. Although missing persons can help themselves to be found by sending out distress signals via smart devices such as phones, sometimes, these devices cannot work or the communication base station is damaged [25]. Therefore, in the paper, we consider using multi-UAVs to search and rescue the lost person without receiving any distress signal. The strategy of using multi-UAV cooperative path planning mainly includes centralized control structure and distributed control structure [26, 27]. In the former, since the communication between UAVs is handled by a single control centre, the optimal deployment of multi-UAVs based on global information can be realized, but its expansibility is poor, and the calculation amount of the central node increases exponentially with the increase of the number of agents [28]. In the distributed control structure, a single UAV can autonomously interact with local information [29], which significantly reduces the amount of calculation in each UAV node and has better flexibility and expansibility. In consequence, compared with centralized control, most researchers choose distributed control strategy for unknown environments. Similarly, the distributed cooperative control strategy is also used in this paper to study the path planning of multi-UAVs.

The multi-UAV target searching model based on distributed control structure is shown in Figure 3. We divide a $H_x \times H_y$ rectangular task area \mathfrak{R} into M cells and use $[gx_j, gy_j]$ to represent the position of cell ζ_j , where $[gx_j, gy_j] \in \mathfrak{R}$ and $1 \leq j \leq M$. Obstacles are randomly distributed in the task area and are represented by symbol O . The target position is denoted by $T = [tx, ty]$. The multi-UAVs are distributed over the task area, and we use $[ux_i, uy_i, uz_i]$ to represent the position of UAV i , where $[ux_i, uy_i] \in \mathfrak{R}$, $1 \leq i \leq N$, N is the number of UAVs, $h_{\min} \leq z_i \leq h_{\max}$, and h_{\min} and h_{\max} ,

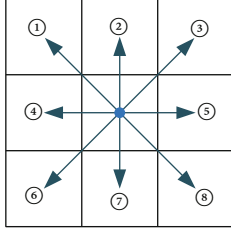


FIGURE 2: The direction of movement of the UAV.

respectively, represent the minimum and maximum flying height of the UAV. In Figure 3, we also see that under the premise of a certain antenna beam width, the flying height of the UAV is proportional to the coverage radius R , which can be represented by $R_i = uz_i \times \tan \theta$, where θ is the cone half angle of UAV. In this paper, the size of R_i is set to be half of the task area cell.

2.2. The Adaptive Target Searching Strategy Based on Whale Algorithm. The Whale optimization algorithm is a random swarm intelligent optimization algorithm modeled by simulating the predation mode of whales in nature. It uses individual whales to update their own position and estimate the position of the prey with a certain optimization strategy, to achieve the optimal algorithm and convergence to the optimal [30]. The strategy architecture of ASWOA is shown in Figure 4, which mainly includes several modules such as target probability graph module, fitness function module, and obstacle avoidance module.

In this paper, each UAV is regarded as a whale in the three-dimensional search space, so the ASWOA is a population composed of N whales, and the position of the i whale is $[ux_i, uy_i, uz_i]$. Each whale constantly updates its position on the signals it catches to get closer to its prey.

2.2.1. Path Marking. In order to improve the task efficiency of multi-UAVs and reduce the waste of energy caused by the repeated searches of multi-UAVs in a certain area, we have defined the concept of nontarget existence rate of regional cell.

Definition 1. The nontarget existence probability $\eta(\zeta_j)$ of the cell will increase if the position ζ_j of the area cell searched by the UAV at a certain moment is not the position of the target.

$$\eta(\zeta_j) = \eta_j(\zeta_j) + 1, \quad \zeta_j \neq T \text{ and } \zeta_j \in \{\mathfrak{R} - O\}, \quad (1)$$

where $\zeta_j \in \{\mathfrak{R} - O\}$ denotes the nonobstacle area in the task area. The larger the value of $\eta(\zeta_j)$, the smaller the probability of target existence in the area, and the UAV should avoid searching this area.

In addition, we record the number of area cells that each UAV has searched and the number of area cells that have been repeated searches, so as to avoid too fast convergence of UAV and provide constraints for UAV position updated

in the following ASWOA. The number of area cells SN_i that UAV $_i$ has searched and the number of area cells RP_i that have been repeated searches are calculated as follows:

$$SN_i = SN_i + 1, \quad i \in N, \quad (2)$$

$$RP_i = RP_i + 1, \quad i \in N, \text{ if } [ux_i, uy_i, uz_i] \in \text{Path}_i, \quad (3)$$

where Path_i denotes the trajectory of the UAV $_i$.

2.2.2. Obstacle Avoidance. In the problem of multi-UAV path planning, once obstacles or other UAVs are predicted by the algorithm, the corresponding actions will be taken through obstacle avoidance strategy to get rid of potential threats.

(1) *Collision Avoidance between UAV and Obstacle.* We fit the obstacles in the task area as a rectangle area with threat values. If the UAV detects an obstacle in front of the flight, it will retreat to its previous position.

$$UAV_i(t+1) = \begin{cases} UAV_i(t), & R_i \geq D(UAV_i, O_j), \\ UAV'_i(t+1), & \text{else,} \end{cases} \quad (4)$$

where $UAV_i(t)$ represents the position of UAV $_i$ at time t , $UAV'_i(t+1)$ represents the position of UAV $_i$ at time $t+1$ obtained by the ASWOA, and $D(UAV_i, O_j)$ represents the distance between UAV $_i$ and the obstacle O_j .

(2) *Collision Avoidance between UAV and UAV.* In addition to the above obstacles affecting the flight safety of UAVs, the distance between UAVs should also be considered during the formation process; otherwise, it is easy to collide. We adopt the virtual force strategy to adjust the flight direction of the UAV to avoid disasters.

Definition 2. There will be a virtual repulsion between the two UAVs if the distance between UAV $_i$ and UAV $_k$ is less than the coverage radius of the UAVs.

In order to reduce the energy consumption of the multi-UAVs, according to Figure 1 and Equation (1), we choose the UAV with a few searching cells to move due to virtual repulsion. For example, if $SN_i < SN_k$ is satisfied, UAV $_i$ generates repulsive force F_{ik} .

$$F_{ik} = X - UAV_i(t), \quad (5)$$

where $X \in H_{UAV_i}$ and $\eta(X) = \min(\eta(H_{UAV_i}))$, H_{UAV_i} denotes the set of adjacent position units of UAV $_i$ (as shown in Figure 2), and X represents the position where the nontarget existence probability is the lowest in the adjacent position unit of UAV $_i$, i.e., $\eta(X) = \min(\eta(H_{UAV_i}))$.

2.2.3. Fitness Function Setting. As mentioned above, the multi-UAVs need to avoid obstacles to find the target node. The target is said to have been detected if the position of UAV meets the following conditions.

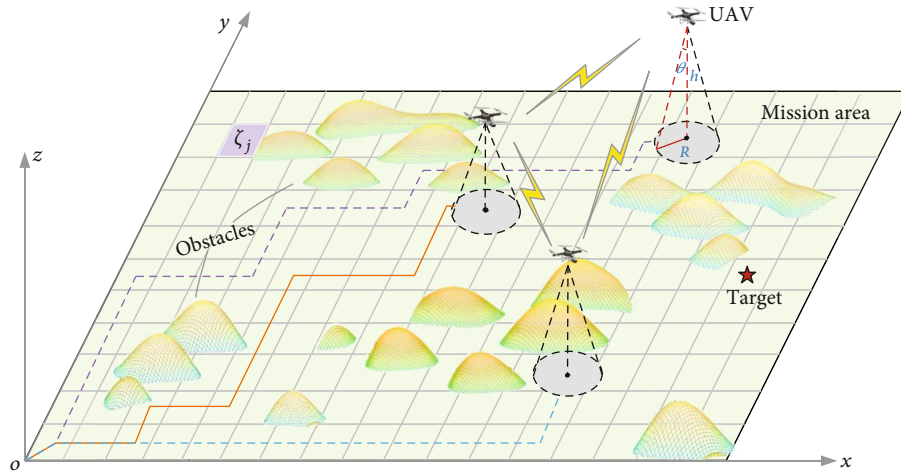


FIGURE 3: Multi-UAV target searching model based on distributed control structure.

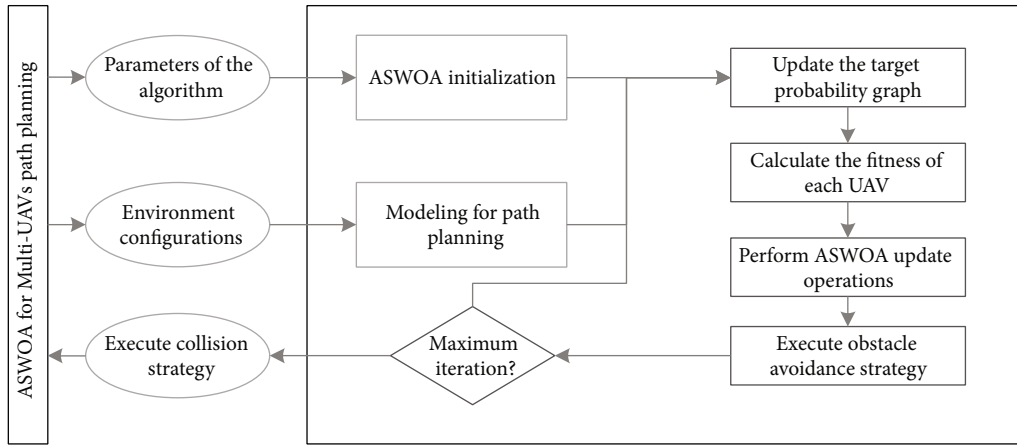
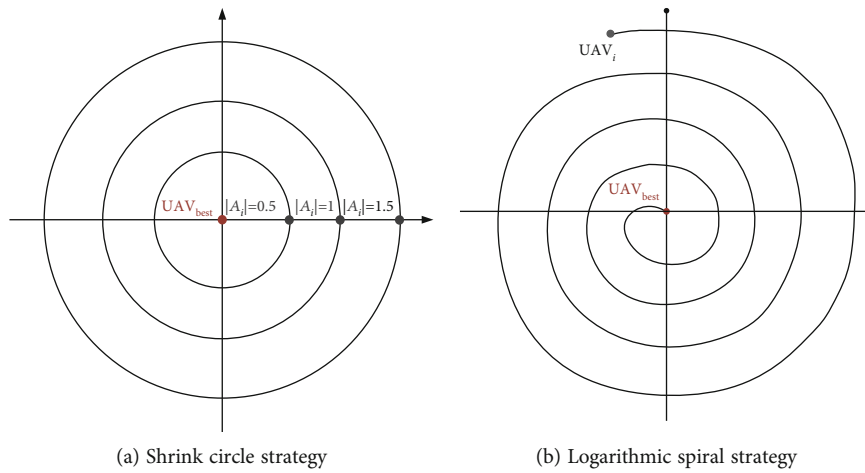


FIGURE 4: Architecture of ASWOA.



(a) Shrink circle strategy

(b) Logarithmic spiral strategy

FIGURE 5: The strategy of UAV position update in ASWOA.

```

Algorithm 1 ASWOA
Input: The UAV cluster UAV, task area  $\mathfrak{R}$ , obstacles set  $\mathcal{O}$ 
Output: Optimal paths for multi-UAVs Path
1 Initialize the UAV cluster  $UAV = \{UAV_1, UAV_2, \dots, UAV_N\}$  and the task area set  $\mathfrak{R} = \zeta \cup \mathcal{O}$ 
2 Calculate the fitness of each individual UAV according to Equation (6)
3 while  $t < \tau$  do
4   for  $UAV_i$  in UAV do
5     Update the values of parameters  $\alpha_1, \alpha_2, \alpha_3, \beta, A_i, l$ 
6     if  $\alpha_1 < 0.5$  then
7       if  $|A_i| < 1$  then
8         Update the position of  $UAV_i$  according to Equation (8) and Equation (9)
9       else if  $|A_i| \geq 1$  then
10        Update the position of  $UAV_{rand}$  according to Equation (11)
11        Update the individual position according to Equation (10)
12      end if
13    else if  $\alpha_1 \geq 0.5$  then
14      Update the position of  $UAV_i$  according to Equation (8)
15    end if
16    Determine whether the  $UAV_i$  exceeds the task area
17    Implement obstacle avoidance strategy according to Equation (3) and Equation (4)
18    Add the current position of  $UAV_i$  to the path set  $Path_i$ 
19    Calculate the fitness of each UAV according to Equation (6)
20
21    Update the global optimal solution  $UAV_{best}$ 
22  end for
23 end while
24 Return to the path planning of the UAV cluster

```

ALGORITHM 1: The ASWOA flow

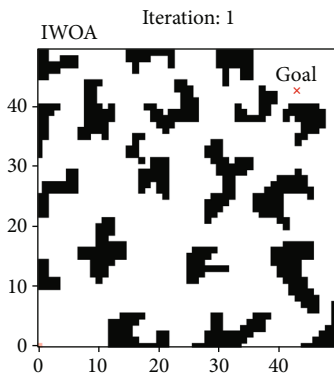


FIGURE 6: The scene of the multi-UAV path planning space.

Definition 3. T is said to be found by UAV_i if the two-dimensional projection position of UAV_i and the position of the target T are less than or equal to the coverage radius R_i .

$$D_i = \sqrt{(ux_i - tx)^2 + (uy_i - ty)^2} \leq R_i. \quad (6)$$

It is known that the choice of fitness function can directly affect the convergence speed of the algorithm and the value of the optimal solution. The principle of path selection for multi-UAVs is to choose less repeated coverage route to find the unknown target node and save the energy consumption of multi-UAVs. We use the fitness function to evaluate the best

path of the UAV. According to Equations (1), (2), and (3), we define the fitness function as

$$\text{fitness} = \begin{cases} \lambda_1 \omega \cdot \exp(\eta(UAV_i(t)) + 1) + \lambda_2 \log_2\left(\left(\frac{RP_i}{(SN_i + 1)}\right) + 1\right), & UAV_i(t) \neq T, \\ 0, & \text{else,} \end{cases} \quad (7)$$

$$\omega = \frac{2\tau}{t + 1}, \quad (8)$$

where ω is called the adaptive inertia weight, which is used to balance the convergence speed and exploration ability of the ASWOA. λ_1 and λ_2 are constants, and $\lambda_1 = \lambda_2$. $\eta(UAV_i(t))$ represents the search times of the current position searched by UAV_i . When the value of fitness function is 0, it means that the UAV has found the target.

2.2.4. Position Update. The process of the ASWOA searching for targets is divided into the development stage and exploration stage.

(1) *Development Stage.* The UAV simulates a whale to produce a bubble network of shrinking circles to update its position to gradually approach and surround the target. The position update equation of the UAV is as follows:

$$\text{UAV}_i(t+1) = \begin{cases} \text{UAV}_{\text{best}}(t) - A_i \cdot D_{1,i}, & \alpha_1 < 0.5, \\ D_{2,i} \cdot e^{bl} \cdot \cos(2\pi l) + \text{UAV}_i(t), & \alpha_1 \geq 0.5, \end{cases} \quad (9)$$

where t is the current iteration number, UAV_{best} is the optimal solution position, and α_1 is a random variable between $[0, 1]$. When $\alpha_1 < 0.5$, we choose a shrinking circle to surround the target, as shown in Figure 5(c). $D_{1,i} = \|C_i \text{UAV}_{\text{best}}(t) - \text{UAV}_i(t)\|$ is the contraction circle, and the values of other parameters are shown in

$$\begin{cases} A_i = 2\beta\alpha_2 - \beta, \\ C_i = 2\alpha_3, \\ \beta = 2 - \frac{2t}{\tau}, \end{cases} \quad (10)$$

where α_2 and α_3 are random variables between $[0, 1]$ and τ represents the maximum number of iterations of the algorithm.

In order to prevent the target from falling into the local optimal by using only the shrink circle search strategy, we use the logarithmic spiral search strategy to expand the optimal solution when $\alpha_1 \geq 0.5$, as shown in Figure 5(b). In Equation (9), b is the constant of the logarithmic spiral shape, and l is a random variable between $[-1, 1]$, so as to better search for the optimal solution space. $D_{2,i}$ represents the length of the i th whale from the target, and $D_{2,i} = \|\text{UAV}_{\text{best}}(t) - \text{UAV}_i(t)\|$ is the distance between the i th solution and the current optimal solution.

(2) *Exploratory Stage*. The position of the target in the whale predation is known, but in the collaborative path planning of multi-UAVs, the position of the target is unknown. In this paper, the optimal solution obtained in each iteration is set as the target position, and each UAV keeps approaching this target. $A_i \in [-\beta, \beta]$, the current whale randomly selects the position of other whales UAV_{rand} as the target position when $|A_i| \geq 1$, then the position update equation of the whale UAV_i at this time.

$$\text{UAV}_i(t+1) = \text{UAV}_{\text{rand}}(t) - A_i \|C_i \cdot \text{UAV}_{\text{rand}}(t) - \text{UAV}_i(t)\|. \quad (11)$$

2.2.5. *ASWOA for Multi-UAV Path Planning*. After the above description, Algorithm 1 provides the detailed implementation process of ASWOA for multi-UAVs path planning.

3. Simulation Analysis

Based on the ASWOA description, in the first part of this section, we introduce the parameter setting of the proposed algorithm in the simulation. Second, through the evaluation and comparison of a series of simulation experiments, we confirmed that ASWOA has the ability to find unknown target in emergency scenarios for multi-UAVs.

TABLE 1: List of important notations used in the paper and value of system parameters.

Symbol	Description	Value
N	The number of UAVs	10
M	The number of cells in the mission area	—
ζ_j	A cell of the mission area	—
O	The set of obstacles	—
T	The position of target, $T = [tx, ty]$	—
UAV_i	The position of UAV, $\text{UAV}_i = [ux_i, uy_i, uz_i]$	—
h_{\min}	Minimum height of UAVs	30 m
h_{\max}	Maximum height of UAVs	150 m
R_i	The radius of an area covered by UAV_i	—
θ	Detector perspective	$\frac{\pi}{9}$
τ	Simulation step size	300
t	Number of current iterations	—

TABLE 2: The performance of ASWOA with different constant values.

λ_1	λ_2	$N_{\text{iteration}}$	N_{UAVs}	N_{repeat}	L_{average}	L_{shortest}
0.1	0.9	300	0	343	189.51	—
0.2	0.8	300	0	327	271.21	—
0.3	0.7	222	4	295	313.72	136.36
0.4	0.6	150	6	266	252.23	184.16
0.5	0.5	141	6	129	220.11	158.92
0.6	0.4	120	6	117	212.55	144.18
0.7	0.3	132	6	213	227.99	166.0
0.8	0.2	195	6	433	238.96	222.12
0.9	0.1	240	3	486	316.24	275.05

3.1. *Parameter Setting*. First, we set the size of the task area R to $50 * 50$. Then, we divide R evenly into 1×1 cells and randomly mark the position of obstacles in R . Finally, the position of multi-UAVs and target node is initialized. In this paper, the UAVs do not know the terrain (including the position of obstacles and target). The terrain is modeled through simulation, and the altitude of multi-UAVs during the flight is uniform and unchanged. The path planning environment of multi-UAVs is shown in Figure 6, where obstacles are modeled as black areas.

The important notations of related sets, variables, and parameters, as well as main parameter values in this paper, are summarized in Table 1. In addition, as in Equation (7), the values of the constants λ_1 and λ_2 affect the rate of population convergence and the selection of the optimal solution, and $\lambda_1 + \lambda_2 = 1$. If λ_1 is too small, the population convergence rate is slow and it is easy to fall into local optimum. If λ_2 is too small, the population cannot guarantee whether the route it takes has been searched, which increases repeated paths and waste resources. After several experiments, the average

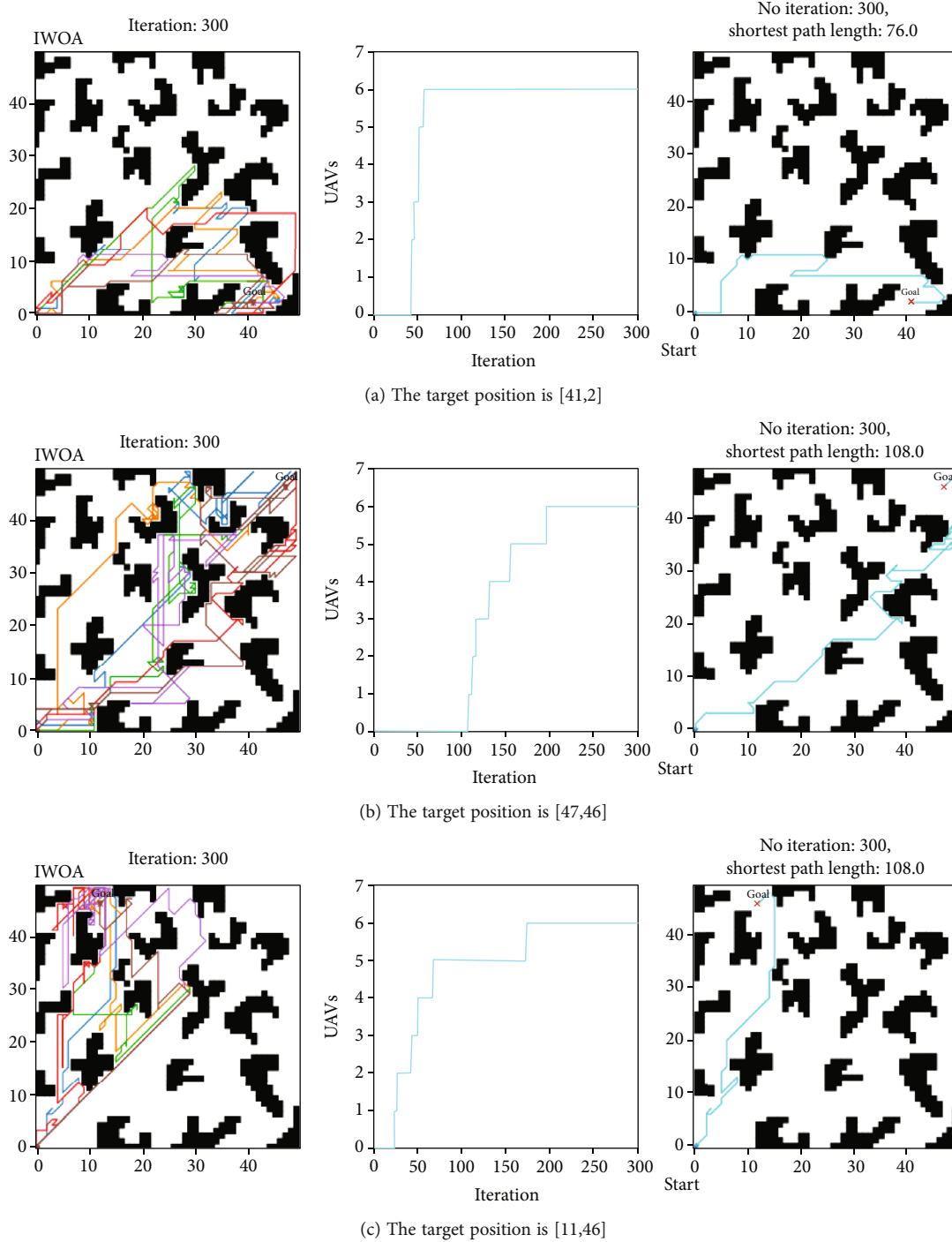


FIGURE 7: Path planning and shortest route results for multi-UAVs in the same location.

performance of the ASWOA with different constant values is shown in Table 2, where κ is the number of iterations when the first UAV finds the target node. If the UAV cluster fails to find the target before the maximum number of iterations of the program, $N_{\text{iteration}}$ is set to the value of τ . N_{UAVs} refers to the total number of UAVs that found the target node. N_{repeat} represents the total number of repeated search cells. L_{average} denotes the average path of the multi-UAVs, and

L_{shortest} represents the shortest path of the UAV from the starting point to the target node. In Table 2, we can see that if λ_1 is too small, the time $N_{\text{iteration}}$ it takes for the UAV to find the target node is correspondingly longer, which is not suitable for emergency environments. Besides, with the decrease of λ_2 , the number N_{repeat} of area cells repeatedly searched by multi-UAVs and the average path length L_{average} of multi-UAVs also increase. In consequence, we set $\lambda_1 = 0.6$ and

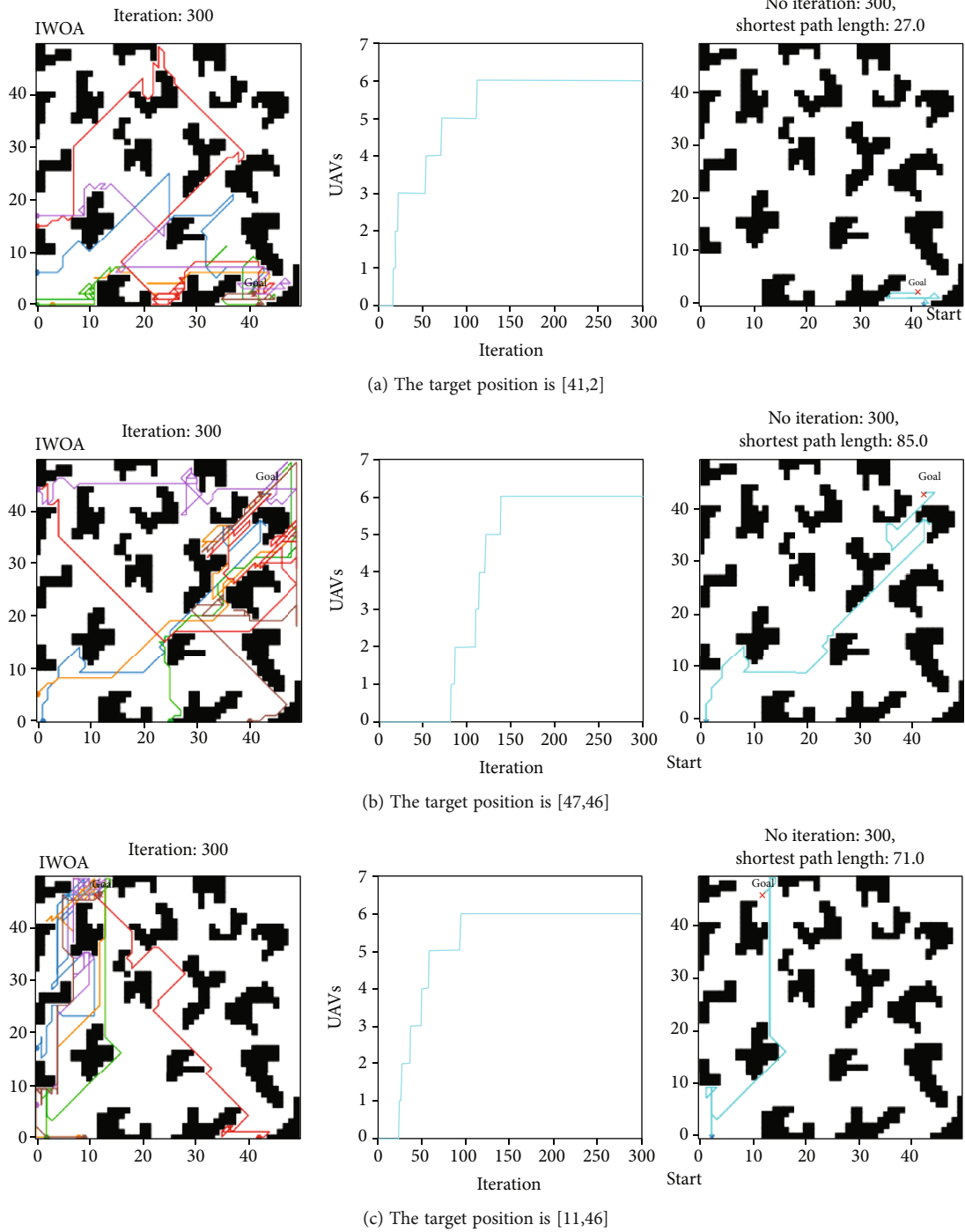


FIGURE 8: Path planning and shortest route results for multi-UAVs in the different locations.

$\lambda_2 = 0.4$; in this case, the algorithm can achieve the best performance, that is, it takes less time for the UAV to find the target and the path it takes is shorter.

3.2. Analysis of Experimental Results. To confirm the reliability of ASWOA, we carried out simulations of different starting points and ending points and conducted extensive simulations, comparisons, and experiments.

3.2.1. Simulation of ASWOA

(1) Dispatching of UAVs from the Same Position. Figure 7 shows the path planning for dispatching multi-UAVs at the same position. In different unknown position target scenarios, ASWOA enables each UAV to avoid obstacles and find target. Moreover, after the first UAV finds the target, the other UAVs can also find the target in a short time. Further, we can see the shortest route taken by the multi-UAVs in Figure 7.

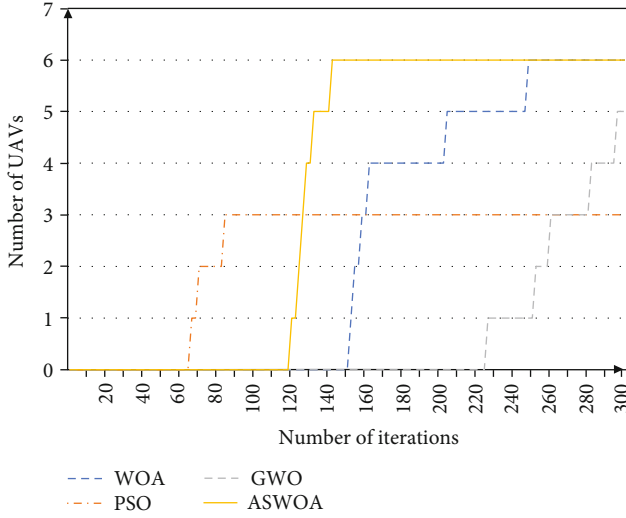


FIGURE 9: Comparison of the number of UAVs and the time cost that use four algorithms to find unknown target.

(2) *Dispatching of UAVs from Different Positions.* When a major disaster occurs, it is usually to dispatch multiple rescue teams from different directions to search for targets at the same time. Figure 8 shows the path planning for dispatching multi-UAVs from different positions. Without knowing the specific position of the missing person, ASWOA allows each UAV to avoid obstacles and share information until it finds the target. Compared with Figure 7, it is obvious that dispatching multi-UAVs from different positions takes shorter time and has a relatively lower path cost than dispatching multi-UAVs from the same position.

3.2.2. *Comparison with Other Optimization Algorithms.* To further evaluate the performance of ASWOA, we compared it with other heuristic optimization algorithms, including the WOA [16], PSO [11], and GWO [15] algorithms. Considering the randomness of the heuristic algorithm, each test algorithm is executed 30 times independently.

Figure 9 plots the speed comparison of six UAVs searching for unknown target node under the same initial position. The convergence speed of the PSO algorithm is relatively fast. When the number of iterations is 66, the UAV cluster finds the target node for the first time, whereas only three UAVs find target, and the remaining three UAVs stagnate around the obstacle, falling into the local optimum. Although the GWO algorithm has more UAVs to find the target node than the PSO algorithm, the convergence speed is slower. When the number of iterations is 227, the UAVs find the target node for the first time, which takes too long to be suitable for emergency scenarios. The WOA can satisfy all UAVs to search for unknown target, but the convergence speed is still slower than that of the ASWOA. The ASWOA can complete the task in only 20 iterations, which is 4.75 times faster than the WOA.

Due to the limited energy of UAVs, it is necessary to reduce path costs in a limited time. Figure 10 shows the comparison of repeated paths, average paths, and shortest paths of the four algorithms. Although the PSO algorithm

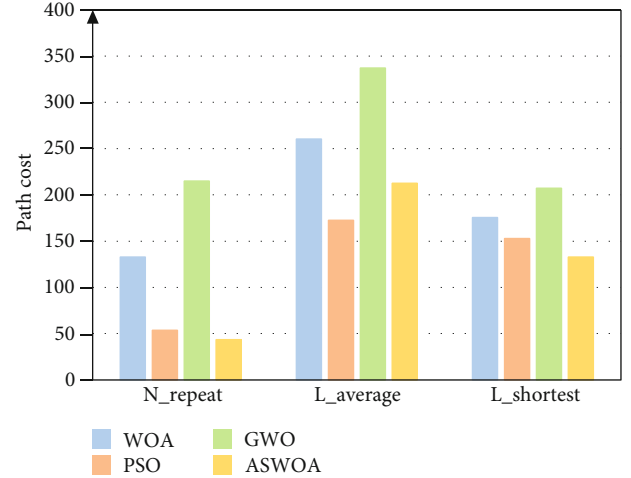


FIGURE 10: The path cost comparison with WOA, PSO, and GWO algorithms.

has better performance in average path consumption, it can be seen from Figure 9 that the PSO algorithm has three UAVs falling into the local optimal and fails to find the target node, so the total path cost is relatively low. The GWO algorithm has high cost of repeated search and path, which is not suitable for emergency scenarios with limited energy resources. Since the ASWOA incorporates strategy to reduce repeated paths, the cost of both repeated paths and average paths is less.

4. Conclusions

In this paper, an adaptive target searching strategy based on the whale algorithm has been successfully applied to solve the multi-UAV search unknown target. We first design a probability map algorithm to calculate the target existence probability map, then use the whale optimization algorithm to optimize the search paths of multi-UAVs. In addition, we design an obstacle avoidance strategy based on virtual repulsion force to avoid any collision problems that may be encountered during the flight of UAVs. In this paper, practical constraints are considered to define various flight scenarios of the UAV. Simulation results show that, compared with other algorithms, the AWOA algorithm has the advantages of high search efficiency and low path cost.

Data Availability

All the data can be generated according to the steps described in our paper, and readers can also ask for the data by contacting wangwenshan@hrbeu.edu.cn.

Conflicts of Interest

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

Acknowledgments

We thank laboratory team members for their assistance with the experiments. This work was supported by the National Natural Science Foundation of Heilongjiang Province of China (JJ2019YX0922) and the Basic Science Research Plan (JCKY2019210B029).

References

- [1] J. Dong, K. Ota, and M. Dong, "UAV-based real-time survivor detection system in post-disaster search and rescue operations," *IEEE Journal on Miniaturization for Air and Space Systems*, vol. 2, no. 4, pp. 209–219, 2021.
- [2] Y. Shih, A. Pang, and P. Hsiu, "A doppler effect based framework for wi-fi signal tracking in search and rescue operations," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 3924–3936, 2017.
- [3] X. Zhang and X. Chen, "UAV task allocation based on clone selection algorithm," *Wireless Communications and Mobile Computing*, vol. 2021, 9 pages, 2021.
- [4] R. Song, T. Long, Z. Wang, Y. Cao, and G. Xu, "Multi-UAV cooperative target tracking method using sparse a search and standoff tracking algorithms," in *IEEE CSAA Guidance, Navigation and Control Conference (CGNCC)*, pp. 1–6, Xiamen, China, 2018.
- [5] Y. Cai, Q. Xi, X. Xing, H. Gui, and Q. Liu, "Path planning for UAV tracking target based on improved A-star algorithm," in *International Conference on Industrial Artificial Intelligence (IAI)*, pp. 1–6, Xiamen, China, 2019.
- [6] J. Chen, Y. Zhou, J. Gong, and Y. Deng, "An improved probabilistic roadmap algorithm with potential field function for path planning of quadrotor," in *Chinese Control Conference (CCC)*, pp. 3248–3253, Guangzhou, China, 2019.
- [7] M. U. Farooq, Z. Ziyang, and M. Ejaz, "Quadrotor UAVs flying formation reconfiguration with collision avoidance using probabilistic roadmap algorithm," in *International Conference on Computer Systems, Electronics and Control (ICCSEC)*, pp. 866–870, Dalian, China, 2017.
- [8] Z. Xu, D. Deng, and K. Shimada, "Autonomous UAV exploration of dynamic environments via incremental sampling and probabilistic roadmap," *IEEE Robotics and Automation Letters*, vol. 6, no. 2, pp. 2729–2736, 2021.
- [9] X. Chen, G. Li, and X. Chen, "Path planning and cooperative control for multiple UAVs based on consistency theory and Voronoi diagram," in *Chinese Control and Decision Conference (CCDC)*, pp. 881–886, Chongqing, China, 2017.
- [10] J. Baek, S. I. Han, and Y. Han, "Energy-efficient UAV routing for wireless sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 1741–1750, 2020.
- [11] Q. Gou and Q. Li, "Task assignment based on PSO algorithm based on logistic function inertia weight adaptive adjustment," in *International Conference on Unmanned Systems (ICUS)*, pp. 825–829, Harbin, China, 2020.
- [12] J. Sánchez-García, D. G. Reina, and S. L. Toral, "A distributed PSO-based exploration algorithm for a UAV network assisting a disaster scenario," *Future Generation Computer Systems*, vol. 90, pp. 129–148, 2019.
- [13] Z. Zhen, Y. Chen, L. Wen, and B. Han, "An intelligent cooperative mission planning scheme of UAV swarm in uncertain dynamic environment," *Aerospace Science and Technology*, vol. 100, article 105826, 2020.
- [14] G. Liu, X. Wang, B. Liu, C. Wei, and J. Li, "Path planning for multi-rotors UAVs formation based on ant colony algorithm," in *International Conference on Intelligent Computing, Automation and Systems (ICICAS)*, pp. 520–525, Chongqing, China, 2019.
- [15] R. Jarray and S. Bouallègue, "Paths planning of unmanned aerial vehicles based on grey wolf optimizer," in *International Conference on Advanced Systems and Emergent Technologies (IC_ASET)*, pp. 56–62, Hammamet, Tunisia, 2020.
- [16] K. Liu, C. Xv, D. Huang, and X. Ye, "UAV path planning based on improved whale optimization algorithm," in *IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE)*, pp. 569–573, Guangzhou, China, 2021.
- [17] K. Li, W. Ni, E. Tovar, and M. Guizani, "Deep reinforcement learning for real-time trajectory planning in UAV networks," in *International Wireless Communications and Mobile Computing (IWCMC)*, pp. 958–963, Limassol, Cyprus, 2020.
- [18] Y. Yu, J. Tang, J. Huang, X. Zhang, D. K. C. So, and K.-K. Wong, "Multi-objective optimization for UAV-assisted wireless powered IoT networks based on extended DDPG algorithm," *IEEE Transactions on Communications*, vol. 69, no. 9, pp. 6361–6374, 2021.
- [19] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via joint trajectory and power control," *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 1376–1389, 2019.
- [20] M. M. Azari, G. Geraci, A. Garcia-Rodriguez, and S. Pollin, "UAV-to-UAV communications in cellular networks," *IEEE Transactions on Wireless Communications*, vol. 19, no. 9, pp. 6130–6144, 2020.
- [21] L. Qingqing, J. Taipalmaa, J. P. Queralta et al., "Towards active vision with UAVs in marine search and rescue: analyzing human detection at variable altitudes," in *IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR)*, pp. 65–70, Abu Dhabi, United Arab Emirates, 2020.
- [22] J. Keller, D. Thakur, M. Likhachev, J. Gallier, and V. Kumar, "Coordinated path planning for fixed-wing UAS conducting persistent surveillance missions," *IEEE Transactions on Automation Science and Engineering*, vol. 14, no. 1, pp. 17–24, 2017.
- [23] X. Wei and J. Xu, "Distributed path planning of unmanned aerial vehicle communication chain based on dual decomposition," *Wireless Communications and Mobile Computing*, vol. 2021, 12 pages, 2021.
- [24] H. Wang, H. Zhao, W. Wu, J. Xiong, D. Ma, and J. Wei, "Deployment algorithms of flying base stations: 5G and beyond with UAVs," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10009–10027, 2019.
- [25] Z. Liu, P. Qian, X. Wang, Y. Zhuang, L. Qiu, and X. Wang, "Combining graph neural networks with expert knowledge for smart contract vulnerability detection," *IEEE Transactions on Knowledge and Data Engineering*, p. 1, 2021.
- [26] Z. Yuan, C. Du, J. Chen, and F. Ling, "Central-distributed control model of UAV group and its application in perception module," in *IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, pp. 677–681, Chongqing, China, 2019.
- [27] Z. Zhen, D. Xing, and G. Chen, "Cooperative search-attack mission planning for multi-UAV based on intelligent self-organized algorithm," *Aerospace Science and Technology*, vol. 76, pp. 402–411, 2018.

- [28] X. Zhou, W. Wang, T. Wang, X. Li, and Z. Li, "A research framework on mission planning of the UAV swarm," in *System of Systems Engineering Conference (SoSE)*, pp. 1–6, Waikoloa, HI, USA, 2017.
- [29] H. X. Pham, H. M. La, D. Feil-Seifer, and M. C. Deans, "A distributed control framework of multiple unmanned aerial vehicles for dynamic wildfire tracking," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 4, pp. 1537–1548, 2020.
- [30] A. Mohamed, A. Ewees, A. Hassanien, M. Mudhsh, and S. Xiong, "Multi-objective whale optimization algorithm for multilevel thresholding segmentation," in *Advances in Soft Computing and Machine Learning in Image Processing*, pp. 23–39, Springer, Cham, 2018.

Research Article

A Hierarchical Provable Massive Data Migration Method under Multicloud Storage

Ma Haifeng,^{1,2} Yu HaiTao ,³ Zhang Ji,¹ Wang Junhua,¹ Xue Qingshui,¹ and Yang Jiahai²

¹School of Computer Science and Information Engineering, Shanghai Institute of Technology, Shanghai 201418, China

²Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China

³School of Tourism and Landscape, Guilin University of Technology, Guilin 541004, China

Correspondence should be addressed to Yu HaiTao; albertyht@163.com

Received 27 June 2021; Revised 8 October 2021; Accepted 9 November 2021; Published 17 December 2021

Academic Editor: Ding Wang

Copyright © 2021 Ma Haifeng 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.

Now, many users have stored files on multiple clouds, and sometime, a large number of files are migrated between clouds. Because cloud providers and cloud servers are not entirely trusted, the corruption of user's files event occur from time to time during the processes of storage and migration. Therefore, integrity verification must be performed, and the time verification overhead should be as low as possible. The existing provable data migrate methods still have the issue of high time overhead when a large number of files are migrated. Aiming at this problem, this paper proposed a hierarchical provable data migration method, which can provide the efficiency of data transfer integrity verification when moving large number of continuous files between clouds. In this paper, the proposed method is described in detail as well as the security analysis performance evaluation. The results proved that the proposed method can significantly decrease the detection latency of files transfer between clouds.

1. Introduction

With the booming development of cloud computing, Internet of Things, and mobile devices etc., our lives have changed profoundly due to convenience and challenge to us. Mobile devices play a central role in the emerging Internet of Everything era. Various kinds of mobile devices appear in our daily life, which facilitate a wide variety of online services [1] due to the provision of continuous and reliable connectivity. However, many emerging challenges have to be considered while deploying mobile devices in large scale due to different characteristics from traditional personal computers, servers, and laptops [2]. For example, mobile devices no longer meet the requirements for limited storage capacity, and cloud storage is the ultimate solution. It can provide massive storage and can reduce overhead of data management significantly. As a result, a large number of users already use cloud storage services and some of them have saved files on multiple clouds. Besides access data, cloud storage users sometimes migrate massive files between

clouds. However, because the cloud service providers and cloud servers are not completely trusted, files corruption on the cloud occurs frequently during migration process. Therefore, data integrity verification must be performed during the process of cloud storage and files migration. At the same time, the original data was confirmed to delete, and it also requires verification overhead.

Data integrity verification of cloud storage is to verify whether the user's data on cloud storage servers are in good condition so that it is avoided that data of users on cloud storage are tampered with or removed. At present, researches on cloud storage integrity mainly focus on two aspects: provable data possession (PDP) [3–6] and proof of retrievability (POR) [7, 8]. Based on pseudorandom sampling, their basic idea is to decrease communication overhead by taking advantage of some form of challenge-response protocol and probabilistic inspection method. PDP proves that files of users are integrated by means of challenge-response protocol. Although PDP can detect higher than a certain percentage of data corruption, it is guaranteed that files are retrievable. Similar

to PDP, POR also uses challenge-response protocols to prove the integrity of files. In addition, users are capable of retrieving files from servers with high probability.

Although many verification methods of data migration between clouds are proposed currently, most of these solutions need to verify all the files. Because complex cipher operations are necessary when authentication is implemented, the authentication of massive files will result in very high computation and communication overhead and even authentication failure. Motivated by the problem, this paper proposed a hierarchical provable data migration method for the scenario of massive data migration between clouds, which is a kind of efficient selection authentication method and can significantly reduce computation and communication overheads as well as bandwidth requirements.

Our contribution can be summarized as follows:

- (1) Pinpointing the source of the efficiency problem in Xue et al.'s scheme [9]. This paper proposes an efficient and secure data migration verification method. It provides efficient integrity protection with strong evidence that untrustworthy server cannot pass the verification unless it indeed keeps the data intact. The authentication time of massive data migration between clouds can be obviously reduced, thus improving the authentication efficiency of file migration
- (2) This paper give a security analysis of the proposed scheme based on our security model and prove that our scheme is secure against internal and external attacks. Moreover, this paper evaluate the performance of proposed scheme and put comparisons with Xue et al.'s scheme
- (3) The proposed method is a verification mode, and it can be combined with other provable data possession and provable data transfer method to further improve authentication efficiency. It also can be applied to many data integration authentication scenarios, such as single cloud storage, multcloud storage, and Internet of things
- (4) The security intensity of the proposed method can be adjusted, either high security intensity and high overhead with fine-grained authentication, or low security intensity and low overhead with coarse-grained authentication

2. Related Work

Ateniese et al. [3] proposed PDP model, a light weight method for remote data authentication. The disadvantages of PDP lie in: the times of data update and authentication are limited and it does not support data with dynamic types. For the reason, an improved PDP [10] is proposed based on public key encryption support files. Different from statistic PDP, the improved PDP can implement operations of update and delete for file blocks. However, the improved PDP does not still support insert operation of file blocks.

Erway et al. proposed DPDP [11], a framework for dynamic provable data possession. On the basis of PDP, DPDP provides the operations of insert, update, and delete for file blocks by means of an authenticated skip list. Wang et al. presented another improved PDP scheme supporting full dynamic operation. The scheme guarantees the correctness of the data block in the position using Merkle hash tree and guarantees the integrity of data value using BLS signature. Curtmola [12] proposed MR-PDP scheme for the verification of multiple different replicas. Etemad [13] also proposed a scheme which can verify not only the contents of files but also the number of replicas. However, due to more encryption computing caused by multiple replicas operation, additional computational overhead is increased.

Xue et al. [9] proposed a provable data transmission scheme, the data owner can migrate the data from one cloud server to another one and check the data integrity through provable data possession scheme, it allows a semitrusted cloud server to generate a simple proof to prove that the data deletion command was executed correctly, and the transmitted data was deleted correctly. Liu et al. [14] designed an improved new provable data transfer scheme, which can resist more attack and more efficient in data integrity checking compared with scheme [9]. Wang et al. [15] proposes an auditing scheme for cloud storage services, and the scheme has the properties of secure data transfer, provable data erasure, high error detection probability, and confidential data storage. The above three schemes are all efficient data transfer authentication methods. However, in above three schemes, all the transfer files between clouds need to be authenticated.

Wang et al. proposed the provable data possession with outsourced data transfer (DT-PDP) [16] scheme. It can satisfy the following: the purchased data integrity and privacy can be ensured; the data transferability's computation can be outsourced to the public cloud servers. Reference [17] proposed a cryptographic-accumulator provable data possession (CAPDP) method, which is based on the RSA password accumulator to verify the integrity of the outsourced data, reducing the data owners' burden and overhead of the verification process. Reference [18] proposed the Tagging of Outsourced Data (TOD), where a tag is used to generate and verify files. Users with lower overhead can achieve data verifiability of public and private and can resist label forgery and tampering. However, because TOD is designed based on the conventional sampling inspection, it is not guaranteed that TOD can detect cloud service provider's illegal behaviors with high probability.

Juel et al. proposed POR model [7] which can guarantee the possession and retrievability of data files on remote servers by means of spot-checking and error-correcting codes, respectively. "sentinels," some special blocks for detections, are embedded into data files at random. The disadvantages of POR lie in queries that are performed at fixed times at clients, and public verifiability is not supported. Combining with the research work of Juel and Shacham, Bowers et al. provided an improved version of POR protocol [8].

Shacham et al. [19] used Ateniese's homomorphism authentication tag to construct a homomorphism authenticator

based on BLS signatures. Because short signatures contribute to the aggregation of individual signatures, a very small authenticated value is necessary for public verifiability. The proposed scheme not only decreases the communication overhead for verifications but also supports challenges with unlimited times.

Wang [20] proposed a scheme where file data privacy is guaranteed by the introduction of a random number in basic BLS signature scheme during challenge-response processes. The disadvantage of the scheme is not supporting insert operation. Reference [21] considers preventing the indistinguishability and privacy of the auditor in the outsourcing data integrity audit. Reference [22] proposed a security audit scheme based on identity protection and a multireplica data scheme.

Reference [23] proposed a conditional identity privacy-preserving mechanism for cloud-based WBANs (wireless body area networks). This scheme is mainly used to protect the identity privacy and sensitive information of patients's EHRs. They used public auditing to ensure that the data integrity of patients and prevents malicious cloud service providers from returning error audit reports. Reference [24] proposed a forward secure PEKS scheme (FS-PEKS) based on lattice assumptions for cloud-assisted Industrial Internet of Things (IIoT). They integrate a lattice-based delegation mechanism with keyword search into FS-PEKS to achieve forward security, and the security of the system is still guaranteed when the keys are compromised by the adversaries. Reference [25] proposed a privacy-preserving anonymous authentication scheme for WBANs. The scheme can provide the message integrity and develop a conditional tracking system to track the misbehaving doctors in the WBAN

3. Preliminaries

3.1. Bilinear Mapping. Assume that (G, G^T) is a cyclic group of the same prime order p , g is the generator of G , and $\hat{e} : G \times G \rightarrow G^T$ is a bilinear map if the following properties are satisfied:

- (1) Bilinear: for all $x, y \in Z_p$, $\hat{e}(g^x, g^y) = \hat{e}(g, g)^{xy}$
- (2) Nondegeneracy: $\hat{e}(g, g) \neq 1_{G^T}$, the identity element is in G^T
- (3) Efficient computability: for all $x, y \in Z_p$, $\hat{e}(g^x, g^y)$ is efficient and computable

3.2. RMHT. Merkle Tree, also known as Merkle Hash Tree (MHT), is a classical data integrity verification structure, which can effectively verify whether an element has been tampered with [26]. When a Merkle tree is built on a data set S , the hash value of each element on S is taken as the leaf node of the tree, and each inner node is the hash value of its left and right children [27].

In Reference [9], an extended Hash Tree Rank-based Merkle Hash Tree (RMHT) was proposed, which is similar to MHT. The difference is that the input of an internal node is not only the left node and the right node but also the

Rank. The Rank refers to the number of leaves of the node, as shown in Figure 1. Nodes $h_1 - h_8$ have one leaf node, and their level is 1; $h_c, h_d, h_e,$ and h_f have two leaf nodes, and their level is 2, but root node h_r has eight leaves and its level is 8.

4. Data Migration Model and Authentication Framework

4.1. Data Migration Model. Provable data transfer model includes four entities: Data Owner (DO), Third Proxy Agent (TPA), and two clouds [9, 28]. The data migration model is shown in Figure 2. The clouds have a large amount of storage resources and strong computing power. The data owner, with limited resources, may be PC or smart mobile devices. They are generally limited in computation capability and restricted storage and energy and use the services provided by CSP [29]. TPA has capabilities that the data owner does not have, and it can initiate authentication requests on behalf of the data owner [30, 31].

In Figure 2, DO chooses cloud A to store the data, and cloud A is used to periodically detect the data integrity. If the user wants to change CSP, he or she first selects cloud B to store data and send data transfer request to cloud A. Cloud A sends the corresponding data to cloud B, and cloud B deletes the migrated data.

In order to ensure the data integrity of cloud B and the secure deletion of data on cloud A, the user sends a verification request to TPA, and TPA verifies whether the data on cloud B is integrity and the data on cloud A has been deleted. And then, TPA returns the verification results to the user. Finally, the user can still request TPA to continue periodically detect the remaining files on cloud A and new files stored on cloud B.

4.2. Cloud Data Migration Integrity Verification Framework. Based on reference [9], the design framework of this method extends PDP model supporting provable data transmission, including five stages: KeyGen, Store, Transfer, DeletCheck, and IntegCheck [30].

- (1) KeyGen: the probabilistic algorithm is run by DO to produce private key and public key, and public key is authenticated by Certification Authority (CA)
- (2) Store: It is an outsourced data generation algorithm. DO generates files and corresponding tags. The files are divided into several blocks, a random number of probe blocks are inserted into the files, and the owner generates a polynomial tag for each block. Then, DO builds the RMHT (rank-based Merkle Hash Tree) and signs the Root. RMHT is similar to Merkle Hash Tree. The difference is that the leaf nodes of RMHT are not only the connection value of the left and right nodes but also contain the level of the current node
- (3) Transfer: a secure data transmission algorithm is run by DO and clouds A and B. As DO transfer data from cloud A to cloud B, the data integrity on cloud

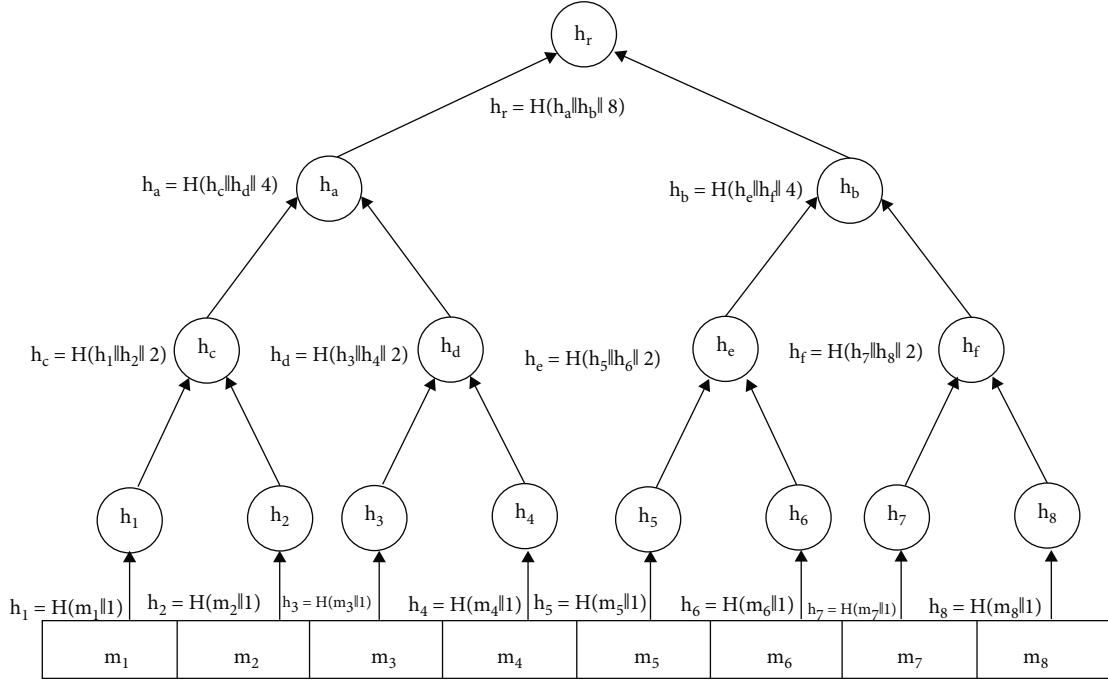


FIGURE 1: An example of RMHT.

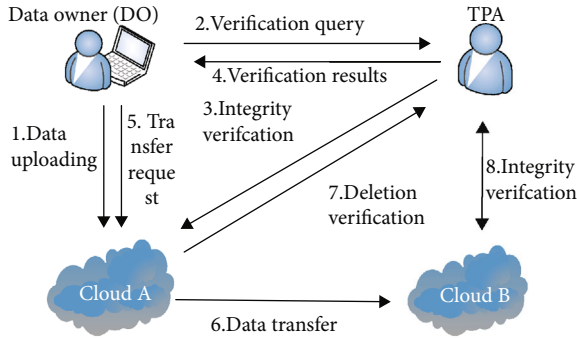


FIGURE 2: A provable data migration model.

A should be checked first. If the data is complete, DO send a data transfer request to cloud A, and then cloud A transmits the data to cloud B. When cloud B receives the data, it checks whether the data is integrated or not. Otherwise, DO requires cloud A to resend the data. DO uses integrity checking algorithms to ensure that the whole file transferred to cloud B is correct

- (4) DeletCheck: run by DO and clouds A and B. When data is successfully transferred to cloud B, Cloud A discards the migrated data. In order to ensure that cloud A executes the data deletion operation correctly and successfully deletes data, DO sends a query request to TPA, and TPA sends a challenge to cloud A to detect whether cloud A has successfully deleted data. After cloud A accepts the challenge, it computes a data deletion proof and sends it to TPA, which verifies the proof and returns the result

to DO. Based on results, DO knows whether the transmitted data was successfully discarded

(5) IntegCheck

It is a data integrity check algorithm, run by DO, TPA, and cloud, to check whether the data on the cloud is integrated. DO generates a validation query and sends it to the TPA, and TPA launch a challenge to cloud to check the integrity of the outsourced data. When accepting the challenge, the cloud computes the proof using the stored data and returns it to TPA, which checks validity of the proof and sends the test result back to DO.

In this framework, DO uses TPA to perform data ownership and data deletion verification, which implement public verification. DO also makes a verification without the help of TPA. Each data check is independent of TPA and DO.

The detailed steps of each stage are in reference [9]. Therefore, no detailed descriptions are given.

5. Hierarchical Data Authentication Mode

5.1. Basic Principle. When authenticating a large number of continuous files on the cloud, the common methods are to authenticate one by one or at random. Unfortunately, the former authentication overhead is too much, while the latter has high rate of missed detection. To solve this problem, a hierarchical verification mode (HVM) is proposed in this paper.

The basic idea of HVM is to select a number of files or data blocks for coarse-grained challenge response authentication and then to carry out fine-grained authentication in the adjacent area. The working process is as followed: firstly, the first layer authenticated data blocks are determined

according to the initial access granularity, and then the coarse-grained authentication at the first layer is carried out.

If the authentication is successful, the data blocks in the adjacent area are considered as being integrated, without the need of authentication. If the authentication fails, the adjacent data blocks will be authenticated at the second level with finer granularity. As the verification fails again, a third level of authentication is performed on adjacent blocks at finer granularity, and so on, until the minimum detection granularity is reached.

5.2. Detail Steps. For multiple files continuously stored on the cloud, the steps of HVM are as followed:

- (1) Set a detection flag bit A for each file on clouds, with an initial value of 0
- (2) The number of files to be authenticated on the cloud server is determined by TPA, and the initial detection granularity (i.e., the number of file intervals) X is determined
- (3) Divide all the files to be detected by X equally, and equal diversion point is the initial detection point
- (4) The agent challenges each file at the first level checkpoint on the server
- (5) The cloud server judge the flag bit of the file. If the flag bit is 1, the server will skip this detection. Otherwise, the cloud server sets the flag bit to be 1 and generates a response proof to this challenge, and sends the proof to agent
- (6) The agent verifies the proof sent by TPA. If the authentication is successful, go to step (10)
- (7) If the authentication fails, judge whether X is the minimum detection granularity. If so, execute step (10); otherwise, $X = X/2$
- (8) The agent challenges files separated by X before and after the file on cloud server
- (9) Execute step (5)
- (10) Verification is over

6. Hierarchical Provable Data Migration Method

In order to solve the problem of high verification overhead when massive files are migrated between clouds, HVM is applied to the integrity verification of cloud data migration. Combined HVM with the framework of integrity authentication of cloud data migration [9], a hierarchical provable data migration method is proposed, which includes two algorithms: H-Transfer (hierarchical provable data migration method) and H-IntegCheck (hierarchical provable integrity detection method).

The application scenario of this method is the data migration model in Figure 2. Data storage, verification, and migration are carried out on clouds A and B. The operation

objects are the batch files continuously stored on clouds A and B. To facilitate verification, DO sets the detection flag bit for each file (the initial value is 0, indicating that the file has not been authenticated) and then determines the initial detection granularity X and the minimum detection granularity X_{\min} .

6.1. H-IntegCheck Algorithm Description. The scenario of this algorithm is to verify the data integrity of massive files continuously stored on cloud A or cloud B, which is described as followed:

Let N be the number of files to be authenticated on clouds. Determine the first layer detection files with N and X and then execute the following operations for each file.

- (1) To verify the data integrity on cloud A or cloud B, TPA chooses a subset S and a random number $\theta \in Z_q^*$ for the current file from $[1, n]$, where n is the number of blocks in the current file. Then, TPA sends the challenge message $\text{chal} = \{S, \theta\}$ to cloud server
- (2) After receiving chal from TPA, the cloud first generates $\{p_i = \theta^i \bmod q\}, i \in S$. Then, the cloud server generates $y = f_{\vec{A}}(\theta)$, where $\vec{A} = \{0, 0, \sum_{i \in S} p_i m_{i,0}, \dots, \sum_{i \in S} p_i m_{i,s-1}\}$. The cloud server divides the polynomial $f_{\vec{A}}(x) - f_{\vec{A}}(\theta)$ by $x - \theta$, and the coefficients vector of the resulting polynomial is denoted by $\vec{\omega}$. $\vec{\omega} = (\omega_0, \omega_1, \dots, \omega_{s+1})$. The cloud server computes $\varphi = \prod_{j=2}^{s+1} (g^{a^j})^{\omega_j}$. Finally, the cloud obtains $\sigma = \prod_{i \in S} \sigma_i^{p_i}$ and sends the proof. $P = \{\sigma, \varphi, y, \text{sig}_{\text{ssk}}(H(R)), \{H(m_i \| 1), \Omega_i\}_{i \in S}\}$ to TPA, where $\{\Omega_i\}_{i \in S}$ is the auxiliary authentication information of block i
- (3) When TPA receives P from the cloud, it will judge whether the flag bit of the corresponding file is 0. If not, the authentication of the current file ends. Otherwise, TPA first generates R with $\{H(m_i \| 1), \Omega_i\}_{i \in S}$ and then authenticates the validity of R with $\text{sig}_{\text{ssk}}(H(R))$, and the corresponding mark position is 1. If the verification fails, TPA aborts and return false, then go to (4). Otherwise, TPA computes $u^{\sum_{i \in S} \{p_i H(\text{name})\}}$, and then TPA checks whether the following equation holds

$$e(\eta, \delta) \cdot e\left(\varphi, \gamma \cdot \delta^{-\theta}\right) \stackrel{?}{=} e(\sigma, g) \cdot e(\delta^{-y}, g). \quad (1)$$

If yes, it means that the data on cloud A or cloud B are integrated; otherwise, output *false*.

When $X/2$ is no less than X_{\min} , the $X/2^{\text{th}}$ file before this file and the $X/2^{\text{th}}$ file after this file are taken as the file in next hierarchy verification process, go to (1).

The process of integrity verification for H-IntegCheck is illustrated in Figure 3.

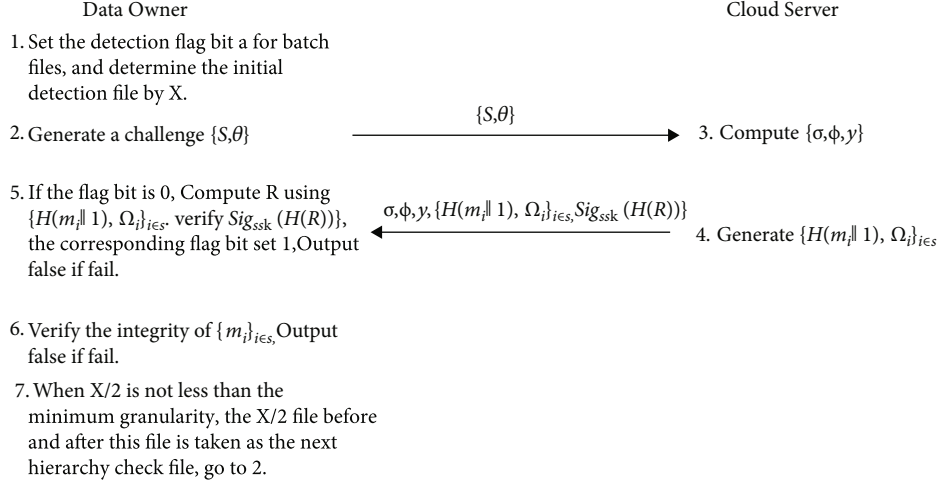


FIGURE 3: The working process of H-IntegCheck.

6.2. H-Transfer Algorithm Description. The scenario of this algorithm is to transfer massive files of continuous stored between cloud A and cloud B and to implement the secure transmission of provable data integrity. Details are illustrated as followed.

Determine the first layer detection files with N and X and then execute the following operations for each file.

- (1) When DO transfers part or all of the current file F from cloud A to cloud B, it first calls H-IntegCheck algorithm to check the data integrity on cloud A. If the file is corrupted, the user aborts check and returns *false*, then go to (5). Otherwise, DO retrieves τ from cloud A and verifies the signature using *spk*. If the signature is invalid, DO aborts check and output *false*, and go to (5). Otherwise, DO obtains the positions of sentinels PF by decrypts C with k
- (2) DO generates the block index Ψ to be transferred and computes the data migration request $Q = \text{fname} || \Psi || \text{sig}_{\text{ssk}}(\text{fname} || \Psi)$ and a tag, $\tau^* = \text{fname} || n^* || C^* || \text{Sig}_{\text{ssk}}(\text{fname} || n^* || C^*)$, where n^* is the number of the data blocks to be transferred, and C^* is the encryption of positions of the sentinels in the block to be transferred. And then DO sends (Q, τ^*) to cloud A
- (3) Cloud A verifies the signature $\text{Sig}_{\text{ssk}}(\text{fname} || \Psi)$ and returns *false* if the signature is invalid. Otherwise, cloud A sends (Q, τ^*, ϵ) to cloud B, with the data blocks $\{m_i\}_{i \in \Psi}$ the corresponding authentication tags $\{\sigma_i\}_{i \in \Psi}$ and $AAI\Omega^*$ of RMHT. $AAI\Omega^*$ is the sibling nodes on the path from the leaves to the root of MHT
- (4) When receiving the messages from cloud A, cloud B verifies the signatures $\text{Sig}_{\text{ssk}}(\text{fname} || \Psi)$ and $\text{Sig}_{\text{ssk}}(\text{fname} || n^* || C^*)$. If either is invalid, cloud B aborts check and returns *false*. Otherwise, cloud B go on to check each block tag σ_i , for $i \in \Psi$ as $e(u^{n^* H(\text{fname})} \prod_{j=0}^{s-1} (g^{\alpha^{j+2}})^{\sum_{i \in \Psi} m_{ij}}, \delta) = ? e(\prod_{i \in \Psi} \sigma_i, g)$.

If the equation does not hold, cloud B aborts check and returns *false*; otherwise, it utilizes the AAI Ω^* , and data blocks m_i , $i \in \Psi$, to reconstruct RMHT to obtain root R^*

- (5) Finally, cloud B verifies whether ϵ is the signature of R^* by using *spk*. If the verification fails, cloud B aborts check and returns *false*; otherwise, it stores $(\tau^*, \{m_i\}_{i \in \Psi}, \Omega^*, \epsilon)$ on its server and returns $(\text{fname}, \Omega^*, \epsilon)$ to DO to affirm the data transfer is successful. The data owner uses Ω^* to reconstruct RMHT to compute its root \hat{R} and checks if it is valid by verifying $\epsilon = ? \text{Sig}_{\text{ssk}}(\hat{R})$. TPA obtains root node h^* by $\{i, \Omega_i\}_{i \in \Psi}$ to reconstruct RMHT, and then TPA verifies $h^* = ? h_R^*$ to confirm if the data is deleted. If authentication fails, TPA outputs false and returns to DO
- (6) When $X/2$ is no less than X_{\min} , the $X/2^{\text{th}}$ file before this file and the $X/2^{\text{th}}$ file after this file are taken as the file in next hierarchy verification process and then go to (1). The integrity verification process of H-Transfer is shown in Figure 4

7. Security Analysis

7.1. Provable Data Possession and Provable Data Transfer Analysis. The proposed hierarchical provable data method includes H-IntegCheck and H-Transfer algorithms, which optimized algorithms IntegCheck and Transfer. The security design goals of H-IntegCheck are provable data possession. It ensures that a polynomial time adversary $Adve$ cannot successfully pass the verification with a forged proof, unless it can guess all the missing blocks. By using $\{H(m_i), \Omega_i\}_{i \in S}$ and $\text{sig}_{\text{ssk}} H(R)$ returned from cloud server, the user can authenticate the validity of R and auxiliary authentication information of m_i . If $\{\Omega_i\}_{i \in S}$ has changed, it cannot pass the signature verification. If the signature scheme is existentially unforgeable, then the $\{\Omega_i\}_{i \in S}$ and $\text{sig}_{\text{ssk}} H(R)$ are preserved completely. For the integrity of the blocks, the

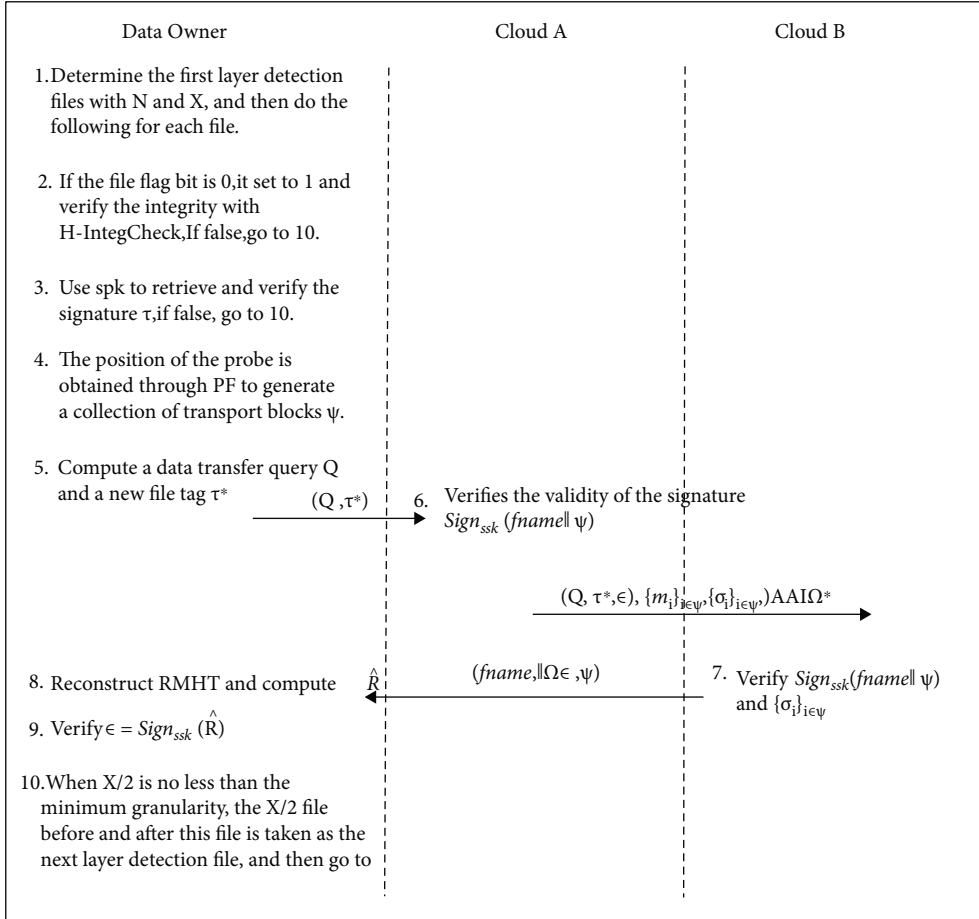


FIGURE 4: The working process of H-Transfer.

adversary cannot obtain a forged proof which can pass the verification in polynomial time.

The security design goals of H-Transfer is provable data transfer. It ensure the data can be transferred successfully. The user firstly checks the data integrity on cloud A before the transfer. If the file is corrupted, the user will investigate legal liability of cloud A. By verifying the signature in τ , user is convinced the ciphertext of table PF is intact. In order to ensure the data integrity during the data transfer, cloud B checks the integrity of each block by aggregatable verification of tags. If the integrity check is successful, then the data are transferred successfully to the cloud B. If only a part of data are received by cloud B, it will reject it and ask cloud A to retransmit the data. For the transfer request contains the user's signature, the adversary cannot forge it in polynomial time; hence, the data transfer operation is executed under the delegation of the user. After the data has been transferred completely, cloud B will send message to acknowledge the user the success of the data transfer. By utilizing the information returned from cloud B, the user checks the correctness of the root. If the verification is successful, the data transfer is successful.

7.2. Missing Report Rate Analysis. For $H\text{-IntegCheck}$ and $H\text{-Transfer}$ algorithms both select part of the files for

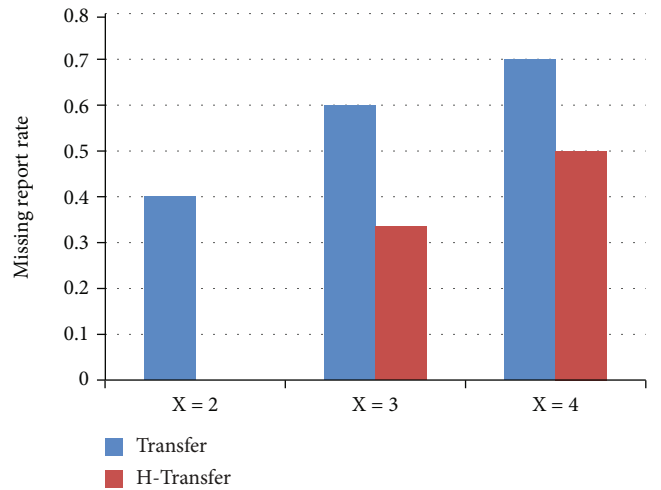


FIGURE 5: Missing report rate with correlation degree of 2.

verification, some corrupted files may not be detected, which may result in missing detection. The following is a brief analysis of the miss detection rate by taking $H\text{-transfer}$ algorithm as an example and Transfer algorithm as the comparison object.

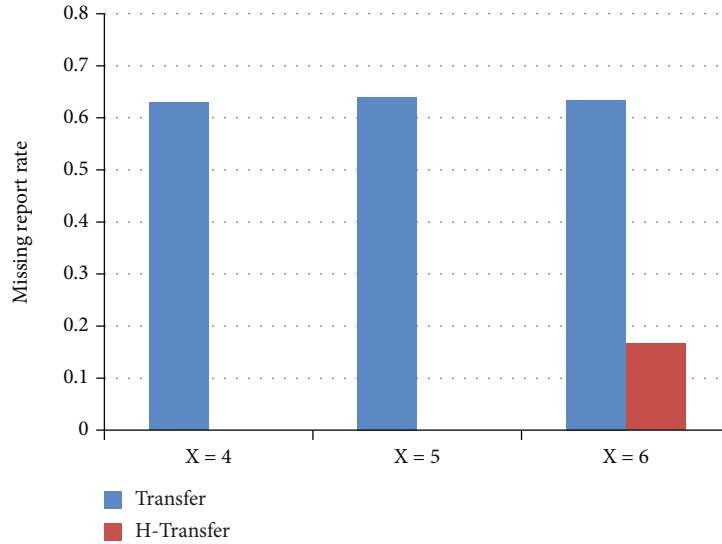


FIGURE 6: Missing report rate with correlation degree of 5.

To complete the analysis, Transfer and H-transfer algorithms are implemented based on PBC Library on Ubuntu14. There are 500 files to be verified, of which 10% files are corrupted. The correlation degrees are 2 and 5, respectively. The correlation degree means the number of files corrupted continuously:

7.2.1. Analysis of Missing Report Rate with a Correlation Degree of 2. The correlation degree is 2, and the missing report rate with the initial detection granularities of 2, 3, and 4 are shown in Figure 5. Compared with Transfer, the missing report rate of H-transfer is significantly decreased. When the initial detection granularity is 2, H-Transfer verifies all files at one interval, and all the error files with correlation degree 2 can be detected. Therefore, the missing report rate is 0. Transfer has a certain rate of missed detection (40%). When the initial detection granularity is 3 or 4, for the detection interval is greater than or equal to 2, there may be two consecutive false files missing detection, and so the missing report rate increase to 33.6% and 50%, respectively. However, the missing detection rate of H-Transfer is 33.6% and 50%, which is reduced by 44% and 28.6%, respectively, compared with Transfer.

7.2.2. Analysis of Missing Report Rate with a Correlation Degree of 5. The correlation degree is 5, and the missing report rate with the initial detection granularity of 4, 5, and 6 is shown in Figure 6. Compared with Transfer, the missing report rate of H-transfer is also significantly decreased. When the initial detection granularity is 4 or 5, H-Transfer verifies all files at intervals of 3 or 4. All the wrong files with a correlation of 5 can be detected; so, the missing report rate is 0. When the initial detection granularity is 6, 5 consecutive error files may be undetected. The missing report rate increases to 16.6%. However, compared with Transfer, its missing report rate is decreased by 73%. According to the above analysis, for H-transfer, when the initial detection granularity is less than or equal to the corre-

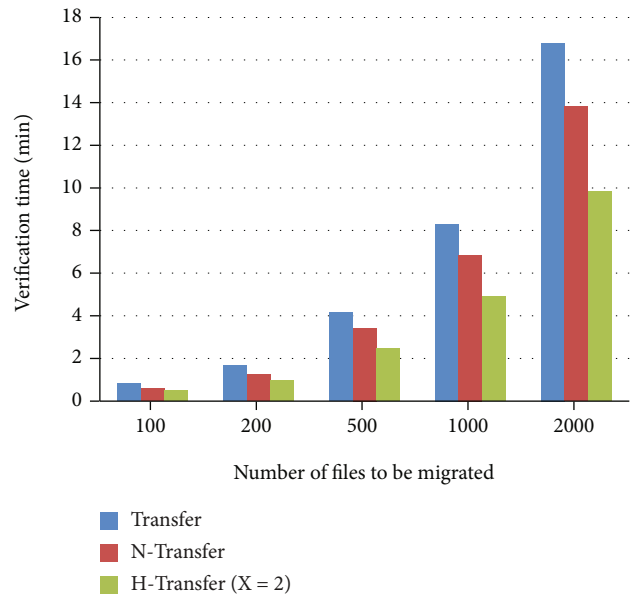


FIGURE 7: Verification time with different numbers of files to be migrated.

lation degree, missing report rate is the lowest, but more detection times are needed. When the initial detection granularity is greater than the correlation degree, there are fewer detection times, but higher missing report rate. In the case of same verification overhead, H-Transfer has a lower missing report rate than Transfer.

8. Performance Evaluation

The performance of the proposed method is evaluated below. The proposed method contains H-Transfer and H-IntegCheck processes. Because H-Transfer and H-IntegCheck work in a similar way, H-transfer is taken as an example to evaluate their performance. The comparison

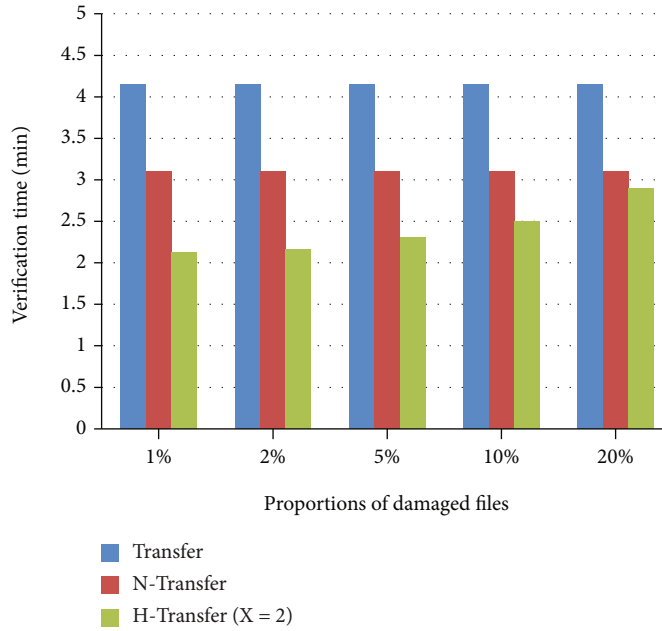


FIGURE 8: Verification time with different proportions of corrupted files.

object is Xue's [9] transfer (Transfer) process and Liu's [14] new transfer (N-Transfer) process with modular multiplication operation and modular exponentiation operation. The experiment is run on a PC with Intel i5 CPU and 4G memory. Transfer, N-Transfer, and H-transfer processes are implemented based on PBC library. The scenario is that cloud A migrates massive files to cloud B as shown in Figure 2, and the files are corrupted in a certain proportion. Transfer, N-Transfer, and H-transfer processes are used to verify the migration files, respectively, and the verification time is selected as the performance evaluation index:

8.1. Performance Evaluation with Different Numbers of Files to be Migrated. In this evaluation, cloud A transfers 100, 200, 500, 1000, and 2000 continuously files to cloud B, respectively. The proportions of corrupted files are 10%. For H-Transfer, both initial detection granularity X and correlation degree are 2. The performance evaluation results are shown in Figure 7. As shown in the figure, the verification time of N-Transfer decreased 21.3% in average than Transfer. For N-Transfer only uses modular multiplication and modular exponential operations, and the complex operations (such as bilinear mapping) do not use, so it is more efficient than Transfer. Moreover, the verification time of H-Transfer decreased 41.5% and 25.3% in average than Transfer and N-Transfer, respectively. For H-Transfer is to efficiently choose high probability of corrupted files for authentication, the overhead is lower than N-Transfer only with modular multiplication and modular exponential operations.

8.2. Performance Evaluation with Different Proportions of Corrupted Files. In this evaluation, the proportions of corrupted files are 1%, 5%, 10%, 15%, and 20%, respectively. Cloud A transfer 500 continuously files to cloud B. Similar

with evaluation (1), both initial detection granularity and correlation degree are 2. The performance evaluation results are shown in Figure 8. For Transfer and N-Transfer, all migrated files need to be authenticated, and the verify overhead is the authentication overhead of all migrated files. Therefore, changes in proportion of corrupted files have little impact on the authentication performance. For H-Transfer, the verification time is lower than Transfer and N-Transfer obviously. Moreover, the performance improvement slowly decreases as the proportion of corrupted files increases. Compare with Transfer and N-Transfer, the verification time of H-Transfer decreases by 48.7% and 31.3%, respectively, when the proportion is 1%, and the verification time decreases by 30% and 6.5%, respectively, when the proportion increases to 20%. The average verification time decrease by 42.2% and 22.6%, respectively. The reason is that with the increase of the proportion, the number of files verified by H-Transfer also gradually increases.

8.3. Performance Evaluation with Different Initial Detection Granularity. In this evaluation, the initial detection granularity X are 2, 3, 4, 5, and 6, respectively. Similar to evaluation (2), cloud A transfer 500 continuously files to cloud B, and the correlation degree is 2. The performance evaluation results are shown in Figure 9. As shown in the figure, the change of initial detection granularity has little impact on the authentication performance for Transfer and N-Transfer. For H-Transfer, the verification time is lower than Transfer and N-Transfer obviously. Moreover, the verification time decreases slowly as initial detection granularity increases. Compare with Transfer and N-Transfer, the verification time of H-Transfer decreases by 39.8% and 19.3% as X is 2 and decreases by 46.5% and 28.4% as X is 6. The average verification time is decrease by 43.9% and 24.9%. The reason is that with the initial detection granularity increases,

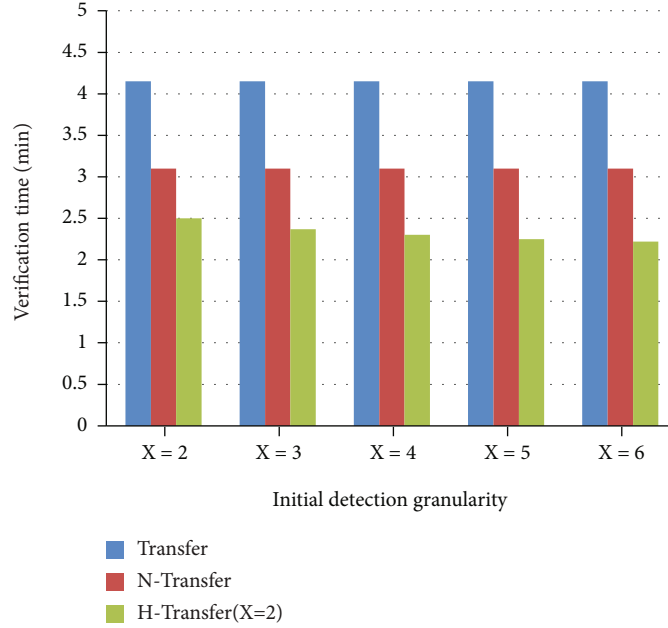


FIGURE 9: Verification time with different initial detection granularity.

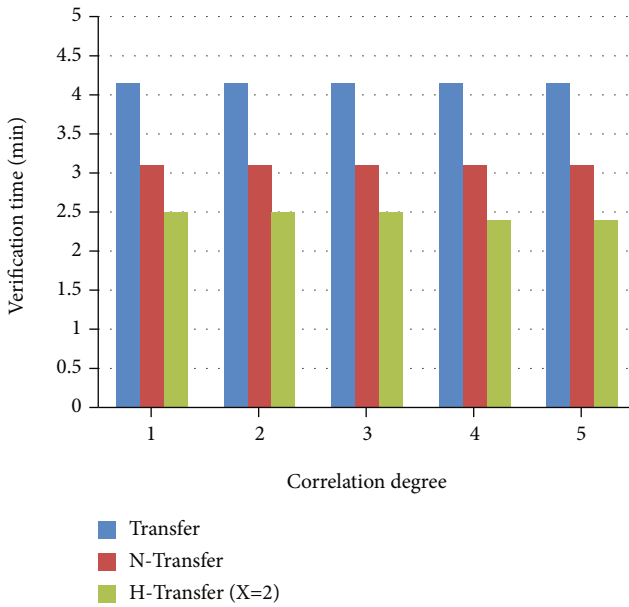


FIGURE 10: Verification time with different correlation degree.

the number of files verified of H-Transfer gradually decreases.

8.4. Performance Evaluation with Different Correlation Degrees. In this evaluation, the correlation degree is 1, 2, 3, and 5, respectively. Similar to evaluation (3), cloud A transfer 500 continuously files to cloud B, and the initial detection granularity is 2. The performance evaluation results are shown in Figure 10. As shown in the figure, the change of correlation degree has little impact on the authentication performance for Transfer and N-Transfer. For H-Transfer,

the verification time is lower than Transfer and N-Transfer obviously. Moreover, the verification time decreases very slowly as correlation degree increases. Compare with Transfer and N-Transfer, the verification time of H-Transfer decreases by 39.8% and 19.4% as correlation degree is 1 and decreases by 42.2% and 22.6% as correlation degree is 5. The average verification time is decrease by 40.7% and 20.6%. The reason is that with the correlation degree increases, the number of files verified of H-Transfer also slowly decreases.

9. Conclusions

This paper proposed a hierarchical verification mode and a hierarchical provable data migration method. The former is an optimized selection authentication mode, which can be combined with multiple data integrity authentication methods to improve the detection efficiency. The latter improves the transfer and integcheck algorithms of the reference [9]. The analysis and evaluations proved that the proposed method can effectively decreased the integrity authentication time of massive files migration between clouds. Therefore, this method can provide better authentication performance.

In the future work, the other algorithms in framework of integrity authentication of cloud data migration will be further optimized, and we will investigate migration security and performance of non-continuous massive files to reduce verification overhead for improving the performance of file migration while guaranteeing security.

Data Availability

Experimental data is randomly generated on simulation tools.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by Guangxi Natural Science Fund (No. 2018GXNSF AA138209), Science Research Start Fund of Shanghai University of Technology (No. 39120K196002-A06), and Science Research Start Fund of Guilin University of Technology (No. GUTQDJJ2017).

References

- [1] C. Wang, D. Wang, G. Xu, and D. He, *Efficient Privacy-Preserving User Authentication Scheme with Forward Secrecy for Industry 4.0*, SCIENCE CHINA: Information Sciences, 2020.
- [2] C. Wang, D. Wang, T. Yi, X. Guoai, and H. Wang, "Understanding node capture attacks in user authentication schemes for wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, 2020.
- [3] G. Ateniese, R. Burns, R. Curtmola et al., "Provable data possession at untrusted stores," in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 598–609, Alexandria, Virginia, 2007.
- [4] S. K. Nayak and S. Tripathy, "SEPDP: secure and efficient privacy preserving provable data possession in cloud storage," *IEEE Transactions on Services Computing*, vol. 1, 2018.
- [5] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. K. Liu, "Towards secure and reliable cloud storage against data re-outsourcing," *Future Generation Computer Systems*, vol. 52, no. 11, pp. 86–94, 2015.
- [6] Y. J. Ren, J. Shen, J. Wang, J. Han, and S. Y. Lee, "Mutual verifiable provable data auditing in public cloud storage," *Journal of Internet Technology*, vol. 16, no. 2, pp. 317–323, 2015.
- [7] A. Juels, S. Burton, and K. Jr, "PORs: Proofs of Retrievability for Large Files," *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS, 07)*, 2007, pp. 584–597, Alexandria, Virginia, USA, October 2007.
- [8] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," in *Proceeding (S) of ACM Workshop on Cloud Computing Security*, pp. 43–53, Chicago, USA, 2009.
- [9] L. Xue, J. Ni, Y. Li, and J. Shen, "Provable data transfer from provable data possession and deletion in cloud storage," *Computer Standards & Interfaces*, vol. 54, pp. 46–54, 2017.
- [10] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in *4th International Conference on Security and Privacy in Communication Networks*, pp. 1–10, Istanbul, Turkey, September 2008.
- [11] C. C. Erway, A. K p c , C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *In 16th ACM CCS*, pp. 213–222, Chicago, Illinois, USA, 2009.
- [12] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-Replica Provable Data Possession," in *The 28th International Conference on Distributed Computing Systems, 2008. ICDCS '08*, Beijing, China, June 2008.
- [13] M. Etemad and A. K p c , "Transparent, Distributed, and replicated dynamic provable data possession," in *Applied Cryptography and Network Security*, vol. 7954, pp. 1–18, Springer, Berlin Heidelberg, April, 2013.
- [14] Y. Liu, S. Xiao, H. Wang, and X. Wang, "New provable data transfer from provable data possession and deletion for secure cloud storage," *International Journal of Distributed Sensor Networks*, vol. 15, no. 5, 2019.
- [15] Y. Wang, X. Tao, J. Ni, and Y. Yu, "Data integrity checking with reliable data transfer for secure cloud storage," *International Journal of Web & Grid Services*, vol. 14, no. 1, p. 106, 2018.
- [16] H. Wang, D. He, A. Fu, Q. Li, and Q. Wang, "Provable data possession with outsourced data transfer," *IEEE Transactions on Services Computing*, pp. 1–1, 2019.
- [17] W. I. Khedr, H. M. Khater, and E. R. Mohamed, "Cryptographic accumulator-based scheme for critical data integrity verification in cloud storage," *IEEE Access*, vol. 7, no. 6, pp. 65635–65651, 2019.
- [18] R. Almarwani, N. Zhang, and J. Garside, "An effective, secure and efficient tagging method for integrity protection of outsourced data in a public cloud storage," *PLoS One*, vol. 15, 2020.
- [19] H. Shacham and B. Waters, "Compact Proofs of Retrievability," *Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'08)*, 2008pp. 90–107, Berlin, Melbourne, Australia, 2008.
- [20] C. Wang, Q. Wang, K. Ren, and W. Lou, *Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing* 29th IEEE INFOCOM, pp. 525–533, San Diego, CA, USA, March 2010.
- [21] Y. Yong, H. A. Man, and G. Ateniese, "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," *IEEE Transactions on Information Forensics & Security*, vol. 12, no. 4, pp. 767–778, 2017.
- [22] H. Huiying, Y. Jia, and Z. Hanlin, "Enabling secure auditing and deduplicating data without owner-relationship exposure in cloud storage," *Cluster Computing*, vol. 21, pp. 1849–1863, 2018.
- [23] X. Zhang, J. Zhao, C. Xu, H. Li, H. Wang, and Y. Zhang, "CIPPA: Conditional identity privacy preserving public auditing for cloud-based WBANs against malicious auditors," *IEEE transactions on cloud Computing*, vol. 9, 2019.
- [24] X. Zhang, C. Xu, H. Wang, Y. Zhang, and S. Wang, "FS-PEK-S: Lattice-based forward secure public-key encryption with keyword search for cloud-assisted industrial internet of things," *IEEE Transactions on Dependable and Secure Computing*, 2019.
- [25] S. Jegadeesan, M. Azees, N. Ramesh Babu, U. Subramaniam, and J. D. Almkhles, "EPAW: efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs)," *IEEE Access*, vol. 8, no. 3, pp. 48576–48586, 2020.
- [26] A. P. Mohan, A. R. Mohamed, and A. Gladston, "Merkle tree and Blockchain-based cloud data auditing," *International Journal of Cloud Applications and Computing (IJCAC)*, vol. 10, 2020.
- [27] Y. Yu, J. Ni, M. H. Au, H. Liu, H. Wang, and C. Xu, "Improved security of a dynamic remote data possession checking protocol for cloud storage," *Expert Systems with Applications*, vol. 41, no. 17, pp. 7789–7796, 2014.
- [28] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud

- Computing,” *Proceedings of the 14th European Symposium on Research in Computer Security (ESORICS'09)*, , pp. 355–370, Springer-Verlag, Berlin, 2009.
- [29] S. Qiu, D. Wang, X. Guoai, and S. Kumari, “Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for Mobile lightweight devices,” *IEEE Transactions on Dependable and Secure Computing*, 2020.
- [30] L. Chen, “Using algebraic signatures to check data possession in cloud storage,” *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1709–1715, 2013.
- [31] S. G. Worku, C. Xu, J. Zhao, and X. He, “Secure and efficient privacy-preserving public auditing scheme for cloud storage,” *Computers & Electrical Engineering*, vol. 40, no. 5, pp. 1703–1713, 2014.

Research Article

Simultaneous Jamming-and-Transmitting Scheme for Spectrum-Sharing Relaying Networks with Nonlinear Energy Scavenging

Triet Pham-Minh ¹, **Khuong Ho-Van** ^{2,3} and **Khanh Nghi-Vinh** ¹

¹Tra Vinh University, Vietnam

²Ho Chi Minh City University of Technology (HCMUT), 268 Ly Thuong Kiet Street, District 10, Ho Chi Minh City, Vietnam

³Vietnam National University Ho Chi Minh City, Linh Trung Ward, Thu Duc District, Ho Chi Minh City, Vietnam

Correspondence should be addressed to Khuong Ho-Van; hvkhuong@hcmut.edu.vn

Received 20 June 2021; Revised 22 September 2021; Accepted 6 October 2021; Published 19 October 2021

Academic Editor: Changqing Luo

Copyright © 2021 Triet Pham-Minh 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.

This paper recommends a simultaneous jamming-and-transmitting scheme for spectrum-sharing relaying networks with nonlinear energy scavenging. More specifically, spectrum-sharing relaying networks include a secondary source which expects to communicate with a secondary destination but impossible due to communication blockage between them, a secondary relay which helps the source overcome this blockage, a primary receiver, and a wiretapper which steals secret messages from both source and relay. To motivate assistance, the relay scavenges radio frequency energy from the source with practical nonlinear energy scavenger (NL-ES) instead of linear energy scavenger (L-ES) as in previous publications. Additionally, both source and relay perform simultaneous jamming-and-transmitting to secure their communication. The intercept and outage probabilities of the recommended scheme are evaluated through exact closed-form formulas, which are corroborated by Monte-Carlo simulations. Illustrative results show that the proposed scheme offers the reliability-security trade-off yet suffers error floor at large maximum transmit/interference power. Moreover, its performance can be optimally set with appropriate system parameters. Notably, the proposed scheme can guarantee absolute security with proper parameter setting. Furthermore, the NL-ES is practical but performs significantly worse than the L-ES.

1. Introduction

1.1. Background. Energy in radio frequency (RF) signals can be scavenged to power wireless users for improving energy efficiency, solving energy shortage, and offering green communication in advanced communication networks [1–4]. Two typical paradigms, expressly power-splitting (PS) and time-switching (TS), efficiently implement RF energy scavenging (ES) where the former performs ES and data restoring at the same time while the latter carries out these operations independently in distinct times [5]. As a result, the former demands lower circuitry implementation than the latter. Energy scavenger can be classified as linear (L) [6] or nonlinear (NL) [7]. Practically, circuit components of the energy scavenger include diodes and inductors. These NL components explicitly mean the NL-ES paradigm is more practical than the L-ES one. Therefore, this paper

focuses on a class of NL energy scavengers, namely, piecewise linearity in [7], to assess performance of RF ES systems.

Spectrum sharing (the literature names the spectrum-sharing operation mode differently as the underlay one; moreover, cognitive radios can operate in other two modes (interweave and overlay) which are beyond our scope) is the typical operation mode of cognitive radios aiming at improving significantly spectrum utilization efficiency [8]. This mode restricts transmit power of cognitive radios by the tolerable interference power at the primary users and their maximum transmit power [9, 10]. These power constraints limit their transmit power, shortening their coverage range and causing discontinuity in direct transmission between cognitive radios. Also, unfavorable propagation conditions (e.g., severe fading and heavy channel loss) are other causes to discontinuity in direct transmission. Consequently, a secondary relay, which can amplify-and-forward

(AF) or decode-and-forward (DF) secondary source signals to a secondary destination, should be utilized to ensure continuity in direct transmission. Nevertheless, the relay, which participates in relaying source signals as a volunteer, may be staggering to spend its personal energy for this operation. To raise the motivation for the relay, the energy scavenged from the source by recent advanced energy scavenging technologies should power its operation [11–13]. As such, the relay not only extends the coverage range of the secondary source but also keeps direct transmission continuous without sacrificing its personal energy. Nonetheless, the energy harvested by the relay is typically limited, and thus, the question is if the relay can assist direct transmission reliably as well as secure its transmission to the secondary destination against the overhearing of wiretappers. Another concern is that wiretappers also overhear communication through the source-relay hop and hence how to secure this hop. The current paper is aimed at solving these concerns. Before presenting the related works, it should be recalled that the jamming method, which produces intentionally jamming signals to interrupt solely the wiretappers, is popular and efficient in securing information transmission [14].

1.2. Related Works. Direct communication with the NL-ES in both cognitive and noncognitive radio networks has been extensively considered in [15–28]. In addition, a variety of publications investigated relaying networks with the NL-ES but for noncognitive users (e.g., [14, 29–36]) or non-spectrum-sharing users (e.g., overlay users [7, 37–40]). Nonetheless, few works studied performance analysis for spectrum-sharing relaying networks with nonlinear energy scavenging (SSRNwNLES). Specifically, Ref. [41] considered the basic system model for SSRNwNLES where a secondary DF relay aids direct secondary source-destination transmission. Secondary communication interferes signal reception of a primary receiver. Nevertheless, Ref. [41] assumed an eavesdropper wiretaps legitimate information over solely the second hop (from the relay to the destination). Moreover, Ref. [41] only simulated the secrecy outage probability under the maximum transmit power constraint (MTPC) and the interference power restriction (IPR) without proposing any technique to protect legitimate information over both (source-relay and relay-destination) hops. In [42], the authors reconsidered the system model in [41] for maximizing the throughput but without the eavesdropper. The authors in [43] considered SSRNwNLES with several secondary relays and primary users. Although [43] presented the bit error rate analysis, the spectrum-sharing mode imposes implicit constraints on the operations of the cognitive radios without explicitly investigating the IPR and the MTPC, simplifying significantly the analysis. Moreover, Ref. [43] did not study the security aspect of the considered system model. In [44], the authors studied SSRNwNLES with several secondary relays and destinations. However, only relays are constrained by both maximum transmit and interference powers while the source is imposed by the interference power restriction. Furthermore, Refs. [42, 44] were not interested in performance analysis and security issue.

1.3. Contributions. The above literature survey indicates that concurrent considerations of performance analysis and security issue in SSRNwNLES have been still an open topic so far. This paper is the first attempt to research that topic with the following contributions:

- (i) Propose a simultaneous jamming-and-transmitting scheme to secure message transmission over both source-relay and relay-destination hops in the system model in [41] by asking both the relay and the source to broadcast simultaneously legitimate and jamming signals. Apparently, the proposed scheme solved the security issue left by previous works [41–44]
- (ii) Recommend the relay to scavenge energy in source signals with the nonlinear energy scavenger to increase its motivation in relaying source messages
- (iii) Propose precise formulas of intercept probability (IP) and outage probability (OP) for evaluating rapidly both security and reliability of the recommended scheme without invoking exhaustive Monte-Carlo simulations. The derivation of the OP and the IP accounts for both the MTPC and the IPR. These analyses were obviously ignored in [41–44]
- (iv) Optimize crucial system parameters using the recommended IP/OP expressions
- (v) Prove the absolute security achievable with proper system parameter setting
- (vi) Illustrate multifarious results of the reliability and security performances to make helpful conclusions; for instance, the unchanged IP/OP as either the MTPC or the IPR is forsaken, considerable security/reliability improvement as setting properly system parameters, the reliability-security trade-off, and the inferiority of the NL-ES to the L-ES

1.4. Organization. The next section describes the recommended simultaneous jamming-and-transmitting scheme for SSRNwNLES. Then, Section 3 details the derivation of the accurate closed-form IP/OP expressions. Next, Section 4 illustrates analytical/simulated results on the recommended scheme. Eventually, Section 5 ends the paper with insightful comments.

2. Simultaneous Jamming-and-Transmitting Scheme

Figure 1 sketches the system model under consideration where the secondary destination D expects to get signals from the secondary source S . The eavesdropper E tries to extract the source message. Because of bad propagation conditions such as dire fading and severe channel loss, direct $S \rightarrow D$ transmission may be discontinuous. Therefore, the DF relay R between S and D should be utilized to relay S 's signal to D for keeping the $S \rightarrow D$ transmission continuous.

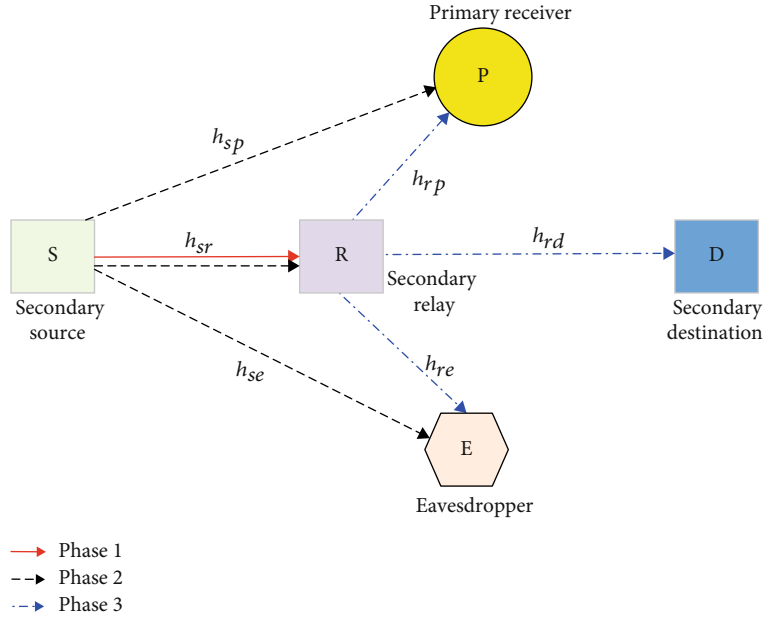


FIGURE 1: System model.

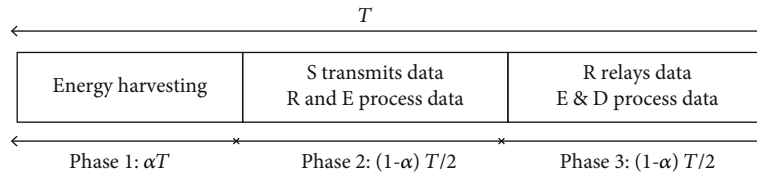


FIGURE 2: Phase times.

To reward for R 's assistance, R only relays the source message with the energy scavenged in the source signals. Accordingly, secret messages reach D in three phases with a total duration of T as shown in Figure 2. Also, due to the spectrum-sharing operation mode, cognitive radios (S and R) interfere (in the spectrum-sharing operation mode, primary users interfere cognitive radios; nonetheless, such an interference is forsaken under scenarios that it follows the Gaussian distribution or the distance between the primary user and the cognitive radio is adequately large; forsaking such an interference is admitted extensively in the literature of the spectrum-sharing networks (please refer to [45–47])) the primary receiver P .

Figure 1 notates channel gain h_{bc} , $b \in \{S, R\}$, $c \in \{E, R, D, P\}$. This paper considers all independent flat block Rayleigh fading channels, and hence, h_{bc} is represented by a zero-mean θ_{bc} -variance complex Gaussian random variable, namely, $h_{bc} \sim \mathcal{CN}(0, \theta_{bc})$, and is unchanged during T but changes independently in the next T . Additionally, state information of all channels is assumed to be perfectly (channel state information (CSI) may be imperfectly estimated [48–50]; we reserve the case of imperfect CSI in our future works; instead, we focus on proposing a solution to secure SSRNwNLES in both transmission phases and analyze its

intercept/outage performance in this paper) acquired, for example, through pilot estimation [51]. Furthermore, the path loss can be considered in θ_{bc} as $\theta_{bc} = d_{bc}^{-\delta}$ where d_{bc} and δ notate the $b \rightarrow c$ distance and the path-loss exponent, correspondingly. The following notates the channel power gain as $g_{bc} = |h_{bc}|^2$ whose pdf (probability density function) and cdf (cumulative distribution function) are addressed, respectively, as

$$\begin{aligned} f_{g_{bc}}(x) &= \frac{1}{\theta_{bc}} e^{-(x/\theta_{bc})} \Phi(x), \\ F_{g_{bc}}(x) &= \left(1 - e^{-(x/\theta_{bc})}\right) \Phi(x), \end{aligned} \quad (1)$$

where $\Phi(x)$ is the unit step function.

We notate P_s as the secondary source's transmit power. Then, the spectrum-sharing operation mode regulates P_s such that S interferes P with the amount of the interference power $P_s g_{sp}$ below the tolerable interference threshold I_t of P , i.e., $P_s g_{sp} \leq I_t$. Also, P_s is restricted by the maximum transmit power \tilde{P}_s according to hardware specification, i.e.,

$P_s \leq \check{P}_s$. Consequently, combining these power constraints regulates P_s as

$$P_s = \min \left(\frac{I_t}{g_{sp}}, \check{P}_s \right). \quad (2)$$

In (2), the equality is set for maximizing the cognitive radios' transmission range [52].

In Phase 1 with a duration of αT , the nonlinear energy harvester at R generates the following power [7].

$$\check{P}_r = \begin{cases} LP_s g_{sr} & , P_s g_{sr} \leq \rho, \\ L\rho & , P_s g_{sr} > \rho, \end{cases} \quad (3)$$

where $L = 2\psi\alpha/(1-\alpha)$ with $\psi \in (0, 1)$ being the energy converting efficiency and $\alpha \in (0, 1)$ being a time fraction; ρ is the power saturation threshold.

Different from the conventional direct communication scheme where S sends only its data to D in Phase 2, our scheme allows S to use a fraction of its power $(1-\beta)P_s$ to send its message x_s and the remaining power βP_s to broadcast jamming signal x_a in order to protect its data against the eavesdropper. Here, $\beta \in (0, 1)$ stands for the power distribution coefficient for the legitimate message and the jamming signal at S . As such, the signal transmitted by S can be expressed as $u_s = \sqrt{(1-\beta)P_s}x_s + \sqrt{\beta P_s}x_a$ and the received signals at R and E are uniquely expressed to be

$$y_m = h_{sm} \left(\sqrt{(1-\beta)P_s}x_s + \sqrt{\beta P_s}x_a \right) + \varepsilon_m, \quad (4)$$

where the additive noise at the receiver $m \in \{r, e\}$ is denoted as $\varepsilon_m \sim \mathcal{CN}(0, \varepsilon_m)$.

The a priori characteristic of the jamming signal is assumably known at R ; for example, x_a can be a pseudorandom signal whose seed is shared with R [14]. As such, the jamming signal merely interrupts the eavesdropper and can be definitely abolished from the received signal of R . After annihilating the jamming signal, R further processes the following signal for decoding x_s :

$$\tilde{y}_r = h_{sr} \sqrt{(1-\beta)P_s}x_s + \varepsilon_r. \quad (5)$$

R obtains the signal-to-noise ratio (SNR) from (5) for recovering x_s to be

$$\Gamma_{sr} = \frac{g_{sr}P_s(1-\beta)}{\varepsilon_r}. \quad (6)$$

Generating x_a is merely shared between S and R but E is blind with it. Accordingly, the signal-to-noise plus interference ratio (SNIR) which E can obtain for recovering x_s in Phase 2 is deduced from (4) to be

$$\Gamma_{se} = \frac{g_{se}P_s(1-\beta)}{g_{se}P_s\beta + \varepsilon_e}. \quad (7)$$

In Phase 3 with a duration of $(1-\alpha)T/2$, R broadcasts the restored signal \hat{x}_s as well as the jamming signal \hat{x}_a to secure \hat{x}_s against the eavesdropper. Consequently, the signals received at E and D have the same form as

$$y_w = h_{rw} \left(\sqrt{(1-\lambda)P_r}\hat{x}_s + \sqrt{\lambda P_r}\hat{x}_a \right) + \varepsilon_w, \quad (8)$$

where the receive antenna of $w \in \{d, e\}$ causes the additive noise $\varepsilon_w \sim \mathcal{CN}(0, \varepsilon_w)$; $\lambda \in (0, 1)$ stands for the power distribution factor for the restored signal and the jamming signal at R ; P_r is the transmit power of R . For the spectrum-sharing operation mode, P_r is constrained as

$$P_r = \min \left(\check{P}_r, \frac{I_t}{g_{rp}} \right). \quad (9)$$

Thanks to the property of the jamming signal \hat{x}_a and processing it similarly to Phase 2, the SNR at D and the SNIR at E in Phase 3 are correspondingly given by

$$\Gamma_{rd} = \frac{g_{rd}P_r(1-\lambda)}{\varepsilon_d}, \quad (10)$$

$$\Gamma_{re} = \frac{g_{re}P_r(1-\lambda)}{g_{re}P_r\lambda + \varepsilon_e}. \quad (11)$$

It is seen from the denominators of (7) and (11) that E suffers the amount of jamming power in both last phases. This amount mitigates the probability of recovering precisely x_s at E , eventually improving the message security.

The DF operation of R results in the aggregated SNIR at D for recovering x_s as

$$\Gamma_d = \min(\Gamma_{sr}, \Gamma_{rd}). \quad (12)$$

In order for E to improve its intercept capability, it needs to combine its received signals in Phase 2 and Phase 3. We assume E prefers affordable complexity. Then, it can employ the signal selection combining method (other combining

methods which E can employ are maximum ratio combining and equal gain combining [53]; nonetheless, although these methods offer better performance, they require higher implementation complexity), which produces the entire SNIR to be

$$\Gamma_e = \max(\Gamma_{se}, \Gamma_{re}). \quad (13)$$

The channel capacity which $w \in \{d, e\}$ acquires to recover x_s is represented to be

$$\mathcal{R}_w = \frac{1-\alpha}{2} \log_2(1 + \Gamma_w). \quad (14)$$

3. Security and Reliability Analyses

Communication reliability and message security can be measured through the OP at D and the IP at E , respectively. These probability expressions of the proposed simultaneous jamming-and-transmitting scheme for SSRNwNLES are derived to quickly evaluate both reliability and security without exhaustive simulations.

3.1. Intercept Probability. The intercept event occurs when the channel capacity of E surpasses the target spectral efficiency $\tilde{\mathcal{R}}_e$. Consequently, the IP is expressed to be

$$\Psi = \Pr \left\{ \mathcal{R}_e \geq \tilde{\mathcal{R}}_e \right\} = \Pr \left\{ \Gamma_e \geq \tilde{\Gamma}_e \right\}, \quad (15)$$

where $\tilde{\Gamma}_e = 2^{2\tilde{\mathcal{R}}_e/(1-\alpha)} - 1$.

Inserting (13) into (15) yields

$$\begin{aligned} \Psi &= \Pr \left\{ \max(\Gamma_{se}, \Gamma_{re}) \geq \tilde{\Gamma}_e \right\} \\ &= 1 - \Pr \left\{ \max(\Gamma_{se}, \Gamma_{re}) < \tilde{\Gamma}_e \right\} \\ &= 1 - \mathcal{E}_{P_s} \left\{ \underbrace{\Pr \left\{ \Gamma_{se} < \tilde{\Gamma}_e \middle| P_s \right\}}_{\Psi_1} \underbrace{\Pr \left\{ \Gamma_{re} < \tilde{\Gamma}_e \middle| P_s \right\}}_{\Psi_2} \right\}, \end{aligned} \quad (16)$$

where $\mathcal{E}\{\cdot\}$ is the expectation operator.

Plugging (7) into Ψ_1 in (16) results in

$$\begin{aligned} \Psi_1 &= \Pr \left\{ \frac{g_{se} P_s (1-\beta)}{g_{se} P_s \beta + \varepsilon_e} < \tilde{\Gamma}_e \middle| P_s \right\} \\ &= \Pr \left\{ g_{se} P_s (1-\beta - \tilde{\Gamma}_e \beta) < \tilde{\Gamma}_e \varepsilon_e \middle| P_s \right\} \\ &= \begin{cases} \bar{\Psi}_1, & \tilde{\Gamma}_e < \frac{(1-\beta)}{\beta}, \\ 1, & \tilde{\Gamma}_e \geq \frac{(1-\beta)}{\beta}, \end{cases} \end{aligned} \quad (17)$$

where

$$\bar{\Psi}_1 = \Pr \left\{ g_{se} < \frac{\tilde{\Gamma}_e \varepsilon_e}{P_s (1-\beta - \tilde{\Gamma}_e \beta)} \middle| P_s \right\} = 1 - e^{-(N/P_s)}, \quad (18)$$

with $N = \tilde{\Gamma}_e \varepsilon_e / (1-\beta - \tilde{\Gamma}_e \beta) \theta_{se}$.

Since $\tilde{\Gamma}_e = 2^{2\tilde{\mathcal{R}}_e/(1-\alpha)} - 1$, (17) shows that the eavesdropping of E in Phase 2 can be completely eliminated by splitting appropriately times for energy harvesting and signal transmission (i.e., selecting α), allocating properly S 's power to the jamming signal (i.e., selecting β), and setting reasonably the target spectral efficiency $\tilde{\mathcal{R}}_e$ such that the inequality $\tilde{\Gamma}_e \geq (1-\beta)/\beta$ holds.

Inserting (11) into Ψ_2 in (16) yields

$$\begin{aligned} \Psi_2 &= \Pr \left\{ \frac{g_{re} P_r (1-\lambda)}{g_{re} P_r \lambda + \varepsilon_e} < \tilde{\Gamma}_e \middle| P_s \right\} \\ &= \Pr \left\{ g_{re} P_r (1-\lambda - \lambda \tilde{\Gamma}_e) < \tilde{\Gamma}_e \varepsilon_e \middle| P_s \right\} \\ &= \begin{cases} \bar{\Psi}_2, & \tilde{\Gamma}_e < \frac{(1-\lambda)}{\lambda}, \\ 1, & \tilde{\Gamma}_e \geq \frac{(1-\lambda)}{\lambda}, \end{cases} \end{aligned} \quad (19)$$

where

$$\begin{aligned} \bar{\Psi}_2 &= \Pr \left\{ g_{re} < \frac{\tilde{\Gamma}_e \varepsilon_e}{P_r (1-\lambda - \lambda \tilde{\Gamma}_e)} \middle| P_s \right\} \\ &= \mathcal{E}_{P_r} \left\{ \Pr \left\{ g_{re} < \frac{\tilde{\Gamma}_e \varepsilon_e}{P_r (1-\lambda - \lambda \tilde{\Gamma}_e)} \middle| P_r, P_s \right\} \right\} \\ &= \mathcal{E}_{P_r} \left\{ 1 - e^{-\left(\tilde{\Gamma}_e \varepsilon_e / (P_r (1-\lambda - \lambda \tilde{\Gamma}_e)) \right) \theta_{re}} \middle| P_s \right\}. \end{aligned} \quad (20)$$

Because $\tilde{\Gamma}_e = 2^{2\tilde{\mathcal{R}}_e/(1-\alpha)} - 1$, (19) indicates that the eavesdropping of E in Phase 3 can be completely eliminated by splitting appropriately times for energy harvesting and signal transmission (i.e., selecting α), allocating properly R 's power

to the jamming signal (i.e., selecting λ), and setting reasonably the target spectral efficiency $\tilde{\mathcal{R}}_e$ such that the inequality $\tilde{\Gamma}_e \geq (1-\lambda)/\lambda$ holds.

Given P_r in (9), (20) is further simplified as

$$\begin{aligned}\bar{\Psi}_2 &= \mathcal{E}_{g_{sr}, g_{rp}} \left\{ 1 - e^{-\left(\tilde{\Gamma}_e \varepsilon_e / (\min(\check{P}_r, I_t / g_{rp})) (1 - \lambda - \tilde{\lambda} \tilde{\Gamma}_e) \theta_{re}\right)} \right\} \Big| P_s \\ &= \mathcal{E}_{g_{sr}} \left\{ 1 - \int_0^{I_t / \check{P}_r} e^{-\left(\tilde{\Gamma}_e \varepsilon_e / (\check{P}_r (1 - \lambda - \tilde{\lambda} \tilde{\Gamma}_e) \theta_{re})\right)} \frac{e^{-x/\theta_{rp}}}{\theta_{rp}} dx \right. \\ &\quad \left. - \int_{I_t / \check{P}_r}^{\infty} e^{-\left(\tilde{\Gamma}_e \varepsilon_e / (I_t (1 - \lambda - \tilde{\lambda} \tilde{\Gamma}_e) \theta_{re}/x)\right)} \frac{e^{-x/\theta_{rp}}}{\theta_{rp}} dx \right\} \Big| P_s \\ &= \mathcal{E}_{g_{sr}} \left\{ \underbrace{1 - e^{-(Q/\check{P}_r)} + H e^{-(Q/\check{P}_r, H)}}_A \right\} \Big| P_s, \end{aligned} \quad (21)$$

where $Q = \tilde{\Gamma}_e \varepsilon_e / (1 - \lambda - \tilde{\lambda} \tilde{\Gamma}_e) \theta_{re}$ and $H = \theta_{rp} Q / (I_t + \theta_{rp} Q)$.

Based on (3), two cases of \check{P}_r are considered when deriving (21) as follows.

Case 1. ($\check{P}_r = L\rho$).

This case holds when $g_{sr} > \rho/P_s$. By averaging \mathcal{A} in (21) over this region, one obtains $\bar{\Psi}_2$ for this case as

$$\bar{\Psi}_{21} = \int_0^{\rho/P_s} \left(1 - e^{-(Q/A\rho)} + H e^{-(Q/AH\rho)} \right) \frac{e^{-x/\theta_{sr}}}{\theta_{sr}} dx = M e^{-(\rho/\theta_{sr} P_s)}, \quad (22)$$

where $M = 1 - e^{-(Q/A\rho)} + H e^{-(Q/AH\rho)}$.

Case 2. ($\check{P}_r = LP_s g_{sr}$).

This case holds when $g_{sr} \leq \rho/P_s$. By averaging \mathcal{A} in (21) over $g_{sr} \leq \rho/P_s$, one obtains $\bar{\Psi}_2$ for this case as

$$\begin{aligned}\bar{\Psi}_{22} &= \int_0^{\rho/P_s} \left(1 - e^{-(Q/LP_s, x)} + H e^{-(Q/LHP_s, x)} \right) \frac{e^{-x/\theta_{sr}}}{\theta_{sr}} dx \\ &= 1 - e^{-(\rho/P_s, \theta_{sr})} + \frac{1}{\theta_{sr}} \int_0^{\rho/P_s} e^{-(x/\theta_{sr})} \left(H e^{-(Q/LHP_s, x)} - e^{-(Q/LP_s, x)} \right) dx. \end{aligned} \quad (23)$$

Using the series expansion for $e^{-x/\theta_{sr}}$, one rewrites (23) as

$$\begin{aligned}\bar{\Psi}_{22} &= 1 - e^{-(\rho/P_s, \theta_{sr})} + \frac{1}{\theta_{sr}} \int_0^{\rho/P_s} \left[\sum_{k=0}^{\infty} \frac{1}{k!} \left(-\frac{x}{\theta_{sr}} \right)^k \right] \\ &\quad \cdot \left(H e^{-(Q/LHP_s, x)} - e^{-(Q/LP_s, x)} \right) dx. \end{aligned} \quad (24)$$

Performing the variable change $t = 1/x$, one reduces (24) to

$$\begin{aligned}\bar{\Psi}_{22} &= 1 - e^{-(\rho/P_s, \theta_{sr})} + \frac{1}{\theta_{sr}} \sum_{k=0}^{\infty} \frac{(-\theta_{sr})^{-k}}{k!} \int_{\frac{P_s}{\rho}}^{\infty} t^{-k-2} \\ &\quad \cdot \left(H e^{-(Qt/LHP_s)} - e^{-(Qt/LP_s)} \right) dt \\ &= 1 - e^{-(\rho/P_s, \theta_{sr})} + \sum_{k=0}^{\infty} \frac{J}{P_s^{k+1}}, \end{aligned} \quad (25)$$

where $J = (((Q/[\theta_{sr} L])^{k+1}) / (k!(k+1)!)) [\sum_{m=1}^{k+1} (-L\rho/Q)^m (m-1)! \{e^{-(Q/L\rho)} + (-1)^{m+1} H^{m-k} e^{-(Q/LH\rho)}\} - \text{Ei}(-Q/L\rho) + H^{-k} \text{Ei}(-Q/LH\rho)]$ with $\text{Ei}(\cdot)$ being the exponential integral.

The total probability law simplifies (21) as

$$\bar{\Psi}_2 = \bar{\Psi}_{21} + \bar{\Psi}_{22} = 1 + (M-1)e^{-(\rho/P_s, \theta_{sr})} + \sum_{k=0}^{\infty} \frac{J}{P_s^{k+1}}. \quad (26)$$

Inserting (18) into (17) and (26) into (19), one obtains Ψ_1 and Ψ_2 as

$$\Psi_1 = \begin{cases} 1 - e^{-(N/P_s)}, & \tilde{\Gamma}_e < \frac{(1-\beta)}{\beta}, \\ 1, & \tilde{\Gamma}_e \geq \frac{(1-\beta)}{\beta}, \end{cases} \quad (27)$$

$$\Psi_2 = \begin{cases} 1 + (M-1)e^{-(\rho/\theta_{sr} P_s)} + \sum_{k=0}^{\infty} \frac{J}{P_s^{k+1}}, & \tilde{\Gamma}_e < \frac{(1-\lambda)}{\lambda}, \\ 1, & \tilde{\Gamma}_e \geq \frac{(1-\lambda)}{\lambda}. \end{cases} \quad (28)$$

Plugging (27) and (28) into (16), one obtains

$$\Psi = \begin{cases} \check{\Psi}_1, & \tilde{\Gamma}_e \geq \max\left(\frac{[1-\beta]}{\beta}, \frac{[1-\lambda]}{\lambda}\right), \\ \check{\Psi}_2, & \frac{(1-\beta)}{\beta} \leq \tilde{\Gamma}_e < \frac{(1-\lambda)}{\lambda}, \\ \check{\Psi}_3, & \frac{(1-\lambda)}{\lambda} \leq \tilde{\Gamma}_e < \frac{(1-\beta)}{\beta}, \\ \check{\Psi}_4, & \tilde{\Gamma}_e < \min\left(\frac{[1-\beta]}{\beta}, \frac{[1-\lambda]}{\lambda}\right). \end{cases} \quad (29)$$

Since $\tilde{\Gamma}_e = 2^{2\tilde{\mathcal{R}}_e/(1-\alpha)} - 1$, it is indicated from (29) that the security of the proposed simultaneous jamming-and-

transmitting scheme experiences four different levels dependent on adjusting the system parameters ($\tilde{\mathcal{R}}_e, \alpha, \beta, \lambda$).

The following sequentially computes $\check{\Psi}_1, \check{\Psi}_2, \check{\Psi}_3$, and $\check{\Psi}_4$ to numerically evaluate (29). First, we start with $\check{\Psi}_1$. It is straightforward to infer that

$$\check{\Psi}_1 = 0. \quad (30)$$

Because $\tilde{\Gamma}_e = 2^{2\tilde{\mathcal{R}}_e/(1-\alpha)} - 1$, (30) indicates that the eavesdropping of E can be completely eliminated in the proposed simultaneous jamming-and-transmitting scheme where both legitimate messages (of S and R) are protected in Phase 2 and Phase 3 by splitting appropriately times for energy harvesting and signal transmission (i.e., selecting α), distributing reasonably S 's power to the jamming signal (i.e., selecting β), allocating properly R 's power to the jamming signal (i.e., selecting λ), and setting the target spectral efficiency $\tilde{\mathcal{R}}_e$ such that the inequality, $\tilde{\Gamma}_e \geq \max([1-\beta]/\beta, [1-\lambda]/\lambda)$, holds.

Second, $\check{\Psi}_2$ is written explicitly as

$$\check{\Psi}_2 = 1 - \mathcal{E}_{P_s} \left\{ 1 + (M-1)e^{-(\rho/\theta_{sr}P_s)} + \sum_{k=0}^{\infty} \frac{J}{P_s^{k+1}} \right\}. \quad (31)$$

Given P_s in (2), one solves (31) in closed form as

$$\begin{aligned} \check{\Psi}_2 &= - \int_0^{I_t/\tilde{P}_s} \left((M-1)e^{-(\rho/\theta_{sr}\tilde{P}_s)} + \sum_{k=0}^{\infty} \frac{J}{\tilde{P}_s^{k+1}} \right) \frac{e^{-x/\theta_{sp}}}{\theta_{sp}} dx \\ &\quad - \int_{I_t/\tilde{P}_s}^{\infty} \left((M-1)e^{-(\rho x/\theta_{sr}I_t)} + \sum_{k=0}^{\infty} \left(\frac{x}{I_t} \right)^{k+1} J \right) \frac{e^{-x/\theta_{sp}}}{\theta_{sp}} dx \\ &= - \left((M-1)e^{-(\rho/\theta_{sr}\tilde{P}_s)} + \sum_{k=0}^{\infty} \frac{J}{\tilde{P}_s^{k+1}} \right) \left(1 - e^{-(I_t/\theta_{sp}\tilde{P}_s)} \right) \\ &\quad - \frac{M-1}{\theta_{sp}} \left(\frac{\rho}{\theta_{sr}I_t} + \frac{1}{\theta_{sp}} \right)^{-1} e^{-((\rho/\theta_{sr}I_t)+1/\theta_{sp})I_t/\tilde{P}_s} \\ &\quad - e^{-(I_t/\tilde{P}_s\theta_{sp})} \sum_{k=0}^{\infty} \sum_{n=0}^{k+1} \frac{(k+1)! \theta_{sp}^{k+1} J}{n! \Gamma_t^{k+1-n} (\theta_{sp}\tilde{P}_s)^n}. \end{aligned} \quad (32)$$

Third, $\check{\Psi}_3$ has an explicit form as

$$\check{\Psi}_3 = 1 - \mathcal{E}_{P_s} \left\{ 1 - e^{-N/P_s} \right\}. \quad (33)$$

With P_s in (2), the expectation in (33) is evaluated as

$$\begin{aligned} \check{\Psi}_3 &= \int_0^{I_t/\tilde{P}_s} e^{-N/\tilde{P}_s} \frac{e^{-x/\theta_{sp}}}{\theta_{sp}} dx + \int_{I_t/\tilde{P}_s}^{\infty} e^{-N/(I_t/x)} \frac{e^{-x/\theta_{sp}}}{\theta_{sp}} dx \\ &= e^{-N/\tilde{P}_s} \left(1 - e^{-I_t/\theta_{sp}\tilde{P}_s} \right) + \left(\frac{\theta_{sp}N}{I_t} + 1 \right)^{-1} e^{-((N/I_t)+(1/\theta_{sp}))I_t/\tilde{P}_s}. \end{aligned} \quad (34)$$

Finally, $\check{\Psi}_4$ is given by

$$\begin{aligned} \check{\Psi}_4 &= 1 - \mathcal{E}_{P_s} \left\{ \left(1 - e^{-N/P_s} \right) \left(1 + (M-1)e^{-\rho/\theta_{sr}P_s} + \sum_{k=0}^{\infty} \frac{J}{P_s^{k+1}} \right) \middle| P_s \right\} \\ &= \check{\Psi}_2 + \check{\Psi}_3 + \mathcal{E}_{P_s} \left\{ (M-1)e^{-((\rho/\theta_{sr})+N)/P_s} + \sum_{k=0}^{\infty} J \frac{e^{-N/P_s}}{P_s^{k+1}} \middle| P_s \right\}. \end{aligned} \quad (35)$$

With P_s in (2), the expectation in (35) is evaluated as

$$\begin{aligned} \check{\Psi}_4 &= \check{\Psi}_2 + \check{\Psi}_3 + \int_0^{I_t/\tilde{P}_s} \left((M-1)e^{-((\rho/\theta_{sr})+N)/\tilde{P}_s} \right. \\ &\quad \left. + \sum_{k=0}^{\infty} J \frac{e^{-N/\tilde{P}_s}}{\tilde{P}_s^{k+1}} \right) \frac{e^{-x/\theta_{sp}}}{\theta_{sp}} dx + \int_{I_t/\tilde{P}_s}^{\infty} \\ &\quad \cdot \left((M-1)e^{-((\rho/\theta_{sr})+N)\frac{x}{I_t}} + \sum_{k=0}^{\infty} J \left(\frac{x}{I_t} \right)^{k+1} e^{-N x/I_t} \right) \frac{e^{-x/\theta_{sp}}}{\theta_{sp}} dx \\ &= \check{\Psi}_2 + \check{\Psi}_3 + \left((M-1)e^{-((\rho/\theta_{sr})+N)/\tilde{P}_s} \right. \\ &\quad \left. + e^{-N/\tilde{P}_s} \sum_{k=0}^{\infty} \frac{J}{\tilde{P}_s^{k+1}} \right) \left(1 - e^{-I_t/\theta_{sp}\tilde{P}_s} \right) + (M-1) \\ &\quad \cdot \left(\frac{\theta_{sp}}{I_t} \left[N + \frac{\rho}{\theta_{sr}} \right] + 1 \right)^{-1} e^{-(N+(\rho/\theta_{sr})+(I_t/\theta_{sp}))I_t/\tilde{P}_s} \\ &\quad + \frac{e^{-(N+I_t/\theta_{sp})I_t/\tilde{P}_s}}{1+\theta_{sp}N/I_t} \sum_{k=0}^{\infty} \sum_{i=0}^{k+1} \left(N + \frac{I_t}{\theta_{sp}} \right)^{i-k-1} \frac{(k+1)! J}{i! \tilde{P}_s^i}. \end{aligned} \quad (36)$$

3.2. Outage Probability. The outage event happens as the channel capacity of D subceeds the target spectral efficiency $\tilde{\mathcal{R}}_d$. Accordingly, the OP is addressed to be

$$Y = \Pr \left\{ \mathcal{R}_d \leq \tilde{\mathcal{R}}_d \right\} = \Pr \left\{ \Gamma_d \leq \tilde{\Gamma}_d \right\}, \quad (37)$$

where $\tilde{\Gamma}_d = 2^{2\tilde{\mathcal{R}}_d/(1-\alpha)} - 1$.

Employing Γ_d in (12) reduces (37) to

$$\begin{aligned} Y &= \Pr \left\{ \min(\Gamma_{sr}, \Gamma_{rd}) \leq \tilde{\Gamma}_d \right\} \\ &= 1 - \Pr \left\{ \min(\Gamma_{sr}, \Gamma_{rd}) > \tilde{\Gamma}_d \right\} \\ &= 1 - \mathcal{E}_{P_s} \left\{ \underbrace{\mathcal{E}_{g_{sr}} \left\{ \tilde{Y} | g_{sr} > \frac{\tilde{\Gamma}_d \epsilon_r}{P_s(1-\beta)} \right\}}_{\tilde{Y}} \middle| P_s \right\}, \end{aligned} \quad (38)$$

where $\tilde{Y} = \Pr \left\{ g_{rd} > \tilde{\Gamma}_d \epsilon_d / P_r(1-\lambda) \right\}$.

Given P_r in (9), \tilde{Y} is rewritten as

$$\begin{aligned}\tilde{Y} &= \mathcal{E}_{g_{rp}} \left\{ \Pr \left\{ g_{rd} > \frac{\tilde{\Gamma}_d \varepsilon_d}{(1-\lambda) \min(\tilde{P}_r, I_t / g_{rp})} \right\} \right\} \\ &= \mathcal{E}_{g_{rp}} \left\{ e^{-\tilde{\Gamma}_d \varepsilon_d / ((1-\lambda)\theta_{rd} \min(\tilde{P}_r, I_t / g_{rp}))} \right\} \\ &= \int_0^{I_t / \tilde{P}_r} e^{-\tilde{\Gamma}_d \varepsilon_d / ((1-\lambda)\theta_{rd} \tilde{P}_r)} \frac{e^{-x/\theta_{rd}}}{\theta_{rp}} dx \\ &\quad + \int_{I_t / \tilde{P}_r}^{\infty} e^{-\tilde{\Gamma}_d \varepsilon_d x / ((1-\lambda)\theta_{rd} I_t)} \frac{e^{-x/\theta_{rp}}}{\theta_{rp}} dx \\ &= e^{-W/\tilde{P}_r} - Ge^{-W/\tilde{P}_r G},\end{aligned}\quad (39)$$

where $W = \tilde{\Gamma}_d \varepsilon_d / ((1-\lambda)\theta_{rd})$ and $G = \theta_{rp} W / (\theta_{rp} W + I_t)$.

Based on (3), two cases of \tilde{P}_r are considered when deriving \bar{Y} in (38) as follows.

Case 1. ($\tilde{P}_r = LP_s g_{sr}$).

This case holds when $g_{sr} \leq \rho/P_s$. Incorporating this condition with $g_{sr} > \varepsilon_r \tilde{\Gamma}_d / (P_s(1-\beta))$ in (38) results in existence region of g_{sr} to be $D/P_s < g_{sr} \leq \rho/P_s$ where $D = \varepsilon_r \tilde{\Gamma}_d / (1-\beta)$. By averaging \tilde{Y} in (39) over this region, one obtains \bar{Y} for this case as $\bar{Y}_1 = \int_{D/P_s}^{\rho/P_s} (e^{-W/LP_s x} - Ge^{-W/LGP_s x}) (e^{-x/\theta_{sr}} / \theta_{sr}) dx$. Applying the series expansion for $e^{-x/\theta_{sr}}$ and then performing the variable change $t = 1/x$, one solves the integral in \bar{Y}_1 as

$$\begin{aligned}\bar{Y}_1 &= \frac{1}{\theta_{sr}} \int_{D/P_s}^{\rho/P_s} \left(\sum_{k=0}^{\infty} \frac{1}{k!} \left[-\frac{x}{\theta_{sr}} \right]^k \right) (e^{-W/LP_s x} - Ge^{-W/LGP_s x}) dx \\ &= \sum_{k=0}^{\infty} \frac{(-\theta_{sr})^{-k-1}}{k!} \int_{P_s/D}^{P_s/\rho} (e^{-Wt/LP_s} - Ge^{-Wt/LGP_s}) \frac{1}{t^{k+2}} dt \\ &= \sum_{k=0}^{\infty} \frac{(-\theta_{sr})^{-k-1}}{k!} \left\{ \int_{P_s/D}^{\infty} (e^{-Wt/LP_s} - Ge^{-Wt/LGP_s}) \frac{1}{t^{k+2}} dt \right. \\ &\quad \left. - \int_{P_s/\rho}^{\infty} (e^{-Wt/LP_s} - Ge^{-Wt/LGP_s}) \frac{1}{t^{k+2}} dt \right\} = \sum_{k=0}^{\infty} \frac{V}{P_s^{k+1}},\end{aligned}\quad (40)$$

where $V = (1/(k!(k+1)!))(W/\theta_{sr}L)^{k+1} \{ \text{Ei}(-W/L\rho) - \text{Ei}(-W/LD) + G^{-k} [\text{Ei}(-W/LDG) - \text{Ei}(-W/LG\rho)] + \sum_{u=1}^{k+1} (u-1)! (-L/W)^u [D^u e^{-W/LD} - \rho^u e^{-W/L\rho} - G^{u-k} (D^u e^{-W/LDG} - \rho^u e^{-W/LG\rho})] \}$.

Case 2. ($\tilde{P}_r = L\rho$).

This case holds when $g_{sr} > \rho/P_s$. Incorporating this condition with $g_{sr} > \varepsilon_r \tilde{\Gamma}_d / (P_s(1-\beta))$ in (38) results in existence region of $g_{sr} > B/P_s$ where $B = \max(\varepsilon_r \tilde{\Gamma}_d / (1-\beta), \rho)$. By averaging \tilde{Y} in (39) over this region, one obtains \bar{Y} for this case as

$$\bar{Y}_2 = \int_{B/P_s}^{\infty} (e^{-W/L\rho} - Ge^{-W/LG\rho}) \frac{e^{-x/\theta_{sr}}}{\theta_{sr}} dx = Ue^{-B/\theta_{sr}P_s}, \quad (41)$$

where $U = e^{-W/L\rho} - Ge^{-W/LG\rho}$.

The total probability law simplifies \bar{Y} in (38) as

$$\bar{Y} = \bar{Y}_1 + \bar{Y}_2 = Ue^{-B/\theta_{sr}P_s} + \sum_{k=0}^{\infty} \frac{V}{P_s^{k+1}}. \quad (42)$$

Plugging (42) into \bar{Y} in (38) with a note that P_s is given in (2) results in

$$\begin{aligned}Y &= 1 - \mathcal{E}_{P_s} \left\{ Ue^{-B/\theta_{sr}P_s} + \sum_{k=0}^{\infty} \frac{V}{P_s^{k+1}} \right\} \\ &= 1 - \int_0^{I_t/\tilde{P}_s} \left(Ue^{-B/\theta_{sr}\tilde{P}_s} + \sum_{k=0}^{\infty} \frac{V}{\tilde{P}_s^{k+1}} \right) \frac{e^{-x/\theta_{sp}}}{\theta_{sp}} dx \\ &\quad - \int_{I_t/\tilde{P}_s}^{\infty} \left(Ue^{-Bx/\theta_{sr}I_t} + \sum_{k=0}^{\infty} V \left(\frac{x}{I_t} \right)^{k+1} \right) \frac{e^{-x/\theta_{sp}}}{\theta_{sp}} dx \\ &= 1 - \left(Ue^{-B/\theta_{sr}\tilde{P}_s} + \sum_{k=0}^{\infty} \frac{V}{\tilde{P}_s^{k+1}} \right) (1 - e^{-I_t/\theta_{sp}\tilde{P}_s}) \\ &\quad - U \left(\frac{\theta_{sp}B}{\theta_{sr}I_t} + 1 \right)^{-1} e^{-((B/\theta_{sr}) + (I_t/\theta_{sp}))1/\tilde{P}_s} \\ &\quad - \sum_{k=0}^{\infty} \sum_{i=0}^{k+1} \left(\frac{\theta_{sp}}{I_t} \right)^{k+1-i} e^{-I_t/\theta_{sp}\tilde{P}_s} \frac{(k+1)!V}{i!\tilde{P}_s^i}.\end{aligned}\quad (43)$$

3.3. Asymptotic Analysis. The asymptotic intercept and outage probabilities are analyzed under consideration of the following extreme cases: (1) Case 1: high maximum transmit power ($\tilde{P}_s \rightarrow \infty$) and (2) Case 2: high maximum interference power ($I_t \rightarrow \infty$). Case 2 corresponds to noncognitive networks (i.e., no interference power constraint) or no interference caused by secondary users on primary users (e.g., secondary users are distant from primary users or secondary-primary channels are blocked).

Case 1. ($\tilde{P}_s \rightarrow \infty$).

The intercept probability in this scenario becomes

$$\Psi_{\tilde{P}_s \rightarrow \infty} = \begin{cases} 0, & \tilde{\Gamma}_e \geq \max\left(\frac{[1-\beta]}{\beta}, \frac{[1-\lambda]}{\lambda}\right), \\ \check{\Psi}_2^{\tilde{P}_s \rightarrow \infty}, & \frac{(1-\beta)}{\beta} \leq \tilde{\Gamma}_e < \frac{(1-\lambda)}{\lambda}, \\ \check{\Psi}_3^{\tilde{P}_s \rightarrow \infty}, & \frac{(1-\lambda)}{\lambda} \leq \tilde{\Gamma}_e < \frac{(1-\beta)}{\beta}, \\ \check{\Psi}_4^{\tilde{P}_s \rightarrow \infty}, & \tilde{\Gamma}_e < \min\left(\frac{[1-\beta]}{\beta}, \frac{[1-\lambda]}{\lambda}\right), \end{cases} \quad (44)$$

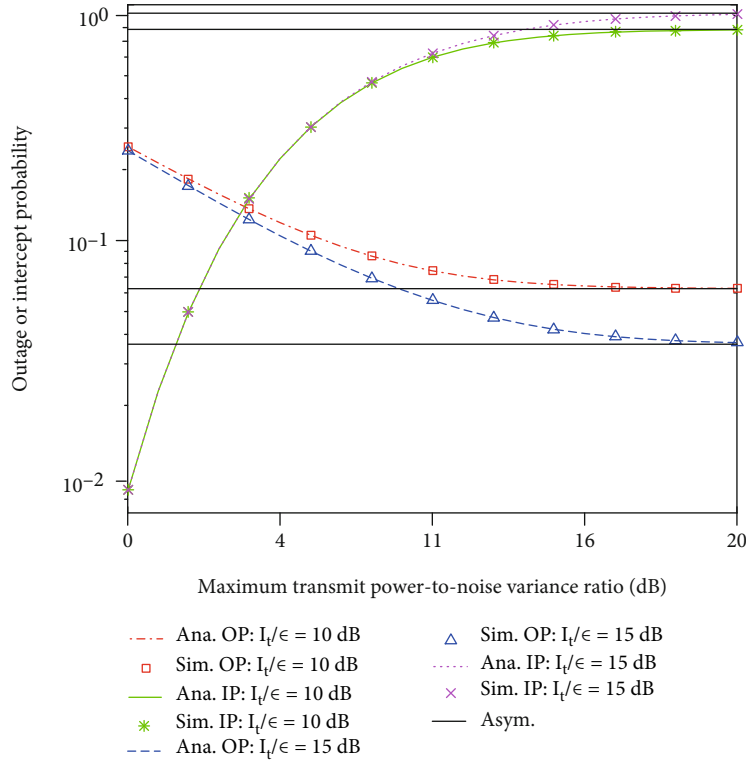


FIGURE 3: IP and OP versus $\Theta = \check{P}_s/\epsilon$. “Ana.” and “Sim.” represent the simulation result and the analytical result in Section 3, respectively, while “Asym.” represents the asymptotic result.

where $\check{\Psi}_2^{\check{P}_s \rightarrow \infty}$, $\check{\Psi}_3^{\check{P}_s \rightarrow \infty}$, and $\check{\Psi}_4^{\check{P}_s \rightarrow \infty}$ are obtained from $\check{\Psi}_2$ in (32), $\check{\Psi}_3$ in (34), and $\check{\Psi}_4$ in (36), respectively, as $\check{\Psi}_2^{\check{P}_s \rightarrow \infty} = \lim_{\check{P}_s \rightarrow \infty} \check{\Psi}_2 = (1 + (\theta_{sp}\rho/\theta_{sr}I_t))^{-1}(1 - M) - \sum_{k=0}^{\infty} (\theta_{sp}/I_t)^{k+1} (k + 1)! J$, $\check{\Psi}_3^{\check{P}_s \rightarrow \infty} = \lim_{\check{P}_s \rightarrow \infty} \check{\Psi}_3 = ((\theta_{sp}N/I_t) + 1)^{-1}$, and $\check{\Psi}_4^{\check{P}_s \rightarrow \infty} = \lim_{\check{P}_s \rightarrow \infty} \check{\Psi}_4 = \check{\Psi}_2^{\check{P}_s \rightarrow \infty} + (M - 1)((\theta_{sp}/I_t)[(\rho/\theta_{sr}) + N] + 1)^{-1} + \check{\Psi}_3^{\check{P}_s \rightarrow \infty} + (I_t/\theta_{sp}) \sum_{k=0}^{\infty} (k + 1)! (N + (I_t/\theta_{sp}))^{-k-2} J$.

Likewise, the outage probability in this scenario is obtained from (43) to be

$$Y^{\check{P}_s \rightarrow \infty} = \lim_{\check{P}_s \rightarrow \infty} Y = 1 - \left(\frac{\theta_{sp}B}{\theta_{sr}I_t} + 1 \right)^{-1} U - \sum_{k=0}^{\infty} (k + 1)! \left(\frac{\theta_{sp}}{I_t} \right)^{k+1} V. \quad (45)$$

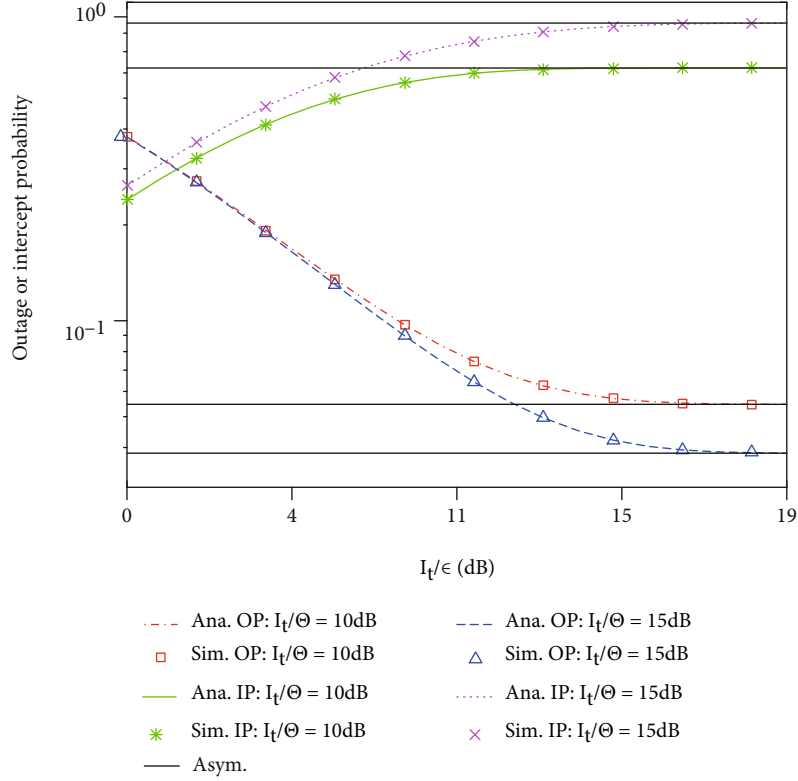
It is observed from (44) and (45) that when the maximum transmit power is large, both IP and OP converge, creating the error floors (or zero diversity orders). This result will be validated in Figure 3.

Case 2. ($I_t \rightarrow \infty$).

The intercept probability in this case becomes

$$\Psi^{I_t \rightarrow \infty} = \begin{cases} 0, & \tilde{\Gamma}_e \geq \max\left(\frac{[1-\beta]}{\beta}, \frac{[1-\lambda]}{\lambda}\right), \\ \check{\Psi}_2^{I_t \rightarrow \infty}, & \frac{(1-\beta)}{\beta} \leq \tilde{\Gamma}_e < \frac{(1-\lambda)}{\lambda}, \\ \check{\Psi}_3^{I_t \rightarrow \infty}, & \frac{(1-\lambda)}{\lambda} \leq \tilde{\Gamma}_e < \frac{(1-\beta)}{\beta}, \\ \check{\Psi}_4^{I_t \rightarrow \infty}, & \tilde{\Gamma}_e < \min\left(\frac{[1-\beta]}{\beta}, \frac{[1-\lambda]}{\lambda}\right), \end{cases} \quad (46)$$

where $\check{\Psi}_2^{I_t \rightarrow \infty}$, $\check{\Psi}_3^{I_t \rightarrow \infty}$, and $\check{\Psi}_4^{I_t \rightarrow \infty}$ are obtained from $\check{\Psi}_2$ in (32), $\check{\Psi}_3$ in (34), and $\check{\Psi}_4$ in (36), respectively, as $\check{\Psi}_2^{I_t \rightarrow \infty} = \lim_{I_t \rightarrow \infty} \check{\Psi}_2 = (1 - M_1)e^{-\rho/\theta_{sr}\check{P}_s} - \sum_{k=0}^{\infty} J_1/\check{P}_s^{k+1}$, $\check{\Psi}_3^{I_t \rightarrow \infty} = \lim_{I_t \rightarrow \infty} \check{\Psi}_3 = e^{-N/\check{P}_s}$, and $\check{\Psi}_4^{I_t \rightarrow \infty} = \lim_{I_t \rightarrow \infty} \check{\Psi}_4 = \check{\Psi}_2^{I_t \rightarrow \infty} + \check{\Psi}_3^{I_t \rightarrow \infty} + (M_1 - 1)e^{-(N+(\rho/\theta_{sr}))1/\check{P}_s} + e^{-N/\check{P}_s} \sum_{k=0}^{\infty} J_1/\check{P}_s^{k+1}$ where $J_1 = \lim_{I_t \rightarrow \infty} J = (1/(k!(k+1)!))(Q/L\theta_{sr})^{k+1} [e^{-Q/L\rho} \sum_{u=1}^{k+1} (u-1)! (-L\rho/Q)^u - \text{Ei}(-Q/L\rho)]$ and $M_1 = \lim_{I_t \rightarrow \infty} M = 1 - e^{-Q/L\rho}$.

FIGURE 4: IP and OP versus I_t/ϵ .

Likewise, the outage probability in this scenario is obtained from (38) to be

$$Y^{I_t \rightarrow \infty} = \lim_{I_t \rightarrow \infty} Y = 1 - U_1 e^{-B/\theta_{sr} \check{P}_s} - \sum_{k=0}^{\infty} \frac{V_1}{\check{P}_s^{k+1}}, \quad (47)$$

where $U_1 = \lim_{I_t \rightarrow \infty} U = e^{-W/L\rho}$ and $V_1 = \lim_{I_t \rightarrow \infty} V = (1/(k!(k+1)!)) (W/\theta_{sr}L)^{k+1} \{Ei(-W/L\rho) - Ei(-W/LD) + \sum_{u=1}^{k+1} (u-1)!(-L/W)^u [e^{-W/LD} D^u - e^{-W/L\rho} \rho^u]\}$.

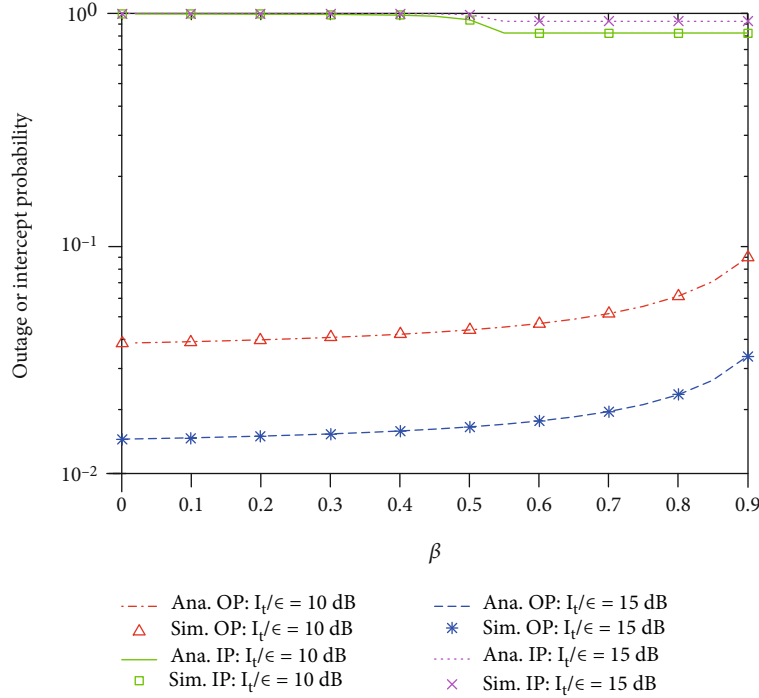
It is seen from (46) and (47) that when the maximum interference power is large, both IP and OP also converge, creating the error floors (or zero diversity orders). This result will be validated in Figure 4.

4. Demonstrative Results

The current section demonstrates simulated/theoretical results to assess both security and reliability of the proposed jamming-and-transmitting scheme for spectrum-sharing relaying networks with nonlinear energy scavenging via essential parameters. Monte-Carlo simulations (the Monte-Carlo simulation is widely accepted, e.g., [54]; therefore, an explanation of its operation should not be included in this paper) produce simulated results while the derived expressions in Section 3 are calculated to achieve theoretical ones. For illustration intention, users are arbitrarily positioned in the 2-dimensional plane as E at $(0.6, -0.5)$, P at $(0.9, 0.8)$,

D at $(1.0, 0.0)$, R at $(0.5, 0.0)$, and S at $(0.0, 0.0)$. Unless otherwise stated, the following parameters are considered: the target spectral efficiency $\mathcal{R}_e = \mathcal{R}_d = 0.3$ bps/Hz, the path-loss exponent $\delta = 3$, the energy converting efficiency $\psi = 0.9$, and equal noise variances $\epsilon_d = \epsilon_r = \epsilon_e = \epsilon$.

Figure 3 plots the IP and the OP versus $\Theta = \check{P}_s/\epsilon$ for $\alpha = 0.35$, $\rho/\epsilon = 10$ dB, $\beta = 0.48$, and $\lambda = 0.63$. The results demonstrate the coincidence between the simulation and the analysis, validating the accurateness of the analytical results. Moreover, the reliability of the system is enhanced and the security is decreased with increasing \check{P}_s , which comes from the reality that increasing \check{P}_s facilitates R in recovering successfully the source data and scavenging more energy in the source signals, hence mitigating the outage probability in Phase 3. Likewise, E is also beneficial in both Phase 2 and Phase 3 when \check{P}_s increases, so the intercept probability also grows with \check{P}_s . However, both IP and OP converge at high \check{P}_s . Such a convergence is owing to the power distribution of the spectrum-sharing operation mode for S and R in (2) and (9) where transmit powers are uncorrelated with \check{P}_s for large \check{P}_s (i.e., as \check{P}_s is adequately large, the MTPC is not necessary), causing the constant IP/OP. Such a constant IP/OP is named as the asymptotic IP/OP, which was analyzed in Subsection 3.3. Furthermore, the OP goes down and the IP goes up with increasing I_t . This observation is comprehended similarly to the case of increasing \check{P}_s owing to the power distribution of the spectrum-sharing operation mode for S and R . Due to the opposite trends of the IP and

FIGURE 5: IP and OP versus β .

the OP, the security-reliability trade-off is observed. By the exhaustive search, any security-reliability trade-off level can be found straightforwardly; for example, Figure 3 reveals that the best security-reliability trade-off wherein the OP and the IP are equal occurs at $\Theta = 3.84$ dB for $I_t/\epsilon = 10$ dB.

Figure 4 plots the IP/OP versus I_t/ϵ for the same specifications as Figure 3. The results reveal the coincidence between the simulation and the analysis, asserting the correctness of the analytical results. Moreover, the reliability/security is improved/degraded with increasing I_t and \check{P}_s , which shows the security-reliability trade-off. By the exhaustive search, any security-reliability trade-off level can be found easily; for instance, Figure 4 unveils that the best security-reliability trade-off wherein the IP and the OP are equal happens at $I_t/\epsilon = 1.46$ dB for $\Theta = 10$ dB. Nonetheless, the reliability and the security converge at large I_t , which validates the asymptotic analysis in Subsection 3.3. The results in Figure 4 are comprehended similarly to those in Figure 3.

Figure 5 exposes the IP/OP versus the power distribution coefficient β at S , which presents the percentage of power that S uses to transmit the jamming signal, for $\check{P}_s/\epsilon = 20$ dB, $\rho/\epsilon = 15$ dB, $\alpha = 0.35$, and $\lambda = 0.48$. The results unveil the coincidence between the analysis and the simulation, affirming the correctness of the analytical results. It is noted that β is the superposition coefficient which is inversely proportional to S 's signal but proportional to the jamming signal in Phase 2. Consequently, the increase in β creates less energy for S to transmit information signal and less chance for R to decode successfully the message, which leads to the growth of the OP and the slight decline of the IP. However, the IP remains constant for $\tilde{\Gamma}_e \geq (1 - \beta)/\beta$ (or $\beta \geq 1/(1 + \tilde{\Gamma}_e)$) as seen from (27). This is because E suffers a com-

plete outage in Phase 2, and hence, the IP only depends on Phase 3. Moreover, the reliability trades off with the security owing to the opposite trends of the IP and the OP, which was also observed similarly to Figure 3. Additionally, the security/reliability is degraded/enhanced with the increase in I_t , which is similar to results in previous figures.

Figure 6 demonstrates the IP/OP versus the power distribution coefficient λ at R , which presents the percentage of power that R uses to transmit the jamming signal, for $\check{P}_s/\epsilon = 20$ dB, $\rho/\epsilon = 15$ dB, $\alpha = 0.35$, and $\beta = 0.63$. The results reveal the coincidence between the analysis and the simulation, asserting the correctness of the analytical results. Moreover, it is seen that the reliability is deteriorated while the security is better with increasing λ . This can be comprehended by the power allocation of the spectrum-sharing operation mode at R for the legitimate signal and the jamming signal, similar to Figure 5. Notably, the IP reduces to zero and the absolute security is achievable when λ is greater than a certain value; for example, $\lambda > 0.5$ as in the case of Figure 6. This can be interpreted as follows. Since $\beta = 0.63$ and $\alpha = 0.35$, the inequality $\beta \geq 1/(1 + \tilde{\Gamma}_e)$ holds where $\tilde{\Gamma}_e = 2^{2\check{P}_s/\epsilon/(1-\alpha)} - 1$. Therefore, when $\lambda \geq 1/(1 + \tilde{\Gamma}_e)$, E suffers a complete outage in both phases (2 and 3) as seen in (29), causing $\Psi = 0$. In addition, the security trades off with the reliability owing to the opposite trends of the IP and the OP, which was also observed similarly to Figure 3. Additionally, the security/reliability is deteriorated/enhanced with respect to the increase in I_t , as anticipated.

Figure 7 plots the IP/OP versus the time fraction α for $\check{P}_s/\epsilon = 20$ dB, $\rho/\epsilon = 15$ dB, $\beta = 0.48$, and $\lambda = 0.63$. The results unveil the coincidence between the analysis and the simulation, affirming the correctness of the analytical results.

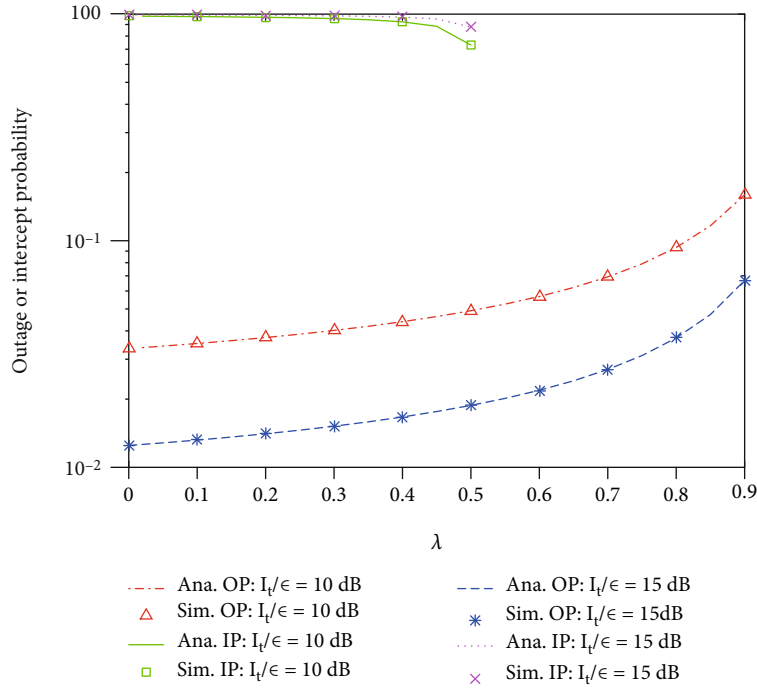


FIGURE 6: OP and IP versus λ .

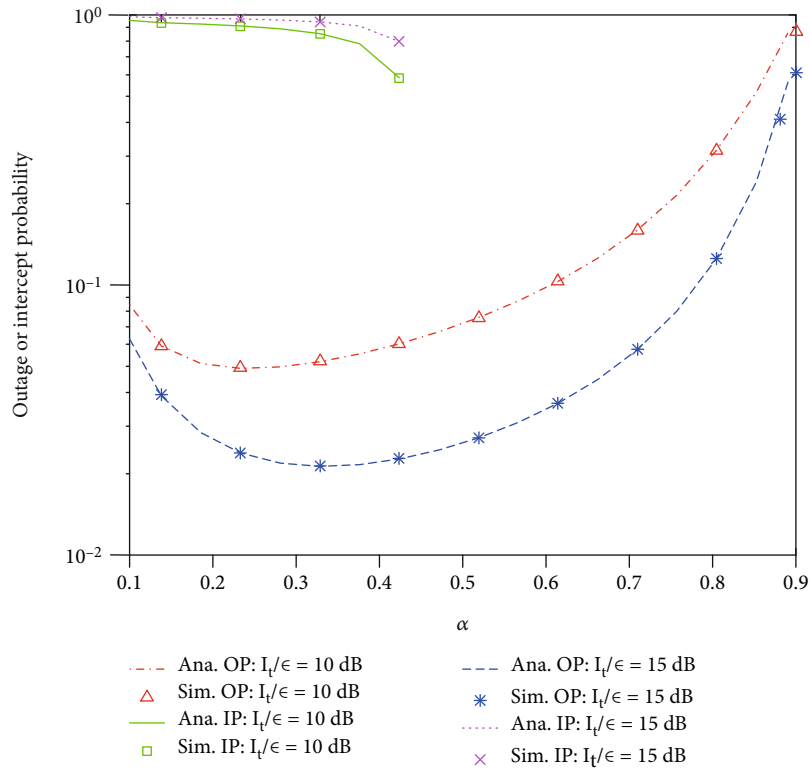
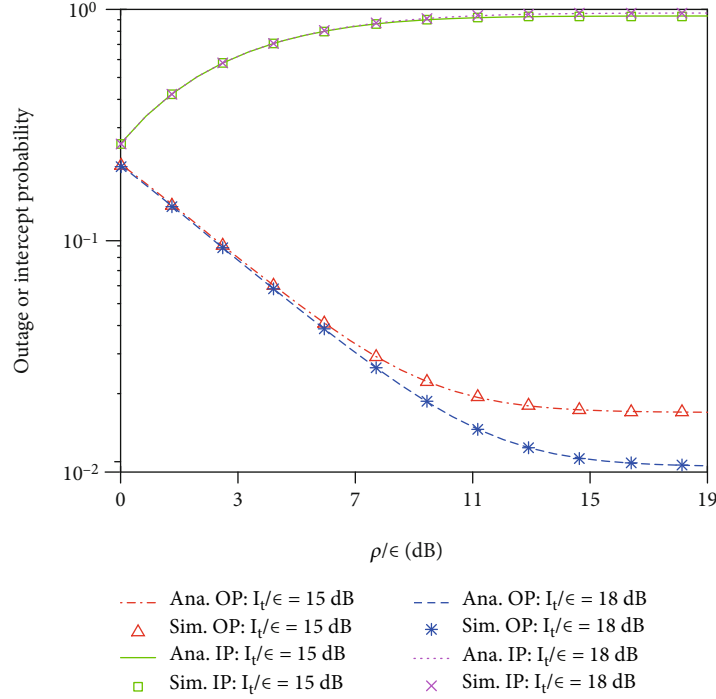


FIGURE 7: IP and OP versus α .

Further, α can be selected optimally for the best reliability; for instance, $\alpha_{\text{opt}} = 0.3$ is seen in Figure 7. α_{opt} is available owing to the following reality. The increase in α extends the duration of Phase 1 (energy harvesting stage), facilitating

R in harvesting more energy and recovering successfully the source message with a higher possibility. Notwithstanding, the increase in α also deteriorates the channel capacities in Phase 2 and Phase 3 (information transmission stage)

FIGURE 8: IP and OP versus ρ/ϵ .

because of the factor $(1 - \alpha)/2$ before the logarithm in (14). Accordingly, α can be optimally adopted to balance the durations of energy scavenging and data transmission stages for the best reliability. Interestingly, the security is enhanced with increasing α . Some reasons lead to this observation as follows. Firstly, increasing α reduces the channel capacities at E , which can be explained as above. Secondly, although increasing α helps R collect more energy, E suffers the increase of the jamming power from R , eventually reducing the IP. Moreover, the IP reduces to zero for large α . This is because large α makes the inequality $\tilde{\Gamma}_e \geq \max([1 - \lambda]/\lambda, [1 - \beta]/\beta)$ holds where $\tilde{\Gamma}_e = 2^{2\tilde{\mathcal{R}}_e/(1-\alpha)} - 1$, and hence, the IP reduces to zero according to (29), which is similar to the results in Figure 6. In addition, the security/reliability is degraded/enhanced with the increase in I_t , as anticipated.

Figure 8 exposes the IP/OP versus ρ/ϵ for $\check{P}_s/\epsilon = 20$ dB, $\beta = 0.63$, and $\lambda = 0.48$. The results reveal the coincidence between the analysis and the simulation, affirming the correctness of the analytical results. Further, the reliability-security trade-off of the proposed jamming-and-transmitting scheme is observed in this figure. Nonetheless, the reliability gain increases faster than the security loss with increasing the power saturation threshold of the NL energy scavenger ρ , exposing the advantage of both relaying and jamming in our scheme in ensuring high reliability with affordable security threat. Moreover, the starting points at which the IP and the OP start to be saturated are coincident at ρ/ϵ of approximately 15 dB. That the IP and the OP are saturated at large ρ is because large ρ reduces the NL energy harvester to the linear one. In addition, the security/reliability is degraded/enhanced with the increase in I_t , as anticipated.

5. Conclusion

This paper recommended the simultaneous jamming-and-transmitting scheme for spectrum sharing relaying networks with the nonlinear energy scavenger. Its security and reliability were analyzed and assessed with the intercept and outage probabilities under the IPR and the MTPC. The recommended analysis is validated by multifarious Monte-Carlo simulations. Illustrative results expose that the relay capable of scavenging RF energy enhances drastically the reliability even when the direct secondary source-destination link is unreliable because of bad propagation conditions. Moreover, jamming in both signal transmission phases achieve better security even with increasing transmission power. Additionally, the reliability of the proposed scheme can be optimized with selecting appropriately the time fraction. Notably, the networks can achieve the absolute security with adopting a suitable set of α , β , λ , and $\tilde{\mathcal{R}}_e$. Further, the proposed scheme offers the security-reliability compromise but suffers saturated performance at large maximum transmit/interference power. Furthermore, the reliability/security of the NL-ES is significantly worse/better than that of the L-ES.

Data Availability

The authors declare that all 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 study/work/research was fully funded by Tra Vinh University under grant contract number 181/HD.HDKH&DT-DHTV. For the other supports, Khuong Ho-Van would like to thank Ho Chi Minh City University of Technology (HCMUT), VNU-HCM, for the support of time and facilities for this study.

References

- [1] N. Shinohara, "Trends in wireless power transfer: WPT technology for energy harvesting, millimeter-wave/THz rectennas, MIMO-WPT, and advances in near-field WPT applications," *IEEE Microwave Magazine*, vol. 22, no. 1, pp. 46–59, 2021.
- [2] F. Benkhelifa, H. ElSawy, J. A. Mccann, and M. S. Alouini, "Recycling cellular energy for self-sustainable IoT networks: a spatiotemporal study," *IEEE Transactions on Wireless Communications*, vol. 19, no. 4, pp. 2699–2712, 2020.
- [3] Z. Liang and J. Yuan, "Modelling and prediction of mobile service channel power density for RF energy harvesting," *IEEE Wireless Communications Letters*, vol. 9, no. 5, pp. 741–744, 2020.
- [4] K. Ali and D. J. Rogers, "An orientation-independent multi-input energy harvesting wireless sensor node," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 2, pp. 1665–1674, 2021.
- [5] L. Ge, G. Chen, Y. Zhang, J. Tang, J. Wang, and J. A. Chambers, "Performance analysis for multihop cognitive radio networks with energy harvesting by using stochastic geometry," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1154–1163, 2020.
- [6] K. Ho-van and T. Do-Dac, "Security enhancement for energy harvesting cognitive networks with relay selection," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 8867148, 13 pages, 2020.
- [7] S. Solanki, P. K. Upadhyay, D. B. D. Costa, H. Ding, and J. M. Moualeu, "Performance analysis of piece-wise linear model of energy harvesting-based multiuser overlay spectrum sharing networks," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 1820–1836, 2020.
- [8] Z. Ali, G. A. S. Sidhu, M. Waqas, L. Xing, and F. Gao, "A joint optimization framework for energy harvesting based cooperative CR networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 2, pp. 452–462, 2019.
- [9] N. I. Miridakis, T. A. Tsiftsis, G. C. Alexandropoulos, and M. Debbah, "Simultaneous spectrum sensing and data reception for cognitive spatial multiplexing distributed systems," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3313–3327, 2017.
- [10] H. Lei, M. Xu, I. S. Ansari, G. Pan, K. A. Qaraqe, and M. S. Alouini, "On secure underlay MIMO cognitive radio networks with energy harvesting and transmit antenna selection," *IEEE Transactions on Green Communications and Networking*, vol. 1, no. 2, pp. 192–203, 2017.
- [11] H. Shi, Y. Cai, D. Chen, J. Hu, W. Yang, and W. Yang, "Physical layer security in an untrusted energy harvesting relay network," *IEEE Access*, vol. 7, pp. 24819–24828, 2019.
- [12] N. I. Miridakis, T. A. Tsiftsis, and G. C. Alexandropoulos, "MIMO underlay cognitive radio: optimized power allocation, effective number of transmit antennas and harvest-transmit tradeoff," *IEEE Transactions on Green Communications and Networking*, vol. 2, no. 4, pp. 1101–1114, 2018.
- [13] D. Mishra and G. C. Alexandropoulos, "Transmit precoding and receive power splitting for harvested power maximization in MIMO SWIPT systems," *IEEE Transactions on Green Communications and Networking*, vol. 2, no. 3, pp. 774–786, 2018.
- [14] F. Wang and X. Zhang, "Secure resource allocation for polarization-based non-linear energy harvesting over 5G cooperative CRNs," *IEEE Wireless Communications Letters*, 2020.
- [15] D. Wang, F. Rezaei, and C. Tellambura, "Performance analysis and resource allocations for a WPCN with a new nonlinear energy harvester model," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 1403–1424, 2020.
- [16] G. Ma, J. Xu, Y.-F. Liu, and M. R. Vedady Moghadam, "Time-division energy beamforming for multiuser wireless power transfer with non-linear energy harvesting," *IEEE Wireless Communications Letters*, vol. 10, no. 1, pp. 53–57, 2021.
- [17] Z. Zhu, N. Wang, W. Hao, Z. Wang, and I. Lee, "Robust beamforming designs in secure MIMO SWIPT IoT networks with a non-linear channel model," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1702–1715, 2021.
- [18] T. X. Vu, S. Chatzinotas, S. Gautam, E. Lagunas, and B. Ottersten, "Joint optimization for PS-based SWIPT multi-user systems with non-linear energy harvesting," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Seoul, Korea, May 2020.
- [19] X. Liu, Y. Gao, M. Guo, and N. Sha, "Secrecy throughput optimization for the WPCNs with non-linear EH model," *IEEE Access*, vol. 7, pp. 59477–59490, 2019.
- [20] Y. Lu, K. Xiong, P. Fan, Z. Ding, Z. Zhong, and K. B. Letaief, "Global energy efficiency in secure MISO SWIPT systems with non-linear power-splitting EH model," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 1, pp. 216–232, 2019.
- [21] S. Gao, K. Xiong, R. Jiang, L. Zhou, and H. Tang, "Outage performance of wireless-powered SWIPT networks with non-linear EH model in Nakagami-m fading," in *2018 14th IEEE International Conference on Signal Processing (ICSP)*, pp. 668–671, Beijing, China, Aug. 2018.
- [22] L. Ni, X. Da, H. Hu, M. Zhang, and K. Cumanan, "Outage constrained robust secrecy energy efficiency maximization for EH cognitive radio networks," *IEEE Wireless Communications Letters*, vol. 9, no. 3, pp. 363–366, 2020.
- [23] F. Zhou, Z. Chu, Y. Wu, N. Al-Dhahir, and P. Xiao, "Enhancing PHY security of MISO NOMA SWIPT systems with a practical non-linear EH model," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, Kansas City, MO, USA, May 2018.
- [24] E. Boshkovska, D. W. K. Ng, L. Dai, and R. Schober, "Power-efficient and secure WPCNs with hardware impairments and non-linear EH circuit," *IEEE Transactions on Communications*, vol. 66, no. 6, pp. 2642–2657, 2018.
- [25] Y. Che, Y. Lai, S. Luo, K. Wu, and L. Duan, "UAV-aided information and energy transmissions for cognitive and sustainable 5G networks," *IEEE Transactions on Wireless Communications*, vol. 20, no. 3, pp. 1668–1683, 2021.
- [26] D. Wang and S. Men, "Secure energy efficiency for NOMA based cognitive radio networks with nonlinear energy harvesting," *IEEE Access*, vol. 6, pp. 62707–62716, 2018.
- [27] N. Shanin, L. Cottatellucci, and R. Schober, "Markov decision process based design of SWIPT systems: non-linear EH

- circuits, memory, and impedance mismatch,” *IEEE Transactions on Communications*, vol. 69, no. 2, pp. 1259–1274, 2021.
- [28] S. Bayat, A. Khalili, and Z. Han, “Resource allocation for MC MISO-NOMA SWIPT-enabled HetNets with non-linear energy harvesting,” *IEEE Access*, vol. 8, pp. 192270–192281, 2020.
- [29] S. A. A. Kazmi and S. Coleri, “Optimization of full-duplex relaying system with non-linear energy harvester,” *IEEE Access*, vol. 8, pp. 201566–201576, 2020.
- [30] A. Anwar, S. T. Shah, S. F. Hasan, and D. R. Shin, “SWIPT-based three-step multiplicative amplify-and-forward two-way relay networks with non-linear energy conversion model,” in *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, pp. 152–157, Chengdu, China, Dec. 2018.
- [31] P. Raut, P. K. Sharma, T. A. Tsiftsis, and Y. Zou, “Power-time splitting-based non-linear energy harvesting in FD short-packet communications,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9146–9151, 2020.
- [32] Y. Liu, Y. Ye, H. Ding, F. Gao, and H. Yang, “Outage performance analysis for SWIPT-based incremental cooperative NOMA networks with non-linear harvester,” *IEEE Communications Letters*, vol. 24, no. 2, pp. 287–291, 2020.
- [33] L. Shi, W. Cheng, Y. Ye, H. Zhang, and R. Q. Hu, “Heterogeneous power-splitting based two-way DF relaying with non-linear energy harvesting,” in *2018 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, Abu Dhabi, United Arab Emirates, Dec. 2018.
- [34] X. Xie, J. Chen, and Y. Fu, “Outage performance and QoS optimization in full-duplex system with non-linear energy harvesting model,” *IEEE Access*, vol. 6, pp. 44281–44290, 2018.
- [35] Y. Liu, F. Gao, X. Deng, T. Wu, and X. Zhang, “Performance analysis for incremental DF relaying networks with non-linear energy harvesting,” in *2020 IEEE 20th International Conference on Communication Technology (ICCT)*, pp. 354–360, Nanning, China, Oct. 2020.
- [36] Y. Zhang, X.-Q. Jiang, H. Hai, J. Hau, and K. Z. Peng, “Generalized non-linear energy harvesting protocol for enhancing security of AF multi-antenna relaying systems,” in *2019 IEEE 2nd International Conference on Electronics and Communication Engineering (ICECE)*, pp. 195–201, Xi’an, China, Dec. 2019.
- [37] M. Babaei, U. Aygolu, M. Basaran, and L. Durak-Ata, “BER performance of full-duplex cognitive radio network with non-linear energy harvesting,” *IEEE Transactions on Green Communications and Networking*, vol. 4, no. 2, pp. 448–460, 2020.
- [38] K. Agrawal, M. F. Flanagan, and S. Prakriya, “NOMA with battery-assisted energy harvesting full-duplex relay,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13952–13957, 2020.
- [39] A. Hakimi, M. Mohammadi, Z. Mobini, and Z. Ding, “Full-duplex non-orthogonal multiple access cooperative spectrum-sharing networks with non-linear energy harvesting,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 10925–10936, 2020.
- [40] A. Prathima, D. S. Gurjar, S. Y. A. Prathima, D. S. Gurjar, and S. Yadav, “Two-way cooperative cognitive radio networks with nonlinear RF-energy harvester,” in *2020 IEEE Latin-American Conference on Communications (LATINCOM)*, pp. 1–6, Santo Domingo, Dominican Republic, Nov. 2020.
- [41] P. Maji, S. D. Roy, and S. Kundu, “Physical layer security with non-linear energy harvesting relay,” in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–6, Kanpur, India, July 2019.
- [42] H. Li and X. Zhao, “Throughput maximization with energy harvesting in UAV-assisted cognitive mobile relay networks,” *IEEE Transactions Cognitive Communications and Networking*, vol. 7, no. 1, pp. 197–209, 2021.
- [43] A. Shome, A. K. Dutta, and S. Chakrabarti, “BER performance analysis of energy harvesting underlay cooperative cognitive radio network with randomly located primary users and secondary relays,” *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4740–4752, 2021.
- [44] T.-V. Nguyen, T.-N. Tran, K. Shim, T. Huynh-The, and B. An, “A deep-neural-network-based relay selection scheme in wireless-powered cognitive IoT networks,” *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7423–7436, 2021.
- [45] X. Zhang, J. Xing, Z. Yan, Y. Gao, and W. Wang, “Outage performance study of cognitive relay networks with imperfect channel knowledge,” *IEEE Communications Letters*, vol. 17, no. 1, pp. 27–30, 2013.
- [46] M. Seyfi, S. Muhaidat, and J. Liang, “Relay selection in cognitive radio networks with interference constraints,” *IET Communications*, vol. 7, no. 10, article 922930, 2013.
- [47] M. Nguyen, N. P. Nguyen, D. B. da Costa, H. K. Nguyen, and R. T. de Sousa, “Secure cooperative half-duplex cognitive radio networks with K -th best relay selection,” *IEEE Access*, vol. 5, pp. 6678–6687, 2017.
- [48] H. Sun, F. Zhou, R. Q. Hu, and L. Hanzo, “Robust beamforming design in a NOMA cognitive radio network relying on SWIPT,” *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 1, pp. 142–155, 2019.
- [49] F. Zhou, Z. Chu, H. Sun, R. Q. Hu, and L. Hanzo, “Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT,” *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 918–931, 2018.
- [50] F. Zhou, Z. Li, J. Cheng, Q. Li, and J. Si, “Robust AN-aided beamforming and power splitting design for secure MISO cognitive radio with SWIPT,” *IEEE Transactions on Wireless Communications*, vol. 16, no. 4, pp. 2450–2464, 2017.
- [51] D. Wang, F. Zhou, and V. C. M. Leung, “Primary privacy preserving with joint wireless power and information transfer for cognitive radio networks,” *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 2, pp. 683–693, 2020.
- [52] R. Zhao, Y. Yuan, L. Fan, and Y. C. He, “Secrecy performance analysis of cognitive decode-and-forward relay networks in Nakagami-m fading channels,” *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 549–563, 2017.
- [53] B. Vucetic and J. Yuan, *Space-Time Coding*, John Wiley & Sons, 2003.
- [54] N. T. Thomopoulos, *Essentials of Monte Carlo Simulation: Statistical Methods for Building Simulation Models*, Springer, New York Heidelberg Dordrecht London, 2013.

Research Article

A Cross-Domain Authentication Optimization Scheme between Heterogeneous IoT Applications

Shichang Xuan , Haibo Xiao , Dapeng Man , Wei Wang , and Wu Yang 

Information Security Research Center, Harbin Engineering University, Harbin 150001, China

Correspondence should be addressed to Wei Wang; w_wei@hrbeu.edu.cn

Received 5 March 2021; Revised 9 August 2021; Accepted 15 September 2021; Published 29 September 2021

Academic Editor: Ding Wang

Copyright © 2021 Shichang Xuan 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 enrichment of the Internet of Things (IoT) applications, the demand for value exchange and collaborative control between heterogeneous IoT applications is increasing. However, the user management space varies depending on the IoT application, where the security domain stands as an example. It is one of the key technologies of data sharing between heterogeneous IoT organizations to cross the boundary of the security domain and verify the identity and authority of users in other security domains. Aiming at the slow speed of authentication protocol authority authentication during cross-domain access and without considering the actual cross-domain situation, the same cryptographic system parameters are used for all communication nodes in a cross-domain environment. This article proposes a heterogeneous Internet of Things data access authority authentication scheme between applications. Based on certificate-less public key cryptography and smart contract technology, a certificate-less cross-domain authentication scheme that supports parameter differentiation is designed and implemented. The theoretical and empirical analyses, comparing the communication volume, identity signature, and verification calculation cost, validated that the method proposed improves the cross-domain identity authorization authentication ability and supports the use of differentiated cryptographic system parameters among different IoT applications.

1. Introduction

The increasing popularity of the Internet of Things (IoT) has resulted in the growth of connected devices, such as sensors and smart devices, at an alarming rate, which have become an integral part of daily human life [1–5]. The Internet data center predicts that by 2025, there will be more than 40 billion IoT devices connected to the Internet [6]. Although the Internet has been deployed on a large scale in many Internet of Things application scenarios such as smart cities, industrial IoT, and vehicle Internet, it is more vulnerable due to limited resources. The traditional client-server architecture mostly relies on a centralized cloud architecture, which means that massive amounts of IoT data will be transmitted to a centralized cloud server via the Internet. The centralized IoT communication model faces the era of the explosive growth of big data and brings many drawbacks, such as high-latency response, lack of security, and a large amount

of workload. Moreover, these peer-to-peer networks and cloud environment-based traditional centralized IoT data sharing solutions cannot prevent the single points of failure and the attacks targeting the centralized storage. The traditional IoT architecture has many major limitations that cannot meet the security requirements of IoT, such as relying on trusted servers, powerless to time-sensitive applications, and high data maintenance costs [7, 8].

The booming blockchain technology is considered highly promising to tighten the security in the IoT. The blockchain can be used to establish a distributed trust mechanism improving the efficiency of IoT communication, thereby solving the security and accuracy problems in the abovementioned centralized IoT architecture. The blockchain is essentially a distributed ledger distributed throughout the distributed system [9]. It is a data structure shared by all nodes and cannot be tampered with. Anyone can upload and access the data, and everyone needs to be

responsible for their data. Therefore, the blockchain can conduct transactions in a mutually distrusted distributed system. Unlike the existing transaction management system where the central agency needs to verify transactions, the blockchain can realize decentralized verification of transactions, thereby greatly saving costs and alleviating the performance bottleneck of the central agency. Besides, every transaction stored in the blockchain is inherently immutable, because every node in the network stores all submitted transactions in the blockchain. At the same time, encryption mechanisms (such as asymmetric encryption algorithms, digital signatures, and hash functions) ensure the integrity of blockchain data blocks [10]. Therefore, the blockchain can ensure the nonrepudiation of transactions. First, the blockchain verifies the data in chronological order and then counts it into unchangeable blocks. Furthermore, it maintains the data consistency of each node through the node consensus, which does not require any trusted intermediary. These features are distributed IoT security. Sexual expansion provides new solutions [11–14].

With the continuous enrichment of IoT applications, there will inevitably be a demand for valuable exchange and collaborative control between different IoT applications, which cannot avoid the problem of cross-domain identity authorization authentication. Cross-domain authentication is one of the key technologies for secure IoT communications as user space and autonomy vary from application to application. However, traditional centralized solutions have problems such as single node failure, key escrow, and man-in-the-middle attacks, which are not suitable for IoT terminals [15]. Blockchain technology with the characteristics of a decentralized, fully distributed P2P network, transaction transparency, nontampering, and encryption algorithms to ensure security is considered an effective means to achieve decentralized authentication [16–18]. The researchers combined blockchain with cross-domain authentication technology to address the issues related to cross-domain user identity authentication and establishing trust between entities in a distributed IoT environment. However, most cross-domain authentication protocols adopt complex bilinear pairing operations, and the authentication efficiency is low, and the actual cross-domain situation is not considered. Using the same cryptographic system parameters between all communication nodes in the cross-domain environment, to guarantee the private key safety, a secure channel is required for transmission, which leads to problems such as reduced security. This work introduces a Certificate-less Cross-domain Authentication Scheme with Different System Parameters (DSP-CCAS) that supports parameter differentiation based on certificate-less passwords. By improving the certificate-less authentication algorithm, the authentication efficiency and security in the cross-domain authentication process of a variety of IoT applications are improved. The contributions of the proposed authentication scheme, DSP-CCAS, can be listed as follows:

- (1) A cross-domain access control authentication method based on certificate-less passwords supporting parameter differentiation is proposed

- (2) A specific implementation plan for cross-domain authentication was proposed, and its effectiveness was evaluated through a prototype system

The remainder of this paper is organized as follows. Section 2 highlights the state-of-the-art research in the area, Section 3 introduces the certificate-less signature algorithm for authentication, Section 4 describes the proposed DSP-CCAS in detail, Section 5 presents the performance evaluation results, and Section 6 finalizes the paper.

2. Related Works

Blockchain was first mentioned by Nakamoto in “Bitcoin: A peer-to-peer electronic cash system” [19] in 2008. Generally, a blockchain is defined as a specific data structure formed by combining data blocks in a chain in a chronological order and cryptographically ensuring that it cannot be tampered with and is unforgeable decentralized, trustless distributed sharing general ledger system. In view of the unique combination of attributes of blockchain, many fields have listed it as the primary development direction, such as financial technology [20], cross-border e-commerce [21], data sharing [22], and other fields. The blockchain also provides the PKI system with the transparency, revocability, and reliable transaction records of the certificate and eliminates the security attributes of the center failure node. At this stage, blockchain-based cross-domain authentication schemes can be divided into two categories, namely, the authentication model for deploying the PKI system on the blockchain and the cross-domain authentication scheme by building an interdomain consortium blockchain model.

2.1. PKI Authentication Model Based on Blockchain Technology. The use of blockchain technology to build a decentralized PKI eliminates the single point of failure caused using CA. If the CA certification node is destroyed, the entire certificate chain may be damaged [23]. Compared to the WoT-based PKI, blockchain-based PKI (PB-PKI) has more advantages. WoT-based PKI has a higher entry threshold and needs more workload to build a trusted network. In the blockchain-based PKI, the proof of web members is not needed between entities, so the workload of executing as network members is eliminated.

The core idea of the PKI system based on blockchain technology is to record user certificates through the public ledger. In 2014, MIT scholar Conner first proposed Certcoin [24]. The core idea of Certcoin is to maintain the public ledger of domain names and the related public keys. The process of account and certificate issuance is accessible by users, which can be queried. This process is to solve the issues related to the single point of failure and certificate management and maintenance in the traditional CA system. However, Certcoin’s operations (registration, update, and verification) are publicly published in the form of transactions through the blockchain. All actions performed using the public key can be traced to the identity owned by the public key by any entity viewing the ledger, so it does not apply to the scenario where the user’s identity privacy needs

to be protected. Based on this, Axon and Goldsmith [25] improved the Certcoin model and offered privacy-awareness to the PB-PKI models. This model provides an unlinkable short-term key update and user control mechanism, in which the identity of the user and the previously used public keys can be revealed by the user itself or through a consensus of the network and use offline keys and online keys for user privacy protection. Privacy protection reduces the risk of users' privacy information leakage.

Aiming at the reputability problem of the traditional credit system in the cloud network transaction architecture, Zhu and Fu [26] proposed a blockchain-based dynamic multicenter collaborative authentication model tailored to the B2B+B2C supply chain. For joint authentication of supply chain transaction behavior, this model uses multiple transaction entities as different authentication centers, which eliminates the problems of tampering with transaction records, fraudulent customers, and single points of failure that exist in the traditional single authentication center, and improves the provability and reliability of transaction behavior. Stability ensures high consistency, transparency, and authenticity of the transaction information.

Chen et al. [27] explore the ways of overcoming the unified trust service challenge of the national PKI via consensus. Furthermore, they applied some functions of the CA management to the blockchain and eventually proposed a blockchain-based revocation list (BCRL). The release cycle of the blockchain revocation list (BCRL) is much shorter than traditional and incremental CRL. The update cycle reaches ten seconds, effectively improving the security of certificate cross-domain verification and authentication. However, this solution consumes a lot of storage. For every thousand transactions (mainly the status of the certificate), a peer node consumes about 3.2 M, and a subscriber node consumes around 3.7 M storage cost, which is not suitable for a large number of nodes and access more frequent systems.

To easily detect malicious certificates when issued, Al-Bassam [28] proposed a decentralized and transparent PKI system by combining smart contracts and the Web-of-Trust model. The design of this model alleviates the verification of fine-grained attributes of another entity's identity (such as company name or domain name), realizing the trust transfer relationship between the identity and attributes of the entity.

2.2. Build a Cross-Domain Authentication Model for Consortium Blockchains. Zhou et al. [29] proposed a blockchain-based PKI interdomain authentication scheme and designed the trust model and the system architecture of the blockchain certificate authority CA (BCCA). The root CA that joins the consortium blockchain in the BCCA model was credible. As a VP, the root CA blockchain certificate was self-generated, and the hash value of the certificate was recorded in the blockchain, which was not easily tampered with as the trust certificate for each domain.

Wang et al. [30] propose a cross-domain authentication model based on consortium blockchain (BlockCAM) and an accompanying protocol. BlockCAM builds a decentralized

network with the root certificate authority as the verification node. Each block stores the hash value of the authorization certificate, and the verification process only needs to compare whether the user-provided hash value calculated by the certificate is consistent with the hash value stored in the blockchain. The authentication process omits the key encryption and decryption overhead, thereby improving authentication efficiency.

Liu et al. [31] proposed a consortium blockchain-based V2G network cross-administrative domain authentication scheme using the SM9 digital signature algorithm. To reduce the number of signatures and verifications in the scheme and improve the efficiency and scalability of the program, a hash algorithm is used in the digital identity verification process.

Given the frequent exchange of trust domain information and the inability of secure and efficient authentication between domains, Ma et al. [32] develop a blockchain-based cross-heterogeneous domain authentication scheme, where the consortium blockchain model consists of the blockchain domain proxy server in the IBC domain and the PKI domain blockchain certificate server. The cross-domain model designs cross-domain authentication protocols and reauthentication protocols. It reduces the computing, communication, and storage burden of the combined terminal; simplifies the reauthentication process; and realizes the safe and efficient communication between IBC and PKI. However, this cross-domain authentication scheme cannot address user identity and certificate update and revocation issues. Blockchain data will only increase and not decrease, which will cause waste of the entire system due to data storage.

Facing user privacy scenarios, Ma et al. [33] proposed a blockchain-based distributed key management architecture (BDKMA) to reduce latency by using fog computing and to achieve cross-domain access through multiple cloud-based blockchains.

Jia et al. [34] proposed a cross-domain authentication scheme for the IoT based on identity (IRBA). Innovated traditional authentication schemes include the IBC-based cross-domain authentication methods and threshold passwords and smart contract-based multidomain joint authorization mechanisms. By joint utilization of these methods, a decentralized cross-domain authentication model is realized. This model has greatly improved the cost of calculation and communication. However, this scheme uses complex bilinear pairing operations in the signature and verification process, and there is still room for improvement.

Shu et al. [35] described a two-tier system model for medical data sharing, in which medical records are stored outside the blockchain and shared in the blockchain. In this model, a blockchain-based MCP certificate-less set signature scheme is proposed by using the proposed multinotch hash function. The purpose is to realize the certification of relevant medical personnel, medical equipment, and medical applications; ensure the integrity of medical records; and support the safe storage and sharing of medical information. This scheme includes a cross domain authentication protocol (MCPSP). The proposed cross domain authentication protocol is based on elliptic curve, which has higher

computational efficiency and lower computational cost. However, this scheme has the same problems as the scheme proposed by Jia et al. and does not consider the different cryptographic system parameters (system master key) in different domains and the private key of secure channel transmission.

The existing data sharing systems based on consortium blockchain, they mainly use the certificate system or the bilinear pairing operation to complete the cross-security domain user access control, resulting in substantial management and calculation costs. Hence, lightweight cross-domain authentication schemes, suitable for frequent access in the IoT, still have a wide research space.

3. Certificate-Less Cross-Domain Signature Algorithm for Authentication

The certificate-less signature algorithm is of utmost importance to the cross-domain authentication scheme. When a user joins the data sharing system, it must be registered; when performing cross-domain access, the key steps of the signature algorithm are executed. First, users who apply for cross-domain, signing a request message with the registered private key. Then, the target security domain needs performing signature verification to verify the validity of the identity. When the verification is passed, verify the authority to complete the cross-domain identity authority authentication. The following details the proposed Certificate-less Cross-domain Signature Algorithm with Different System Parameters (DSP-CCSA) that supports parameter differentiation and discusses its correctness and security.

3.1. Procedure of the DSP-CCSA. DSP-CCSA mainly includes seven stages: setup, secret-value-set, partial-private-key-set, private-key-set, public-key-set, sign, and verify. Algorithm 1 shows the detailed process of DSP-CCSA.

The first five stages are performed during registration, where the last two are performed meanwhile execution. The registration is interactively executed by the authentication server and the device.

3.1.1. The Setup. First, the security parameter λ is used as the input, and the public system cryption parameter (CSP) of the Key Generation Center (KGC) is returned as follows:

- (1) Assume that there exists a root KGC, which calculates and creates a tuple $\{q, G\}$ according to λ , where G refers to an additive cyclic group and q denotes the order of group G . Then, choose 4 hash functions: $H_1 : \{0, 1\}^* \times G^2 \rightarrow Z_q^*$, $H_2 : G^3 \rightarrow Z_q^*$, $H_3 : G^2 \times (Z_q^*)^2 \rightarrow Z_q^*$, $H_4 : G^2 \rightarrow \{0, 1\}^*$
- (2) The KGC of each security domain generates a tuple $\{s_k, P_k\}$, where P_k is the generator of group G and $s_k \in Z_q^*$ is the master private key of KGC. KGCs in different security domains can generate different tuples $\{s_k, P_k\}$

- (3) The KGC of each security domain calculates its master public key $KC_k = s_k P_k$; each KGC publishes the system parameters $\{q, G, P_k, KC_k, H_1, H_2, H_3, H_4\}$ and secretly saves its master private key s_k

3.1.2. The Secret-Value-Set. A user UE_k whose identity information is ID_{UE_k} chooses a random secret value $x_{UE_k} \in Z_q^*$, calculates $PK_{UE_k} = x_{UE_k} \cdot P_k$, and sets x_{UE_k} as his secret value (where it is assumed that UE_k is a user in the security domain D_k and is connected to KGC in the domain k with system parameters P_k).

3.1.3. The Partial-Private-Key-Set. The algorithm uses the system cryption parameters, master private key, user identity, and public key of the KGC as the input and returns part of the private key for users in the domain.

- (1) The user equipment UE_k in the security domain D_k submits its identity information ID_{UE_k} and part of the public key PK_{UE_k}
- (2) After receiving the registration information sent by the user, KGC in the security domain D_k randomly selects $r_i \in Z_q^*$ and calculates $R_i = r_i KC_k$, $h_i = H_1(ID_i, R_i, PK_{UE_k})$.
- (3) KGC in the security domain D_k further calculates $s'_{UE_k} = r_i \cdot s_k \cdot h_i + H_1(ID_{UE_k}, R_i, s_k, PK_{UE_k})$ and sends $\{s'_{UE_k}, R_i\}$ to the user via the public channel

3.1.4. The Private-Key-Set. When the user receives the message $\{s'_{UE_k}, R_i\}$ returned by KGC in the security domain D_k , the user can calculate $sk_{UE_k} = s'_{UE_k} - H_1(ID_{UE_k}, R_i, x_{UE_k}, KC_k)$ to verify whether the message $\{s'_{UE_k}, R_i\}$ is valid and check whether the equation $sk_{UE_k} P_k = h_i R_i$ is true; if it is true, the user sets $\{sk_{UE_k}, x_{UE_k}\}$ as its complete private key. Suppose that the full private key of KGC is $sk_{KGC_k} = (x_k + r_k s_k h_k) \bmod q$.

3.1.5. The Public-Key-Set. Since the user UE_k in the security domain D_k sets $\{PK_{UE_k}, R_i\}$ as its complete public key, we consider $PK_{KGC_k} = sk_{KGC_k} P_k$ as KGC's complete public key.

3.1.6. Signs. If the user UE_1 in the security domain D_1 is aimed at using the service of the security domain D_2 , the UE_1 first sends an authentication request $\{\text{request}, PK_{UE_1}\}$ to the KGC_{D_2} in security domain D_2 .

After KGC_{D_2} receives the authentication request message, it will generate a random number $N \in Z_q^*$ and send a response message $\{N, PK_{UE_k}\}$ to the user device UE_1 .

In response to the KGC_{D_2} , the user equipment UE_1 performs the following calculations $U_1 = (N \cdot x_{UE_1}) P_2$, $T_1 = (N \cdot x_{UE_1}) PK_{KGC_2}$, $y_1 = H_2(U_1 || T_1 || PK_{KGC_2})$, $Q_1 = (N + y_1) P_1$, $V_1 = (y_1 \cdot sk_{UE_1})^{-1} (N + x_{UE_1} + y_1)$, $MID_1 = H_4(U_1 || T_1) \oplus (ID_1 || V_1 || C_1 || T_m)$. T_m is the current timestamp, sending a message $\{U_1, MID_1\}$ to KGC_{D_2} in the security domain D_2 .

```

1/*G refers to the additive cyclic group, and q denotes the order of group G
2{0, 1}^* × G^2 → Z_q^*, H2 : G^3 → Z_q^*,
3G^2 × (Z_q^*)^2 → Z_q^*, H4 : G^2 → {0, 1}^*
4 * /
5//Registration phase
6[Setup]:
7GenMP(k) → {q, G, H1, H2, H3, H4} // Generate main system parameters
8 Gen(G) → {s_k, P_k} //Each domain randomly generates its system parameters
9 {q, G, P_k, KC_k, H1, H2, H3, H4} → params // Release parameters
10[Secret-value-set]:
11 Gen(params) → x_{UE_i}
12[Partial-private-key-set]:
13 GenSk(params, ID_{UE_i}, PK_{UE_i}) → {sk'_{UE_i}, R_i}
14[Private-key-set]:
15 GenS_k(params, sk'_{UE_i}, R_i, ID_{UE_i}, x_{UE_i}) → {sk_{UE_i}, x_{UE_i}}
16[Public-key-set]:
17 GenP_k(x_i, R_i) → {PK_{UE_i}, R_i}
18//Execution phase
19[Sign]:
20 SigID(m, params, pk_{KGC}, P_2) → {U_i, MID_i}
21[Verify]:
22 Ver(U_i, MID_i, params, sk_{KGC}) → valid/invalid

```

ALGORITHM 1: DSP-CCSA.

3.1.7. *Verify.* When KGC_{D_2} in security domain D_2 receives the response message $\{U_1, MID_1\}$ from user UE_1 in security domain D_1 at time T_c , it performs the following operations:

- (1) Calculate $T'_1 = sk_{KGC_2} U_1, (ID_1 || V_1 || C_1 || T_m) = MID_1 \oplus H_4(U_1 || T'_1)$, if $T_c - T_m < \Delta t$, within the reauthentication time, pass the authentication directly, otherwise proceed to step (2).
- (2) Calculate $y'_1 = H_2(U_1 || T'_1 || PK_{KGC_2})$, $Q' = y'_1 h_1 V_1 R_1 - PK_{UE_1}$, $C'_1 = H_3(Q'_1 || y'_1 || V_1 || PK_{UE_1})$, if $C_1 \neq C'_1$, the authentication fails, otherwise, passes

3.2. *Correctness Analysis.* When the user in the security domain D_1 sends a signed message $\{U_1, MID_1\}$ to the KGC_{D_2} in the security domain D_2 , the KGC_{D_2} has to validate that the data is valid.

Proof. Because $T'_1 = sk_{KGC_2} U_1 = sk_{KGC_2} N \cdot x_{UE_1} P_2 = (N \cdot x_{UE_1}) PK_{KGC_2}$

$$\text{Thus, } y'_1 = H_2(U_1 || T'_1 || PK_{KGC_2}) = y_1$$

Thus

$$\begin{aligned} Q' &= y'_1 h_1 V_1 R_1 - PK_{UE_1} = y'_1 h_1 (y_1 \cdot sk_{UE_1})^{-1} (N + x_{UE_1} + y_1) R_1 - x_{UE_1} P_1 \\ &= y'_1 h_1 (y_1 r_1 s_1 h_1)^{-1} (N + x_{UE_1} + y_1) r_1 s_1 P_1 - x_{UE_1} P_1 \\ &= (N + x_{UE_1} + y_1) P_1 - x_{UE_1} P_1 = (N + y_1) P_1 = Q. \end{aligned}$$

(1)

$$\text{Thus, } C'_1 = H_3(Q'_1 || y'_1 || V_1 || PK_{UE_1}) = C_1. \quad \square$$

3.3. *Safety Analysis.* In this part, it is proved that the proposed DSP-CCSA is safe in the random prediction model. In DSP-CCSA, the communication entities originated from different security domains can employ different system parameters, CSP. Using different CSPs is safer than using the same CSP. The security of the proposed Certificate-less Cross-domain Signature Algorithm is affected by the difficulty of certain mathematical problems. To better understand the following security proof, a brief introduction to the mathematical assumptions is made firstly.

- (1) The elliptic curve discrete logarithm (ECDL) problem

The problem of ECDL calculates the integer value of $x \in Z_q^*$ for a prime q order additive cyclic group G by the setting $Q = xP$ ($P, Q \in G$). However, given P and Q , there are no known algorithms that can effectively determine x , and the use of brute force methods is computationally expensive; that is, assuming that the base point of the elliptic curve is known, it is impossible to find the discrete logarithm corresponding to a random element [36].

- (2) The Diffie-Hellman decision calculation problem (DCDH)

The problem of DCDH is to determine whether the equation $\xi = abP$ holds for a random instance (P, aP, bP, ξ) , where $a, b \in Z_q^*$ and $P \in G$. [37].

3.3.1. Security Analysis of Cross-Domain Authentication Protocol

- (1) The proposed cross-domain authentication scheme realizes the security of the cross-domain authentication protocol (CAP) against the adversary under the assumption of the DCDH problem

Type I adversary. This type of adversary A^{\wedge}_I is a dishonest user. We supposed that A^{\wedge}_I can acquire the public keys and secret values of KGC (AS) and group users. The public keys of KGC (AS) and user can be replaced by A^{\wedge}_I . A^{\wedge}_I can not acquire the master private key of KGC (AS).

Type II adversary. This type of adversary A^{\wedge}_{II} is modeled as a malicious KGC (AS). We supposed that A^{\wedge}_{II} can acquire the master private key of KGC (AS). The public keys of KGC (AS) and user cannot be replaced by A^{\wedge}_{II} .

Proof. Assume that C^{\wedge} is the challenger of the Diffie-Hellman decision calculation problem, and he has a living example of the DCDH problem (P, aP, bP, ξ) . If C^{\wedge} can distinguish $\xi = abP$, it can help the opponent $A^{\wedge}(A^{\wedge}_I \text{ or } A^{\wedge}_{II})$ by winning the next game to destroy the CAP security of the proposed DSP-CCSA [38]. \square

Initialization: C^{\wedge} chooses a random identity C_{ID} as the identity of the KGC, it wants to challenge. Afterward, C^{\wedge} creates the CSP and the pair of master private and public keys $(s \in Z_q^*, PK = sP)$ of the KGC. Then, the cryptographic system parameters and public key of the security domain are returned to the opponent A^{\wedge} , and the private key s is transferred to A^{\wedge}_{II} .

Probe: The below query is executed:

- (i) *Hash Query.* C^{\wedge} retains four lists $L_i (i = 1, 2, 3, 4)$, which represent the corresponding Hash query $H_i (i = 1, 2, 3, 4)$. All lists are empty when initialized. When A^{\wedge} submits the corresponding message m_j for H_i query, if there is a tuple $\{m_j, h_j\}$ in the corresponding hash list L_i , the corresponding hash value h_j will be returned. Otherwise, C^{\wedge} randomly selects a value $h_j \in H_i$ and stores it in the list L_i , and finally, C^{\wedge} returns h_j to A^{\wedge}
- (ii) *Secret Value Query.* C^{\wedge} retains a list L_s , empty at first, for secret value query. When A^{\wedge} enters the user identity information UID_i for query, if there is a record $\{UID_i, x_i, pk_i\}$ in the list L_s , then C^{\wedge} returns x_i . Otherwise, C^{\wedge} randomly selects a value $x_i \in Z_q^*$ and calculates $pk_i = x_i P$, and finally, C^{\wedge} stores $\{UID_i, x_i, pk_i\}$ in L_s and returns x_i to A^{\wedge}
- (iii) *Partial Private Key Query.* C^{\wedge} retains a list L_p , empty at first, for this query. When A^{\wedge} enters user identity information UID_i for this query (assuming that the secret value query is executed beforehand), if there are records $\{UID_i, sk_i, R_i\}$ in the list L_p ,

then C^{\wedge} returns sk_i . Otherwise, when A^{\wedge} is A^{\wedge}_I , C^{\wedge} randomly selects a value $r_i \in Z_q^*$ and then calculates $R_i = r_i \cdot pk_i$, $h_i = H_1(UID_i, R_i, pk_i)$, $sk_i = r_i \cdot h_i \cdot x_i \bmod q$. When A^{\wedge} is A^{\wedge}_{II} , C^{\wedge} randomly selects a value $r_i \in Z_q^*$ and then calculates $R_i = r_i \cdot PK$, $h_i = H_1(UID_i, R_i, pk_i)$, $sk_i = r_i \cdot h_i \cdot s \bmod q$. Finally, C^{\wedge} stores $\{UID_i, sk_i, R_i\}$ in L_p and returns sk_i

- (iv) *Private Key Query.* It is assumed that the secret value query and partial private key query have been queried before executing this query. When A^{\wedge} enters the user identity information UID_i for this query, C^{\wedge} returns the data $\{x_i, sk_i\}$ in the lists L_p and L_s . When A^{\wedge} enters KGC identity information C_{ID_j} for this query, C^{\wedge} updates the list L_r with the initial tuple $\{C_{ID_j}, \perp, bp\}$. If $C_{ID_j} = C_{ID}$, then C^{\wedge} returns “fail”; otherwise, C^{\wedge} randomly selects a value $sk_j \in Z_q^*$, then calculates $pk_j = sk_j P$, and then, C^{\wedge} returns sk_j . Finally, C^{\wedge} stores $\{C_{ID_j}, sk_j, pk_j\}$ into the list L_r
- (v) *Public Key Query.* When A^{\wedge}_I enters the tuple information $\{UID_i, x'_i, r'_i\}$ for this query, C^{\wedge} executes the secret value query and partial private key query by using $\{UID_i, x'_i, r'_i\}$, generate new values $\{sk'_i, pk'_i, R'_i\}$, and then use $\{UID_i, x'_i, pk'_i\}$ to query the corresponding result $\{UID_i, x_i, pk_i\}$ in L_s , use $\{UID_i, s, k'_i, R'_i\}$ to query the corresponding tuple $\{UID_i, sk_i, R_i\}$ in L_p , and return the query result. When A^{\wedge}_I enters the tuple information $\{C_{ID_j}, sk'_j\}$ to perform this query, if $C_{ID_j} = C_{ID}$, C^{\wedge} returns “fail”; otherwise, C^{\wedge} is performed by using $\{C_{ID_j}, sk'_j\}$ query the private key and generate a new pk'_j value. Finally, C^{\wedge} returns $\{C_{ID_j}, sk'_j, pk'_j\}$ the corresponding value $\{C_{ID_j}, sk_j, pk_j\}$ in the list L_r
- (vi) *Send Query.* When A^{\wedge} logs a query with a request message $\{m_s, C_{ID_j}\}$, C^{\wedge} first selects a random integer $\alpha \in \{1, 2, \dots, q_s\}$ (assuming that A^{\wedge} executes this query at most q_s times). If $C_{ID_j} = C_{ID}$ and $k = \alpha$, C^{\wedge} sets $U_i = U_\alpha = aP$. At the same time randomly selects a $MID_i = MID_\alpha \in \{0, 1\}^*$. Otherwise, C^{\wedge} executes the signature operation and generates the response message $\{U_i, MID_i\}$. Finally, C^{\wedge} returns $\{U_i, MID_i\}$
- (vii) *Test Query.* When A^{\wedge} logs a query with request message $\{C_{ID_j}, U_i, MID_i\}$, if $C_{ID_j} \neq C_{ID}$, $U_i \neq U_\alpha$, $MID_i \neq MID_\alpha$, C^{\wedge} declares “fail” or randomly picks a value $b \in \{0, 1\}$ to perform some operations: If $b = 1$, C^{\wedge} sets $T'_i = T_\alpha = \xi$, calculates $ID_i || V_i || C_i || T_{mi} = MID_i \oplus H_4(U_i || T'_i)$, $y'_i = H_2(U_i || T'_i || pk_{KGC})$, $Q'_i = y'_i h_i V_i R_i - pk_i$, $C'_i = H_3(Q'_i || y'_i || V_i || pk_i)$. Verify that whether $C'_i = C_i$ is established

Finally, A^\wedge returns a guess bit $b' \in \{0, 1\}$. If $b' = b$, then A^\wedge can destroy the CAP security of DSP-CCSA, because C^\wedge can crack the DCDH problem by discriminating $T_\alpha = \xi = abP$. However, it is accepted that there is not a known method to solve the DCDH problem in polynomial time. Therefore, the proposed certificate-less signature algorithm realizes CAP security against the adversary A^\wedge under the assumption of DCDH.

3.3.2. Security Analysis of Partial Private Key Transmission. In the proposed certificate-less cross-domain authentication algorithm, the KGC in the security domain D_k calculates the partial private key $sk'_{UE_k} = r_i \cdot s_k \cdot h_i + H_1(\text{ID}_{UE_k}, R_i, s_k, \text{PK}_{UE_k})$ of user UE_k . An attacker C^\wedge can obtain part of the private key sk'_{UE_k} transmitted on the public channel. However, under the assumption that the ECDL problem is difficult to solve, he does not have the master key s_k of the security domain D_k or the secret value of the user UE_k . It is impossible to calculate the user's real partial private key $sk_{UE_1} = r_i \cdot s_k \cdot h_i$, so DSP-CCSA is safe for partial private key public channel transmission.

3.3.3. Antireplay Attack. Whenever UE_i signs a specific message m , it selects a new timestamp T_m . If the attacker intercepts the interactive information $\langle U_i, \text{MID}_i = H_4(U_i || T_i) \oplus (\text{ID}_{UE_i} || V_i || C_i || T_m) \rangle$ and replies it to the KGC in the security domain D_k , by verifying the freshness of the timestamp T_m , the KGC can determine that is a reply message.

4. Certificate-Less Cross-Domain Authentication Scheme Supporting Parameter Differentiation

4.1. Scheme Model. The identity authentication process consists of two main stages: (i) authorization and (ii) authentication [39]. In the former, the security domain D_A validates the authenticity of the device identity in the domain. After passing the authenticity verification, the authorization is granted, and the smart contract is used to automatically obtain the authorization joint signature of the domain to be accessed and recorded in the blockchain. In the latter, mainly, the validity of the device identity and network access rights are checked. Considering these, this article introduces a Certificate-less Cross-domain Authentication Scheme with Different System Parameters (DSP-CCAS). The scheme model shown in Figure 1 has two aspects: (i) it uses the smart contract and consensus mechanism of blockchain to replace the trusted third-party authorization process, and (ii) it completes the cross-domain authentication process using the proposed DSP-CCAS algorithm.

In Figure 1, each dashed box represents a security domain, which represents a data sharing unit. The local domain authentication server (AS) plays the role of KGC and completes the authentication calculation of user identity and permission to access the domain. The APP server stores the actual shared data. And the terminal represents the user terminals in the IoT who want to obtain cross-domain authorization data. Ultimately, the consortium blockchain

is a consortium blockchain composed of authentication servers in each security domain that stores user permissions. Security domains A and B build a consortium relationship. When user X in security domain A requests data in security domain B , traditional RSA authentication is not used, but a self-authentication method is used. In this way, the authentication server of the security domain B can complete the authentication of the X identity without the authority of a trusted third party. Next, check whether the user authority record stored on the blockchain contains the authorization result for the user X ; if it exists, the authentication is successful; otherwise, the authentication fails. Compared with the centralized authentication model, decentralized authentication can guarantee the autonomy and initiative of the security domain. There is no need to rely on a third party to dynamically adjust the mutual trust relationship.

4.2. Authorization Mechanism

4.2.1. Smart Contract in Authorization Mechanism. Smart contracts mainly refer to general-purpose calculations performed on blockchains or distributed ledgers. They are composed of computer code and constitute a set of rules or conditions agreed by the parties. When these predefined rules or conditions are met, the smart contract will execute itself and provide output [40]. To request and publish cross-domain permissions, the following three types of smart contracts are used to implement a complete traceable, irreversible, and secure authorization process in a fully distributed environment without centralized trusted institutions.

- (i) *The Main Contract.* It accepts authorization requests and maintains a list of applications. The blockchain consists of only one master contract, and the blockchain address is known by all entities. The authentication server needs to use the master contract to establish a new authorization contract, obtaining cross-domain authorization
- (ii) *Authorization Contract.* A product of the main contract, which receives the authorization signature. It can be automatically executed in the blockchain to collect the permissions granted by each security domain to the user
- (iii) *Storage Contract.* It acts as the receiver of transactions containing authorized data and signatures

4.2.2. Cross-Domain Access Permission Acquisition. Figure 2 shows the authorization process when the device UE_1 belonging to the domain D_1 tries accessing the service of another domain.

The parameter descriptions are provided in Table 1.

Step 1. User UE_1 from domain D_1 applies for cross-domain access authorization. Then, he sends the application of cross-domain access authorization $\text{Sig}sk_{UE_1}(\text{Request})$ signed with his private key sk_{UE_1} to the local authentication server AS_1 .

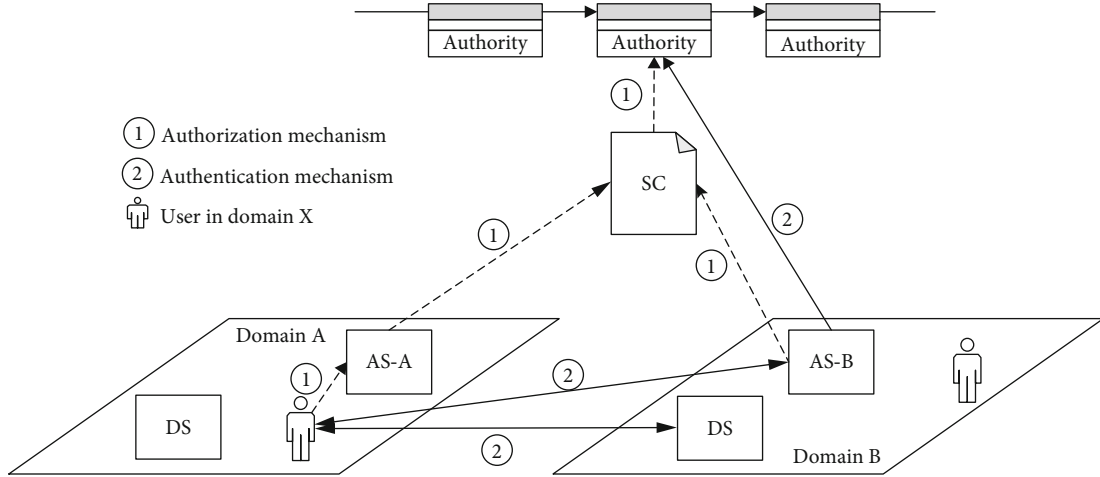


FIGURE 1: Scheme model.

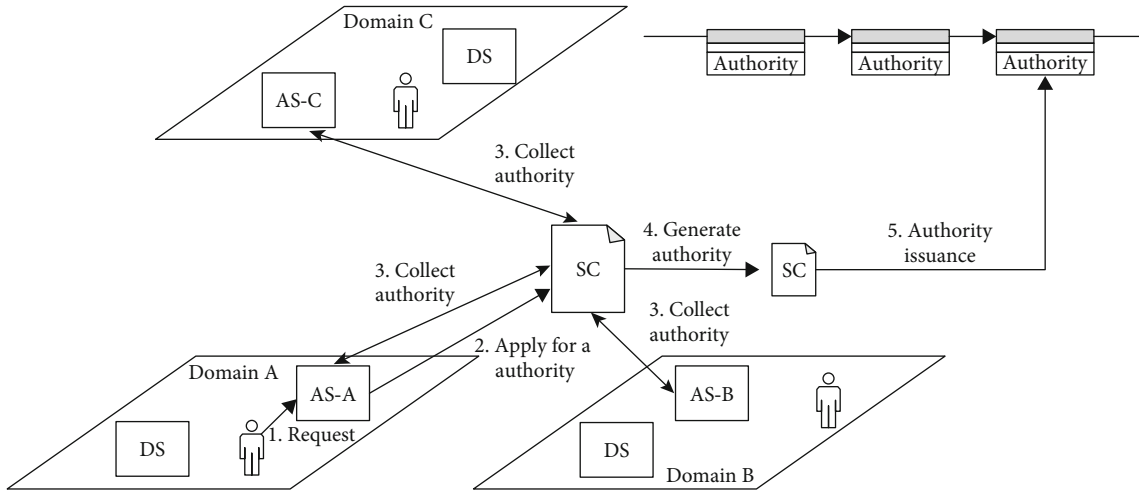


FIGURE 2: Authorization process for cross-domain access.

TABLE 1: Parameter descriptions.

Parameter	Description
UE_i	User in domain i
AS_i	Authentication server in domain i
$Sigs_k()$	Sign with the private key sk
PK_{UE_i}	The public key of UE_i
P_i	Generator in domain i
BC	Blockchain
SK_X	The private key of X
$Authority_i$	Authority of UE_i

Step 2. After AS_1 receives the cross-domain application from UE_1 in the same domain, it first uses the public key of UE_1 to verify the request message. After the verification is passed, AS_1 uses the master contract to create an authorization contract and specifies the AS_1 address of the security domain to be accessed to collect the signature.

Step 3. The authorization contract encrypts the authorization request with the public key of the identity authentication server in the designated security domain and then sends it to the identity authentication server of the corresponding security domain.

Step 4. The authorization contract collects user authority records and submits the collected user authority records to the storage contract.

Step 5. The storage contract stores the authorized transaction in the blockchain after packing it into a block.

4.3. The Cross-Domain Authentication Process. Now, let us assume that the user UE_1 in the security domain D_1 issues a cross-domain authentication request to AS_2 in the security domain D_2 as illustrated in Figure 3, and the protocol procedure is detailed afterward.

$$(1) UE_1 \longrightarrow AS_2 : \{Access\ Request, PK_{UE_1}\}$$

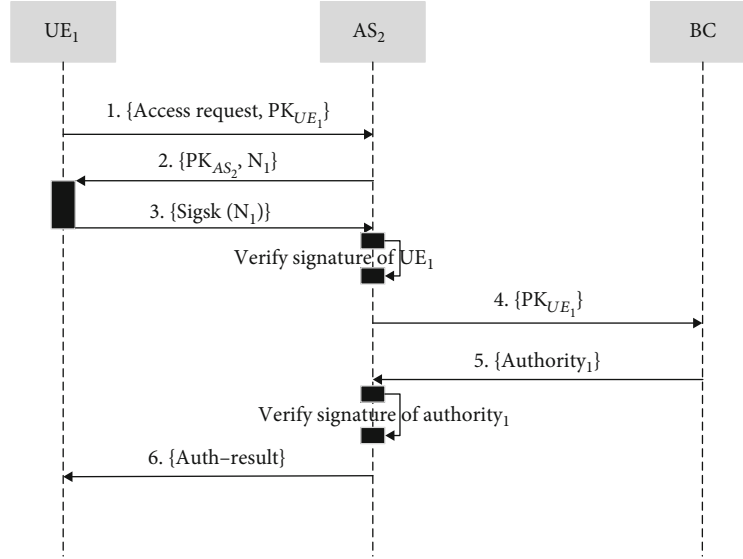


FIGURE 3: Cross-domain authentication process.

The user UE_1 in the security domain D_1 sends a request for cross-domain authentication to the user authentication server AS_2 in the security domain D_2 and sends the public key PK_{UE_1} required in the subsequent process together.

$$(2) AS_2 \longrightarrow UE_1 : \{PK_{AS_2}, N_1\}$$

After receiving the cross-domain authentication request from user UE_1 in the security domain D_1 , the authentication server AS_2 in the security domain D_2 sends the random number N_1 and the public key PK_{AS_2} of the security domain D_2 to the user UE_1 in the security domain D_1 . To complete the cross-domain authentication needs to support different system parameters.

$$(3) UE_1 \longrightarrow AS_2 : \{Sigs_{k_{UE_1}}(N_1)\}$$

- (i) After the user UE_1 in the security domain D_1 receives the response from the AS_2 in the security domain D_2 , it uses the private key SK_{UE_1} to generate the identity signature $Sigs_{k_{UE_1}}(N_1)$
- (ii) The user UE_1 in the security domain D_1 responds to the message of the authentication server AS_2 . Then, it sends the signature $Sigs_{k_{UE_1}}(N_1)$ of the random number N_1 to the authentication server AS_2 in the security domain D_2

$$(4) AS_2 \longrightarrow BC : \{PK_{UE_1}\}$$

- (i) The authentication server AS_2 in the security domain D_2 uses the public key PK_{UE_1} of user UE_1 in the security domain D_1 to verify the signed message $Sigs_{k_{UE_1}}(N_1)$
- (ii) After the verification is passed, the authentication server AS_2 queries the authorization result of UE_1 from the blockchain

$$(5) BC \longrightarrow AS_2 : \{Authority_1\}$$

If there is an authorization record of the security domain D_2 for the user UE_1 in the query record, the authentication is passed; otherwise, the authentication fails.

$$(6) AS_2 \longrightarrow UE_1 : \{Auth - result\}$$

The authentication server AS_2 in the security domain D_2 returns the authentication result of user UE_1 in the security domain D_1 .

5. Experiment and Result Analysis

5.1. Experimental Design

5.1.1. Experiment Environment. A simulation experiment platform was constructed to evaluate the performance of each program. The platform has ten authentication servers installed on a super ledger structure, which formed a consortium blockchain for a security domain. Each server performed cross-domain access authorization and device cross-domain access authentication. The authentication servers establish a structure-based permissioned blockchain. The servers can be set up as various node types, such as confirmation, endorsement, and authentication center nodes. They locally store the identity information of domain members, besides maintaining distributed ledgers and smart contracts. The ordering service deployment employs the Kafka model of fabric to ensure the reliability of the blockchain system, avoiding the single point of failure of the ordering node [41].

The simulation experiment was completed on a Linux server. The authentication server had an Intel-Core i5 6300 HQ CPU (2.30 GHz) with 16 GB memory and CentOS Linux 7.4 operating system. The blockchain platform is Hyperledger Fabric version v1.0, the experimental code writing language is Go, and the version is 1.15.1.

5.1.2. *Experimental Design.* The experimental design mainly compares the cross-domain authentication performance and authority processing performance of several blockchain-based certificate-less cross-domain authentication schemes.

(1) *Experiment 1: Authority Granting Processing Performance.* This experiment measures the processing performance of the DSP-CCAS authority granted and verifies whether the solution works well in the resource-constrained IoT data sharing environment. Considering the impact of the size of the security domain in the shared system on the authorization processing performance, the cross-domain access relationship is, respectively, established from 2 to 10 security domains. And the performance of authorized signature calculation is observed to change with the increase of the number of security domains. In other terms, first, the users in 2 security domains, then the users in 4 security domains, and finally the users in 10 security domains can access each other. To facilitate data statistics, a user with cross-domain access requirements is set in each security domain, and the abovementioned access process is performed to calculate the performance of the authorized signature calculation. Table 2 shows the relevant settings of the blockchain during the experiment.

(2) *Experiment 2: Authority Verification Processing Performance.* In this round of experiments, the processing performance of authorization verification between different numbers of security domains is evaluated, and the approximate time consumption of one authorization verification process is counted. It is validated that the proposed DSP-CCAS scheme is in the IoT massive data system, and the number of security domains continues to increase. Which can verify whether the proposed DSP-CCAS scheme can maintain efficient processing performance and high scalability, with the increase number of security domains in the massive data system of the Internet of Things. Taking the number of security domains T as a variable, where $T = \{2, 4, 6, 8, 10\}$, the test model is repeated a hundred times, and a hundred samples are averaged.

(3) *Experiment 3: Cross-Domain Authentication Processing Performance.* To validate the performance of the proposed DSP-CCAS cross-domain authentication processing, it includes identity signature time, signature verification time, authority verification time, and communication volume. Compare the proposed scheme (the certificate-less cross-domain authentication scheme DSP-CCAS that supports different system parameters) with the existing blockchain-based certificate-less cross-domain authentication schemes, including IRBA proposed by Jia et al. [34] and MCPSP proposed by Shu et al. [35]. From the comparison of the two indicators of computation time consuming and communication cost, three authentication schemes were loaded on the simulation experiment platform, and two security domains were selected for 100 cross-domain requests, and the average value was taken compare.

IRBA, a pairing-based cross-domain authentication scheme, can be simulated on the bilinear pair $e : G_1 \times G_2$

TABLE 2: Blockchain-related parameter settings.

Parameter	Value
Sorting algorithm	Kafka
Size of blockchain	50 transactions per block
Timeout of blockchain	2 seconds

TABLE 3: Parameter settings.

Parameter	Description	Size/bit
$ G_i $	Size of group G_1 and G_2	128
$ G $	Size of group G	40
$ ID $	Size of user's identity ID	64
$ N $	Size of random number N	32
$ T $	Size of timestamp	32
q	Size of the element in Z_q^*	20
m	Size of request or result	8

— G_2 . G_1 is the additive group of order q_1 generated on the A-type elliptic curve $E_1 : y^2 = x^3 + x \pmod{p_1}$, G_2 is the factorial group of q_1 generated by E_1 , and p_1 and q_1 are, respectively, 512-bit and 160-bit prime numbers. For the elliptic curve-based cross-domain authentication scheme (MCPSP and DSP-CCAS), the simulation can be performed on the nonsingular elliptic curve $E : y^2 = x^3 + ax + b \pmod{p_2}$. G is the additive group of order q_2 generated by E , where p_2 and q_2 are two 160-bit prime number. The aforementioned bilinear pair and elliptic curve constructed in the experiment are at the same 80-bit security level. As shown in Table 3, some basic parameter settings in the experiment are given.

5.2. Result Analysis

5.2.1. *Processing Performance Granted by Access Rights.* According to the design of experiment 1, the number of security domains T in the data sharing consortium blockchain is continuously adjusted, gradually increasing from $T = 2$ to $T = 10$, and the value of T is increased by 2 each time. That is, starting from 2 security domains, add 2 security domains each time until the number of security domains reaches 10. Through the log records, the average processing time of cross-domain access authorization in the proposed DSP-CCAS scheme and the influence of the number of security domains T on the performance (processing time/sec) of cross-domain access authorization are calculated. According to the statistical data, the results are illustrated in Figure 4.

Figure 4 shows that the time needed to issue authorization changes marginally with the number of data sharing security domains T for the proposed cross-domain authentication scheme (DSP-CCAS) that supports different system parameters. However, the authorization processing time is no more than five seconds, and the authorization duration is no more than three seconds in most cases, which accounts for 65%-72% of the test samples. According to the above data analysis, the proposed DSP-CCAS scheme has a higher performance in the processing of authorization.

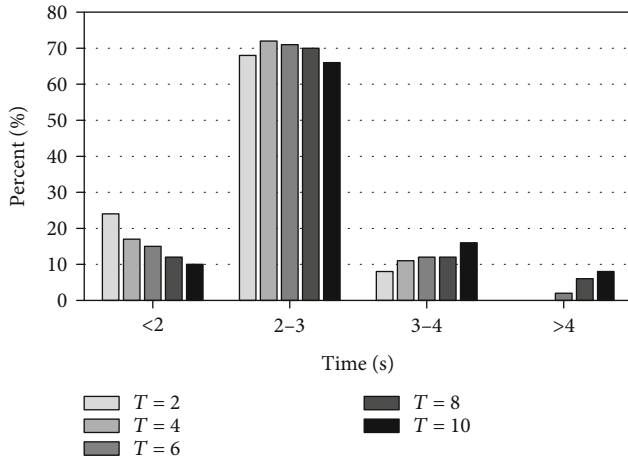


FIGURE 4: Authorization time allocation for different domain values (T).

5.2.2. *Processing Performance of the Authorization Verification.* Again, the number of security domains, i.e., the number of authentication servers T , is used as a variable to repeat the test model a hundred times, and a hundred samples are averaged. Figure 5 illustrates the results.

The experimental results showed that the verification time of DSP-CCAS does not dramatically vary with the change of threshold T and is stable at around 4.2 ms, which means that the proposed DSP-CCAS scheme has good scalability.

5.2.3. *Processing Performance of the Cross-Domain Authentication.* Calculation cost and communication cost are two important factors for evaluating certificate-less cross-domain authentication schemes. According to the design of experiment three, the computational and communication costs of the proposed scheme are compared with two recent blockchain-based certificate-less collective signature schemes, namely, IRBA and MCPSP. Since the registration phase, performance evaluation, and the running time of some lightweight operations minimally affect the overall system performance, they are ignored. Table 4 provides a comparison between the proposed and the related blockchain-based cross-domain authentication schemes in terms of computational cost.

Table 4 reveals that DSP-CCAS has a significant improvement in the calculation time of individual signature, individual verification, and authorization verification compared with the scheme IRBA. This is because the IRBA scheme uses a complex bilinear mapping in the calculation process. The proposed scheme DSP-CCAS and scheme MCPSP are all completed under the elliptic curve cryptosystem. Under the same security level, the elliptic curve cryptosystem is more effective than bilinear mapping. Therefore, the elliptic curve-based certificate-less cross-domain authentication scheme has the characteristics of low calculation, low storage, high reliability, privacy protection, and timeliness. And it is suitable for the sharing of massive data based on blockchain technology in the resource-constrained IoT environment. Compared with the scheme MCPSP based

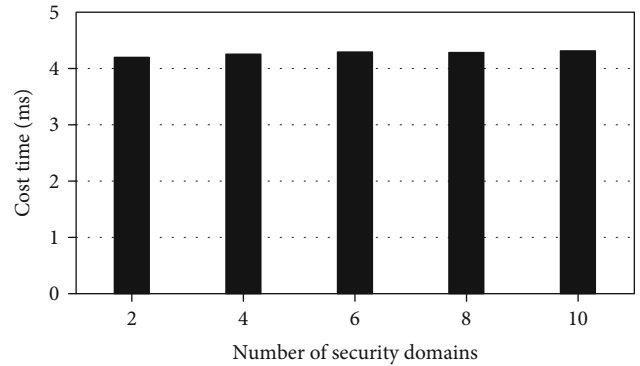


FIGURE 5: Permission verification time.

TABLE 4: Comparing calculation costs.

Program	Sign time/ms	Verify signature time/ms	Verify authority time/ms	Total time/ms
IRBA	24.124	8.972	6.627	39.768
MCPSP	2.165	6.534	5.424	14.123
DSP-CCAS	6.495	2.178	4.268	12.941

on the elliptic curve cryptosystem, the proposed scheme DSP-CCAS has a higher computational cost for personal signatures. Because in the scheme, MCPSP personal signatures only use 1 scalar multiplication, but to support different security domains with different system parameters, DSP-CCAS requires 3 scalar multiplications when signing. However, in individual signature verification and authorization verification, DSP-CCAS is better than the scheme MCPSP. This is because, in the verification phase, the scheme MCPSP requires 3 scalar multiplications and 3 scalar additions on the elliptic curve, while DSP-CCAS only needs 1 scalar multiplication and 1 scalar addition to reduce 2 scalar multiplications and 2 scalar addition operations. In terms of overall authentication calculation time (verify signature time + verify authority time), the proposed scheme is significantly better than the related cross-domain authentication schemes IRBA and MCPSP based on blockchain technology, which only takes 6.446 ms. Figure 6 presents the comparison of the proposed DSP-CCAS with IRBA and MCPSP in terms of cross-domain identity authentication performance.

Compared with IRBA that uses complex bilinear pairing operations, the proposed DSP-CCAS scheme has greatly improved performance at all stages. It not only decreases the signature time by 73.07% but reduces the signature verification time by 75.72%. The authorization verification time also reduced by 35.6%. Even the overall authentication time is decreased by 67.46%. As for comparing with the MCPSP scheme that is the same as based on the nonsingular elliptic curve, although the signature time of DSP-CCAS is 66.67% longer than it, we greatly shorten the signature verification time and authority verification time, which are decreased 66.67% and 21.31%. Respectively, the overall cost of verification time has reduced by 8.37%. It is a significant improvement. From the above analysis, it can be seen that,

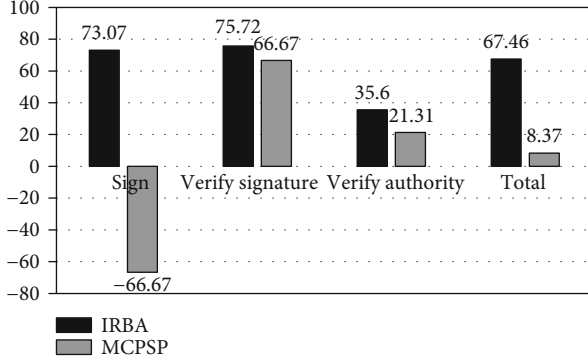


FIGURE 6: Comparison of the time of each stage of certification.

TABLE 5: Communication cost of blockchain-based solutions.

Program	Communication volume/bit
IRBA	Request+2 ID +N+2(2 G ₁ +2 G ₁) + result = 8 + 2 * 64 + 32 + 2(2 * 128 + 2 * 128) + 8 =1200
MCPSP	Request+2 ID +2 G +N+2(G +2q) + result = 8 + 2 * 64 + 2 * 40 + 20 + 2(40 + 2 * 20) + 8 =404
DSP-CCAS	Request+4 G +N+2(G +2q)+2 ID +result = 8 + 4 * 40 + 20 + 2(40 + 2 * 20) + 2 * 64 + 8 =484

compared with these schemes, the identity authentication process of the proposed scheme requires less calculation time.

DSP-CCAS uses the same password parameter value as MCPSP. The details are shown in Table 3. As shown in the process described in Figure 3, in the cross-domain request application phase, IRBA directly uses the identity as the public key. However, the public keys of the DSP-CCAS and MCPSP schemes consist of the user-calculated part of the public key and the part of the public key generated by KGC. To prevent replay attacks, the authentication server specifies a random number N during authentication. The user signs N and returns the signature and N to the authentication server. Once the identity authentication is passed, the authentication server uses the user ID for requesting the cross-domain authority of the user from the blockchain. This is a signature of the same user with the same aggregate signature size.

Table 5 presents the total communication cost of the above-analyzed schemes. As seen, IRBA needs 1200 bit, MCPSP needs 404 bit, and DSP-CCAS proposed in this paper needs 484 bit. Obviously, the proposed DSP-CCAS is significantly better than the IRBA communication cost in terms of communication cost, which is mainly affected by the security requirements of the algorithm itself. Under the same security level, the algorithm based on bilinear pairing requires a larger group size. And DSP-CCAS is slightly higher than the communication cost of MCPSP. This is because MCPSP is the same as IRBA, can only use the same parameters between security domains, and part of the pri-

vate key is transmitted must through a dedicated security channel. However, unlike them, the scheme DSP-CAAS proposed in this paper (1) supports parameter differentiation of different systems. Although a certain communication cost has been added for this, the autonomy, privacy, and security of each security domain have been greatly improved. Each security domain can independently control the settings of its own authentication system security parameters without negotiating with other systems and share system security parameters. Moreover, the increased overhead is at an acceptable level. (2) Support the partial private keys to be transmitted through public channels. There is no need to build a dedicated transmission channel for partial private key transmission, and an open network can be used, such as a mobile data network, which reduces construction and operation and maintenance costs.

6. Conclusions

This article introduces a certificate-less cross-domain authentication scheme that supports parameter differentiation by improving the certificate-less signature algorithm. Through theoretical analysis and security classification, the correctness of the scheme is proved, and it can support different security domains using different master private key/master public key pairs and supports a , which enhances the security of cross-domain authentication. Through comparative experiments, it is found that the overall verification time reaches 6.446 milliseconds, compared to the IRBA and MCPSP, in the case of cross-domain request access. That addressed the authority authentication issue in the current certificate-free cross-domain authentication scheme based on blockchain technology. The cost of one-time authentication communication is only 484 bits, which can meet the resource-constrained IoT data sharing environment.

Regarding the proposed scheme enabling blockchain-based massive data sharing, how to further reduce communication costs and design cross-domain authentication between heterogeneous domains that support different cryptosystems is worthy of further study in the future.

Data Availability

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

Conflicts of Interest

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

Acknowledgments

This work was supported by the National Natural Science Foundation of China (grant numbers 61802086 and U20B2048), the Defense Industrial Technology Development Program (grant number 2020604B004), the Heilongjiang Provincial Natural Science Foundation of China (grant number LH2021F016), and the Fundamental

Research Funds for the Central Universities (grant number 3072021CF0608).

References

- [1] J. Ding, T. R. Tang, Y. Zhang, and W. Chi, "Using intelligent ontology technology to extract knowledge from successful project in IoT enterprise systems," *Enterprise Information Systems*, pp. 1–27, 2021.
- [2] S. Qu, L. Zhao, and Z. Xiong, "Cross-layer congestion control of wireless sensor networks based on fuzzy sliding mode control," *Neural Computing and Applications*, vol. 32, no. 17, pp. 13505–13520, 2020.
- [3] K.-H. Wang, C.-M. Chen, W. Fang, and T. Y. Wu, "On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags," *The Journal of Supercomputing*, vol. 74, no. 1, pp. 65–70, 2018.
- [4] C.-M. Chen, B. Xiang, Y. Liu, and K. H. Wang, "A secure authentication protocol for Internet of Vehicles," *IEEE Access*, vol. 7, pp. 12047–12057, 2019.
- [5] E. K. Wang, J. Chen, Y. Peng, and L. Zhang, "Editorial: physical layer security and wireless access control (QSHINE 2017)," *Mobile Networks and Applications*, vol. 25, no. 1, pp. 1–3, 2020.
- [6] K. Qiao, W. You, L. Wang, and H. Tang, "Data sharing scheme for 5G IoT based on blockchain," *Chinese Journal of Network and Information Security*, vol. 6, no. 4, pp. 45–55, 2020.
- [7] M. A. Khan and K. Salah, "IoT security: review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.
- [8] C. Wang, D. Wang, G. Xu, and D. He, "Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0," *Science China: Information Sciences*, vol. 65, pp. 1–15, 2022.
- [9] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, 2017.
- [10] S. Underwood, "Blockchain beyond bitcoin," *Communications of the ACM*, vol. 59, no. 11, pp. 15–17, 2016.
- [11] Y. Qian, Y. Jiang, J. Chen et al., "Towards decentralized IoT security enhancement: a blockchain approach," *Computers & Electrical Engineering*, vol. 72, pp. 266–273, 2018.
- [12] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet of Things*, vol. 1-2, no. 2, pp. 1–13, 2018.
- [13] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: the case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 618–623, Kona, HI, USA, 2018.
- [14] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: a lightweight scalable blockchain for IoT security and anonymity," *Journal of Parallel and Distributed Computing*, vol. 134, pp. 180–197, 2019.
- [15] Z. Li, D. Wang, and E. Morais, "Quantum-safe round-optimal password authentication for mobile devices," *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2020.
- [16] R. Reisman, "Blockchain serverless public/private key infrastructure for ADS-B security, authentication, and privacy," in *AIAA Scitech 2019 Forum*, American Institute of Aeronautics and Astronautics, San Diego, California, 2019.
- [17] D. Li, W. Peng, W. Deng, and F. Gai, "A blockchain-based authentication and security mechanism for IoT," in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–6, Hangzhou, China, 2018.
- [18] J. Wang, L. Wu, K. K. R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1984–1992, 2020.
- [19] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Consultcd, 2008.
- [20] H. U. A. N. G. Wei, "Potential risk and model construction of blockchain technology applied to derivatives market," *Financial Regulation Research*, vol. 2, pp. 97–111, 2019.
- [21] Y. Yu, C. Taowei, and Z. Kun, "Data exchange model and application of certificate of origin based on blockchain technology," *E-Business Journal*, vol. 3, pp. 53–55, 2018.
- [22] L. Yue, H. Junqin, Q. Shengzhi, and W. Ruijin, "Big data model of security sharing based on blockchain," in *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)*, pp. 117–121, Chengdu, China, 2017.
- [23] C. Ellison and B. Schneier, "Ten risks of PKI: what you're not being told about public key infrastructure," *Computer Security Journal*, vol. 16, no. 1, pp. 1–7, 2000.
- [24] C. Fromknecht, D. Velicanu, and S. Yakoubov, *Certcoin: A Namecoin Based Decentralized Authentication System 6.857 Class Project*, Unpublished class project, 2014.
- [25] L. Axon and M. Goldsmith, "PB-PKI: a privacy-aware blockchain-based PKI," in *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications*, pp. 311–318, Madrid, 2017, SCITEPRESS - Science and Technology Publications.
- [26] Z. H. U. Jian-ming and F. U. Yong-gui, "Supply chain dynamic multi-center coordination authentication model based on block chain," *Chinese Journal of Network and Information Security*, vol. 2, no. 1, pp. 27–33, 2016.
- [27] Y. Chen, G. Dong, J. Bai, Y. Hao, F. Li, and H. Peng, "Trust enhancement scheme for cross domain authentication of PKI system," in *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pp. 103–110, Guilin, China, 2019.
- [28] M. Al-Bassam, "SCPki: a smart contract-based PKI and identity system," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, pp. 35–40, New York, NY, USA, 2017.
- [29] Z. Zhicheng, L. Lixin, and L. Zuohui, "Efficient cross-domain authentication scheme based on blockchain technology," *Journal of Computer Applications*, vol. 38, no. 2, pp. 316–320+326, 2018.
- [30] W. Wang, N. Hu, and X. Liu, "BlockCAM: a blockchain-based cross-domain authentication model," in *2018 IEEE Third International Conference on Data Science in Cyberspace (DSC)*, pp. 896–901, Guangzhou, China, 2018.
- [31] D. Liu, D. Li, X. Liu, L. Ma, H. Yu, and H. Zhang, "Research on a cross-domain authentication scheme based on consortium blockchain in V2G networks of smart grid," in *2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pp. 1–5, Beijing, China, 2018.
- [32] M. Xiao-ting, M. Wen-ping, and L. Xiao-xue, "A cross domain authentication scheme based on blockchain technology," *Acta Electronica Sinica*, vol. 46, no. 11, pp. 2571–2579, 2018.
- [33] M. Ma, G. Shi, and F. Li, "Privacy-oriented blockchain-based distributed key management architecture for hierarchical

- access control in the IoT scenario,” *IEEE Access*, vol. 7, pp. 34045–34059, 2019.
- [34] X. Jia, N. Hu, S. Su et al., “IRBA: an identity-based cross-domain authentication scheme for the Internet of Things,” *Electronics*, vol. 9, no. 4, p. 634, 2020.
- [35] H. Shu, P. Qi, Y. Huang, F. Chen, D. Xie, and L. Sun, “An efficient certificateless aggregate signature scheme for blockchain-based medical cyber physical systems,” *Sensors*, vol. 20, no. 5, p. 1521, 2020.
- [36] A. Meneghetti, M. Sala, and D. Taufer, “A new ECDLP-based PoW model,” *Mathematics*, vol. 8, no. 8, article 1344, 2020.
- [37] Y. X. Yan, L. Wu, W. Y. Xu, H. Wang, and Z. M. Liu, “Integrity audit of shared cloud data with identity tracking,” *Security and Communication Networks*, vol. 2019, Article ID 1354346, 11 pages, 2019.
- [38] S. Qiu, D. Wang, G. Xu, and S. Kumari, “Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices,” *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2020.
- [39] X. Jiang, F. R. Yu, T. Song, Z. Ma, Y. Song, and D. Zhu, “Blockchain-enabled cross-domain object detection for autonomous driving: a model sharing approach,” *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3681–3692, 2020.
- [40] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F. Y. Wang, “An overview of smart contract: architecture, applications, and future trends,” in *2018 IEEE Intelligent Vehicles Symposium (IV)*, pp. 108–113, Changshu, China, 2018.
- [41] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, “A blockchain-based medical data sharing and protection scheme,” *IEEE Access*, vol. 7, pp. 118943–118953, 2019.

Research Article

A Secure and Efficient Lightweight Vehicle Group Authentication Protocol in 5G Networks

Junfeng Miao , Zhaoshun Wang , Xue Miao , and Longyue Xing 

The School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China

Correspondence should be addressed to Zhaoshun Wang; zhswang@sohu.com

Received 3 July 2021; Accepted 13 August 2021; Published 22 September 2021

Academic Editor: Weizhi Meng

Copyright © 2021 Junfeng Miao 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 mobile network enters 5G era, 5G networks have a series of unparalleled advantages. Therefore, the application of 5G network technology in the Internet of Vehicles (IoV) can promote more intelligently vehicular networks and more efficiently vehicular information transmission. However, with the combination of 5G networks and vehicular networks technology, it requires safe and reliable authentication and low computation overhead. Therefore, it is a challenge to achieve such low latency, security, and high mobility. In this paper, we propose a secure and efficient lightweight authentication protocol for vehicle group. The scheme is based on the extended chaotic map to achieve authentication, and the Chinese remainder theorem distributes group keys. Scyther is used to verify the security of the scheme, and the verification results show that the security of the scheme can be guaranteed. In addition, through security analysis, the scheme can not only effectively resist various attacks but also guarantee security requirements such as anonymity and unlinkability. Finally, by performance analysis and comparison, our scheme has less computation and communication overhead.

1. Introduction

It is an inevitable trend that all things are connected. With the development of the IoV, vehicular networks are becoming more and more important in modern life [1]. By the continuous increase of motor vehicles, road traffic has become gradual complex, which results in higher requirements for the IoV [2, 3]. As mobile cellular networks rapidly develop, 5G networks have officially entered our lives. Due to the characteristics of 5G networks (high speed, low latency, high reliability, and wide coverage) and the newly concomitant technologies (millimeter wave communication, MIMO, D2D, etc.), it greatly improves the mobile Internet field of IoV [4–6]. Supporting Internet of Vehicles services through 5G network technology can overcome the limitations of current IoV. Recently, more attention is paid on the integration of 5G technology and the IoV [7].

The deepening application of 5G technology provides a strong guarantee for the vehicular networks. The current research of vehicular networks focuses on driving safety, improving the traffic efficiency of vehicles, ensuring the safe and efficient communication between vehicle and vehicle

(V2V) and vehicle and roadside infrastructure (V2I), and realizing the vehicle safety applications such as emergency braking warning [2]. This can effectively avoid vehicle collisions or reduce the personal injury caused by traffic accidents. Vehicular network communication mainly relies on Cellular Vehicle to Everything (C-V2X) [8]. Through the communication among vehicle to vehicle, vehicle to person, vehicle to infrastructure, and vehicle to network, it can ensure the driving safety and comfort and drive the realization of automatic driving. C-V2X includes two standards: Long-Term Evolution Vehicle to Everything (LTE-V2X) and 5G Vehicle to Everything (5G-V2X). Compared with the two standards, the performance of 5G-V2X is better than that of LTE-V2X [9]. LTE-V2X has insufficient delay and reliability, while 5G-V2X has the advantages of long coverage time, low delay and high reliability. It can obtain various state information of the road timely and accurately, interact with each other in real time, and complete the driving task better. It is the key technology of the future of the Internet of vehicles application, especially the autonomous driving and overtake, which require very low network latency [10]. At the same time, as a kind of ultrareliable and low-latency

communications (URLLC), it requires safe and reliable authentication and low computation overhead [11, 12]. Therefore, a better solution is to use group key agreement (GKA) in vehicle group [13]. In this way, the vehicle group communicate safely. So, our paper mainly studies the key agreement scheme between groups in the Internet of Vehicles under the 5G networks. In addition, due to the openness of the wireless channel, the signal exposed in the open environment is likely to be stolen, interfered, or even modified by the attacker, which brings adverse effects to the vehicular networks [14–17].

This paper proposes a vehicle group authentication protocol based on extended chaotic mapping in 5G networks. This solution enables the participating vehicles to communicate securely through the group key in the 5G networks. Therefore, this paper mainly does the following work:

- (1) This paper proposes a vehicle group authentication scheme under the 5G network architecture. In order to protect the security of RSU, the shared key will be updated. In addition, this scheme is a lightweight authentication scheme based on extended chaotic mapping and distributes group key through Chinese remainder theorem
- (2) This paper verifies the security of the scheme by using the Scyther tool
- (3) By comparing the existing schemes, this scheme can effectively reduce the computation and communication overhead

Other parts of this paper are as follows. Section 2 reviews the related research work of this paper. Section 3 introduces the preliminary knowledge of this paper. Section 4 introduce a lightweight and secure vehicle group authentication protocol in detail. We carried out security and performance analysis, respectively, in Sections 5 and 6. Finally, Section 7 summarizes the full paper.

2. Related Work

At present, in order to solve the problems faced by vehicular networks, the scholars have proposed many authentication schemes for vehicular networks. The following mainly introduces from three aspects: group signature authentication, group key agreement, and based on trusted authority.

First, we introduce the authentication protocol based on group signature. In 2011, Huang et al. [18] proposed an anonymous batch identity authentication and key agreement protocol in the Internet of Vehicles. The scheme could not only authenticate request messages from multiple vehicles but also carry out key agreement. Cui et al. [19] proposed a solution based on software without relying on any special hardware. In the batch verification stage, it adopted cuckoo filtering and binary search methods, which achieved a higher success rate than previous solutions. Vijayakumar et al. [20] proposed a privacy preserving anonymity scheme with high computational efficiency. At the same time, an efficient anonymous batch authentication protocol was introduced

to authenticate multiple vehicles on the road of the Internet of Things, which reduced the authentication time and was more efficient in certificate and signature verification. These schemes can complete the certification of vehicle group. However, these schemes will bring higher verification costs, thereby affecting the performance of the schemes.

Next, we introduce the related group key agreement. In 2016, Han et al. [21] established an efficient group authentication scheme by adopting a self-certification without certification authority. The scheme could set up groups between roadside units and vehicles. In [22], Vijayakumar et al. proposed a dual group key scheme, which distributed the group keys to each vehicle and ensured that the group keys were updated. In [23], Vijayakumar et al. proposed an effective anonymous group key distribution protocol, which can safely distribute the group key to the vehicle group. The RSU can use the group key to send location-based information to the vehicle group in a secure way. In 2018, Cui et al. [24] proposed a conditional privacy preserving authentication scheme based on hash function. The scheme distributed group keys through the mechanism of the Chinese remainder theorem (CRT) and provided update mechanism for vehicles to join and leave. Zhang et al. [25] proposed an identity authentication scheme based on the Chinese remainder theorem (CRT). This scheme avoided the use of bilinear pairing operations and solved the leakage problem of side channel attacks, and both safety and performance were guaranteed. In [26], Lai et al. proposed a lightweight group access authentication scheme based on message authentication code aggregation technology, which could resist DoS attacks. In 2019, Zhang et al. [27] proposed a group key agreement protocol, in which directional attribute layering was used. Shi et al. [28] proposed a password-based conditional confidentiality authentication and group key generation protocol. The protocol provided the generation of group keys, and the calculation and communication overheads were small. In 2020, Gharsallah et al. [29] proposed a scheme to authenticate a group of vehicles in 5G networks. The protocol supported group authentication of vehicle equipment in 3GPP network. Cui et al. [13] proposed a session key agreement scheme based on chaotic mapping. In this scheme, the fog server was introduced, and the chaotic mapping algorithm was used for group key agreement between vehicles. In this group, vehicles could communicate with each other through group key. Zhang et al. [30] proposed a privacy preserving authentication framework based on edge technology in 5G-enabled vehicular networks. In this scheme, edge computing was used to calculate and verify on vehicles, so as to achieve the communication between vehicles. Ouaisa et al. [31] proposed an authentication protocol for a large number of vehicle equipment following 5G-AKA authentication framework. The protocol used ECDH algorithm to establish the key and authenticate the identity, which ensured the information security and integrity. Although the scheme could resist a variety of attacks, the computation overhead was relatively large. Although these schemes reduced the cost of verification, some schemes had a large computation and communication overhead, which affected the performance of the schemes.

Thirdly, we introduce the authentication protocol based on trusted authority. Azees et al. [32] proposed an effective anonymous authentication scheme. The scheme provided a conditional tracking mechanism to prevent malicious vehicles from entering the VANET. Zhang et al. [33] proposed a many-to-many authentication and key agreement scheme for security authentication between multiple vehicles and CSP. Under the premise of information leakage, this scheme could prevent illegal access and provide key security. In 2019, Cui et al. [34] proposed a lightweight authentication protocol based on reputation system for 5G-enabled vehicular networks. The authority was responsible for reputation management, and vehicles with low reputation score could not participate in communication, which significantly reduces the possibility of untrusted vehicles entering IoV. Huang et al. [35] proposed a new privacy preserving authentication scheme based on 5G software-defined vehicular networks. This scheme uses 5G software to define the advantages of the network, so that the vehicle certification process will only need light-weighted hash operation, thus greatly reducing the computation overhead. Li et al. [36] proposed a lightweight authentication scheme. In this scheme, only hash function and XOR operations are used to realize vehicle identity authentication and anonymity. Wang et al. [37] proposed a lightweight authentication protocol that could avoid emergency vehicles in VANET. After the first authentication with the nearest roadside unit, the scheme could complete the mutual authentication with the subsequent roadside unit without repeating the cumbersome calculation. Although these schemes can resist various attacks and ensure the safety of vehicles, they are not suitable for vehicle group authentication, and some schemes have relatively large computation overhead.

3. Preliminaries

3.1. System Model. This paper mainly studies the vehicle communication in the same RSU range in V2V communication. As shown in Figure 1, the specific system model includes the following communication entities.

5G core (5GC): 5GC controls the entire 5G-V2X network and provides mobile data connection and services. 5GC is divided into access and mobility management function (AMF), security anchor function (SEAF), authentication server function (AUSF), authentication credential repository and processing function (ARPF), and unified data management (UDM) [38]. AMF is responsible for handling connection and mobility management tasks. SEAF is used for authentication and communication. AUSF performs identity verification. ARPF calculates authentication data and keys. UDM carries functions related to data management. According to literature [38], UDM should be protected from physical attacks. In addition, in order to ensure the security of vehicle identity, the security is provided and insured by technical and legal [39]. In order to simplify the certification process and facilitate research, they are collectively referred to as 5GC.

Trusted authority (TA): TA is a completely trusted public organization, which is mainly responsible for system ini-

tialization, generation of public parameters, and registration for other entities participating in communication. In the registration stage, TA generates the pseudonym of the vehicle, then records the real identity of the vehicle, and shares the data with 5GC through the secure channel [29]. When a malicious vehicle is found, the 5GC can directly identify the opponent by searching for the malicious vehicle.

Roadside unit (RSU): RSU is an important communication entity in the system. It acts as a roadside unit to communicate with the vehicle in real time.

Vehicles: Each vehicle has an on-board unit (OBU), and each OBU has an antitampering device to protect secret information. It is responsible for collecting relevant information and transmitting other vehicles and RSU.

3.2. Security Requirements. The main goal of this article is to design a lightweight, safe, and effective vehicle group communication solution in the 5G networks to ensure the safe communication of the vehicular networks. Therefore, here are the security requirements to be met [13, 29–31, 34–37, 40–45].

- (1) **Anonymity:** the true identity of the vehicle must not be disclosed to any organization or user other than the authority and 5GC. To ensure that the attacker cannot obtain the true identity of the vehicle from the transmitted data, the vehicles participating in the communication should use fake identities
- (2) **Message authentication and integrity:** in the process of vehicle communication, the authenticity and integrity of the transmitted data should be guaranteed. The receiver can confirm that the received content is a true and complete message by authenticating the sender, rather than a message forged or modified by others
- (3) **Traceability:** when there is a malicious vehicle that releases false information, the authority can quickly trace the real identity of the malicious vehicle and broadcast its real identity to the outside world
- (4) **Unlinkability:** the attacker cannot link different messages of the same vehicle through intercepted transmission data.
- (5) **Common attack resistance:** it can resist common attacks such as replay attacks, man-in-the-middle attacks, and modification attacks in the Internet of Vehicles

3.3. Chebyshev Chaotic Mapping. Bergamo et al. [46] clearly proposed that public-key cryptographic algorithms designed based on the semigroup characteristics of Chebyshev polynomial did not satisfy security. Therefore, the solution in this paper adopts the more secure extended Chebyshev polynomial proposed by Zhang [47], which is defined as follows:

Definition 1. Let n be a positive integer, $x \in (-\infty, +\infty)$, n -order Chebyshev polynomial is defined as:

$$T_n(x) = \cos(n \arccos(x)) \pmod{P}. \quad (1)$$

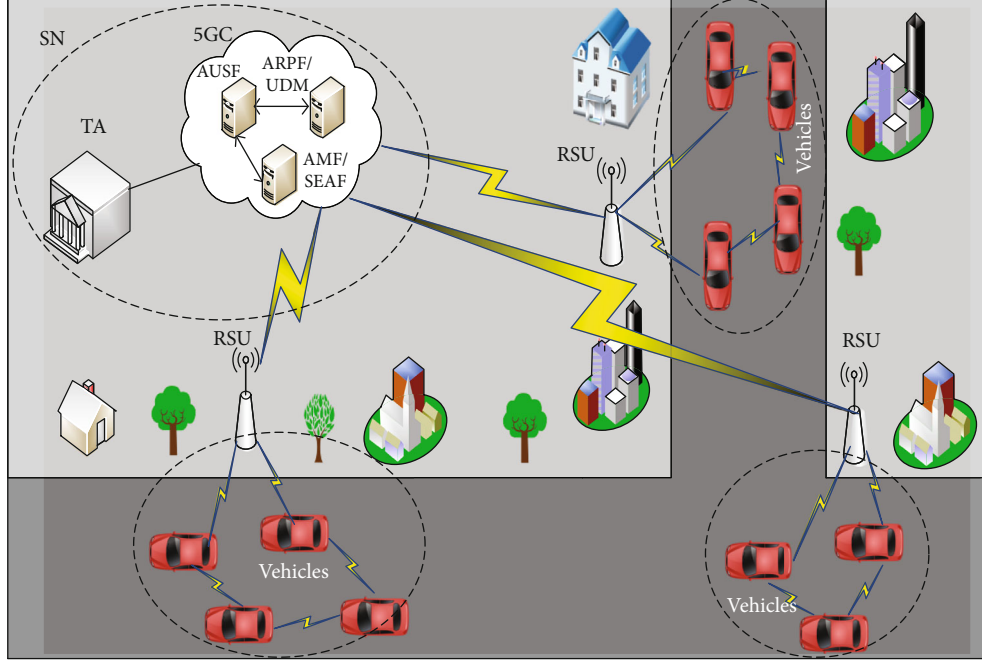


FIGURE 1: System model.

The iterative relation of Chebyshev polynomial is as follows:

$$T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x)) \bmod P, \quad (2)$$

where $T_0(x) = 1$, $T_1(x) = x \bmod P$, $n \geq 2$, and P is a large prime [48].

Property 2. Semigroup property

Let n , r , and s be positive integers, and $n \geq 2$, $x \in (-\infty, +\infty)$: $T_r(T_s(x)) = T_s(T_r(x)) = T_{rs}(x) \bmod P$.

Property 3. Discrete logarithm problem of extended Chebyshev polynomials

Here, the value of the extended Chebyshev polynomial is $T_n(x) = y \pmod{p}$, given x , y , and a large prime number p , then solve for n' so that $T_{n'}(x) = y \pmod{p}$, which is a discrete logarithm difficult problem.

Property 4. Extended Chebyshev polynomial DH problem

Given $x \in (-\infty, +\infty)$, a large prime number p , and the value of the extended Chebyshev polynomial $T_r(x) \pmod{p}$, $T_s(x) \pmod{p}$ (r and s are positive integers), solving the value of the extended Chebyshev polynomial $T_{rs}(x) \pmod{p}$ is a Diffie-Hellman difficult problem [49].

3.4. Chinese Remainder Theorem. The definition of Chinese remainder theorem [50, 51] is as follows: Let p_1, p_2, \dots, p_n

be pairwise prime integers.

$$\begin{cases} c \equiv y_1 \pmod{p_1}, \\ c \equiv y_2 \pmod{p_2}, \\ \vdots \\ c \equiv y_n \pmod{p_n}. \end{cases} \quad (3)$$

Then, the positive integer solution of the congruence equation system can be expressed as:

$$c \equiv y_1 P_1 P'_1 + y_2 P_2 P'_2 + \dots + y_n P_n P'_n \pmod{P}, \quad (4)$$

where:-

$P = p_1 p_2 \dots p_n = p_1 P_1 = p_2 P_2 = \dots = p_n P_n$. $P_i = P/p_i$ ($i = 1, 2, \dots, n$); P'_i is an integer solution satisfying $P_i P'_i \equiv 1 \pmod{p_i}$ ($i = 1, 2, \dots, n$).

4. Proposed Scheme

Based on research [13, 18–36, 48], this paper proposes a vehicle group authentication protocol based on extended chaotic mapping in 5G networks. This solution enables the participating vehicles to communicate securely through the group key in the 5G networks. Table 1 lists the main notations used here. Figure 2 shows the detailed authentication process of the protocol.

4.1. System Setup. In this stage, TA generates public parameters and master private key for the system and preloads the public parameters to the RSU and vehicle. TA selects large prime numbers p and q , randomly selects a secret value $s_{TA} \in \mathbb{Z}_q^*$ as the system key, selects $x \in (-\infty, +\infty)$, and

calculates the system public key $P_{TA} = T_{s_{TA}}(x)$. TA chooses the safe anticollision hash function, namely, $H_1 : \{0, 1\}^* \rightarrow Z_q^*$, $H_2 : \{0, 1\}^* \rightarrow \{0, 1\}^*$. $\{G\}$ is a prime number generation library, which contains infinite nonrepeated positive integers, and these positive integers are prime numbers to each other. The numbers are randomly selected for use and then discarded after use. This ensures that each number is not reused. Finally, TA publishes the system parameters $\{p, q, P_{TA}, x, H_1, H_2, \{G\}\}$.

4.2. Registration. At this stage, the vehicle and RSU obtain the required system parameters from TA and register with TA. The specific registration process is as follows.

(1) RSU registration

RSU_i first safely sends the network messages connected with TA. TA assigns unique identity EID_i to RSU_i, selects secret value $e_i \in Z_q^*$, and sends (EID_i, e_i) to RSU_i through secure channel. e_i is shared by RSU_i and TA, and {EID_i, e_i } is stored in TA.

(2) Vehicle registration

The vehicle U_j first sends its real identity VID_j to TA through secure channel. TA selects $n_j \in Z_q^*$, and calculates PID_j = $H_1(\text{VID}_j \| s_{TA} \| n_j)$. TA stores VID_j in the database, then sends PID_j to the vehicle U_j and saves it to the OBU_j.

Here, the registration data stored in TA are shared with 5GC through secure channel.

4.3. Access Authentication

(1) When RSU_i detects that there is a group communication between vehicles, it broadcasts a group access authentication notification message to the surroundings

(2) When the vehicle receives the notification, the OBU_j of the vehicle that needs to access the network first generates a random number $h_j \in Z_q^*$, a prime number $y_j \in \{G\}$, and current timestamp T_j and calculates. $A_{j_1} = T_{h_j}(x)$, $A_{j_2} = T_{h_j}(P_{TA})$,

-,
 $\text{MAC}_j = H_2(\text{VID}_j \| A_{j_2} \| A_{j_1} \| \text{PID}_j \| T_j)$, $A_{j_3} = H_1(A_{j_2} \| T_j \| \text{PID}_j) \oplus (\text{VID}_j \| y_j \| \text{MAC}_j)$. Then OBU_j sends the message {PID_j, A_{j_1} , A_{j_3} , T_j }

(3) RSU_i receives authentication request messages from n members of the group and first verifies the validity of the timestamps. If they are legal, it selects the current timestamp T_i , generates group identity GID_i, and calculates $\text{MAC}_i = H_2(\text{GID}_i \| e_i \| \text{EID}_i \| T_i)$. Finally, RSU_i packages the generated message and received vehicle messages into $\{(\text{PID}_j, A_{j_1}, A_{j_3}, T_j)_{j=1,2,\dots,n}, \text{GID}_i, \text{EID}_i, \text{MAC}_i, T_i\}$ and sends them to 5GC

TABLE 1: Notations.

Notations	Definitions
TA	A trusted authority
RSU	A roadside unit
OBU	On-board units
H_i	The hash function
$\{G\}$	Mutually prime nonrepeating positive integer library
\oplus	Exclusive-OR operation
$\ $	Concatenation operation
T_x	The timestamp
p, q	The large prime number
P_{TA}	The system public key
s_{TA}	The system master key
MAC_x	Message authentication code

(4) When 5GC receives the message, it first verifies the validity of the timestamp T_i . If it is legal, it calculates $\text{MAC}'_i = H_2(\text{GID}_i \| e_i \| \text{EID}_i \| T_i)$ and verifies whether MAC_i and MAC'_i are equal. If they are equal, the validity of RSU_i is verified and authentication continues. Otherwise, authentication is terminated. Then, 5GC verifies the validity of vehicle timestamp T_j . If it is equal, it calculates $A'_{j_2} = T_{s_{TA}}(A_{j_1})$, $(\text{VID}_j \| y_j \| \text{MAC}_j) = H_1(A'_{j_2} \| T_j \| \text{PID}_j) \oplus A_{j_3}$ to get VID_j, y_j , MAC_j , and then 5GC looks for the database to find the VID_j. If it finds the VID_j, then proceed to the next steps; otherwise, the authentication is terminated. 5GC calculates $\text{MAC}'_j = H_2(\text{VID}_j \| A'_{j_2} \| A_{j_1} \| \text{PID}_j \| T_j)$, and verifies whether MAC'_j and MAC_j are equal. If they are equal, the validity of the vehicle is verified, and the certification continues. 5GC reselects $n_j^{\text{new}}, e_i^{\text{new}} \in Z_q^*$, calculates $\text{PID}_j^{\text{new}} = H_1(\text{VID}_j \| s_{TA} \| n_j^{\text{new}})$ and updates database {EID_i, e_i^{new} }. 5GC selects current timestamp T_{TA} and the random values $g_j, v_i \in Z_q^*$, and calculates $F_{j_1} = T_{g_j}(x)$, $F_{j_2} = T_{g_j}(A_{j_1})$, $F_{j_3} = \text{PID}_j^{\text{new}} \oplus H_1(F_{j_2} \| \text{VID}_j \| T_{TA})$, $F_{i_1} = T_{e_i}(x)$, $F_{i_2} = T_{v_i}(x)$, $F_{i_3} = T_{v_i}(F_{i_1})$, $F_{i_4} = e_i^{\text{new}} \oplus H_1(F_{i_3} \| e_i \| T_{TA})$, $F_{i_5} = H_1(\text{GID}_i \| e_i \| e_i^{\text{new}} \| F_{i_3} \| \text{EID}_i \| T_{TA})$. 5GC selects group key $MK \in Z_q^*$ for vehicle group and a random number $R \in Z_q^*$, calculates $\text{MAC}_{TA} = H_1(\text{PID}_j \| \text{PID}_j^{\text{new}} \| A'_{j_2} \| \text{VID}_j \| F_{j_2} \| T_{TA})$, $P_j = (MK \| \text{MAC}_{TA}) \oplus H_1(A'_{j_2} \| \text{VID}_j \| T_{TA})$, $Y = \prod_{j=1}^n y_j$, $Y_j = Y / y_j$, $Y_j t_j \equiv 1 \pmod{y_j}$, and obtains $S = \sum_{j=1}^n P_j t_j Y_j \pmod{Y}$ through Chinese remainder theorem. Finally, 5GC calculates the certification confirmation value $\text{CCV}_j = H_2(\text{VID}_j \| MK)$ and gets the group authentication confirmation value $\text{CCVS} = \oplus_{j=1}^n \text{CCV}_j$, and hashes it to get $\text{HCCVS} = H_1(\text{CCVS} \| R)$. Then, 5GC sends the message

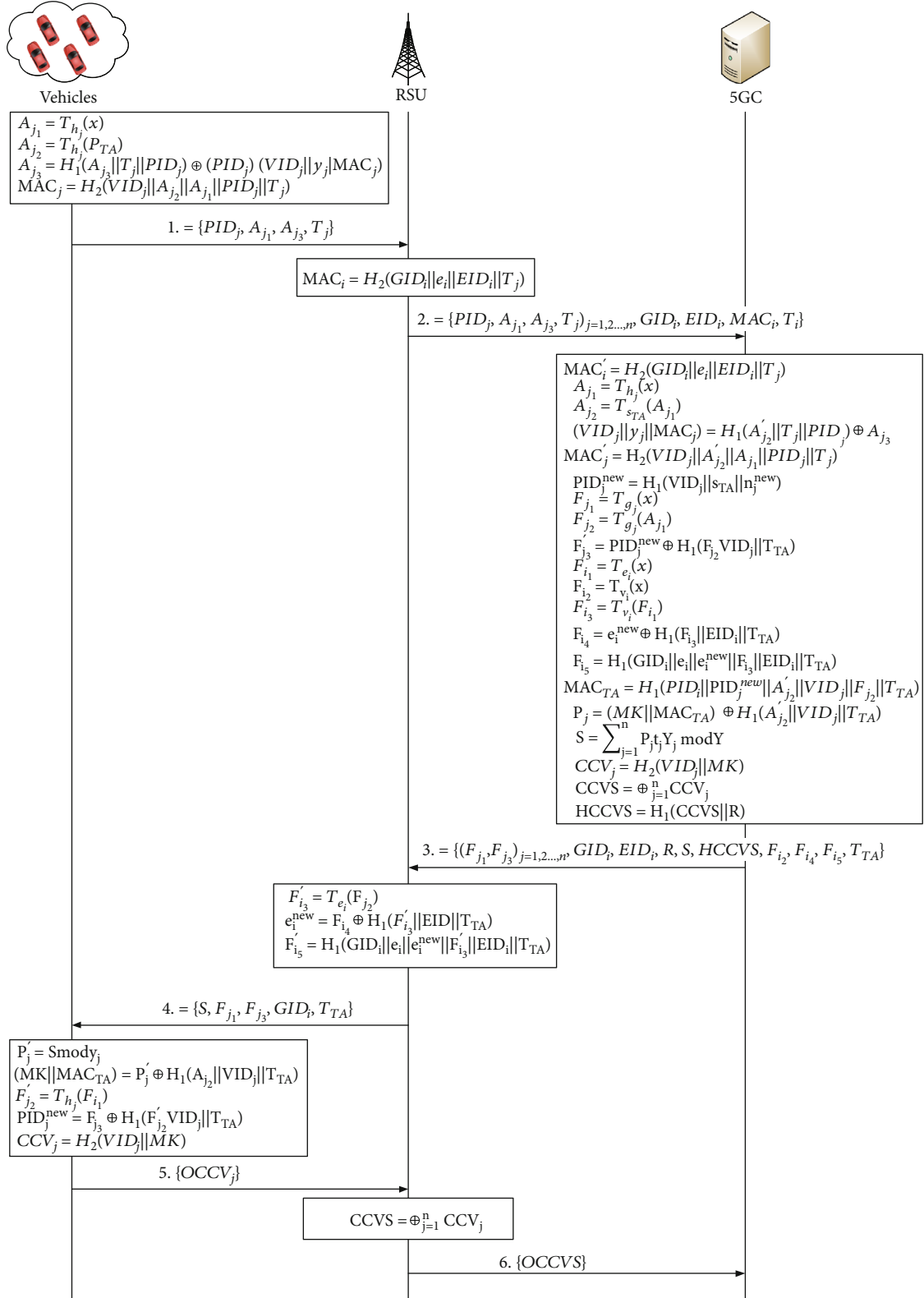


FIGURE 2: Authentication process of the proposed protocol.

$\{-$
 $(F_{j_1}, F_{j_3})_{j=1,2,\dots,n}, \text{GID}_i, \text{EID}_i, R, S, \text{HCCVS}, F_{i_2}, F_{i_4},$
 $F_{i_5}, T_{TA}\}.$

- (5) After receiving the message sent by 5GC, RSU_i first verifies whether the timestamp T_{TA} is within the legal range. If the timestamp is valid, RSU_i calculates $F'_{i_3} = T_{e_i}(F_{i_2})$, gets $e_i^{\text{new}} = F_{i_4} \oplus H_1(F'_{i_3} \| e_i \| T_{TA})$, and calculates $F'_{i_5} = H_1(\text{GID}_i \| e_i \| e_i^{\text{new}} \| F'_{i_3} \| \text{EID}_i \| T_{TA})$. Then, it verifies whether F'_{i_5} and F_{i_5} are equal. If they are equal, it uses e_i^{new} to update the secret value e_i . At the same time, RSU_i extracts the HCCVS, R and saves them to the database. Finally, the message $\{\text{GID}_i, S, F_{j_1}, F_{j_3}, T_{TA}\}$ is forwarded to the corresponding vehicle
- (6) When the corresponding message is received in the group vehicles, the OBU_j first verifies whether the timestamp T_{TA} is the legal. If the timestamp is valid, it calculates $P'_j = S \bmod y_j$, $(\text{MK} \| \text{MAC}_{TA}) = P'_j \oplus H_1(A_{j_2} \| \text{VID}_j \| T_{TA})$ and obtains the vehicle group key MK and MAC_{TA} . Then, OBU_j calculates $F'_{j_2} = T_{h_j}(F_{i_1})$, $\text{PID}_j^{\text{new}} = F_{j_3} \oplus H_1(F'_{j_2} \| \text{VID}_j \| T_{TA})$, $\text{MAC}'_{TA} = H_1(\text{PID}_j \| \text{PID}_j^{\text{new}} \| A_{j_2} \| \text{VID}_j \| F'_{j_2} \| T_{TA})$. OBU_j verifies whether MAC'_{TA} and MAC_{TA} are equal. If they are equal, OBU_j certifies 5GC. At this time, it can know that OBU_j gets the group key MK and updates $\text{PID}_j^{\text{new}}$. OBU_j calculates $\text{OCCV}_j = H_2(\text{VID}_j \| \text{MK})$ and sends the message $\{\text{OCCV}_j\}$ to RSU_i
- (7) When RSU_i receives the messages from the group vehicles, it calculates $\text{OCCVS} = \oplus_{j=1}^n \text{OCCV}_j$, $\text{HCCVS} = H_1(\text{OCCVS} \| R)$. And it verifies whether it is equal to the stored value HCCVS. If they are equal, it means that the group vehicles have been approved. Then, RSU_i sends OCCVS to 5GC and at the same time sends a successful authentication notification message to vehicular members
- (8) After 5GC receives the sent message, it verifies whether OCCVS and CCVS are equal. If they are equal, the group members are successfully authenticated

5. Security Evaluation

5.1. Formal Verification with Scyther Tool. Here, we use the Scyther tool to verify our protocol, which is a formal verification tool for security protocols [52]. There are many models in the Scyther, such as standard Dolev-Yao model, CK model, and eCK model. By using the Scyther to model our protocol, the Scyther can effectively discover potential security issues. The tool evaluates the confidentiality and authenticity of protocol information by writing protocol roles. Moreover, the tool provides a friendly graphical user interface, which is convenient to analyze and verify the com-

plex attack scenarios on the target protocol. Authentication statement in Scyther is as follows: Alive, Weakagree, Niagre, and Nisynch are used to detect malicious attacks such as replay attacks, reflection attacks, and man-in-the-middle attacks [53].

In this scheme, there are four roles: GV, RSU_i , 5GC, and TA. Since the protocol proposed in this paper is secure in the registration phase, we only consider the security in the access authentication phase. In the process of verification, we choose Dolev-Yao model to test, because attackers can carry out related attacks by controlling the network in this model. The simulation results based on Scyther are shown in Figure 3. It can be concluded from the results that our scheme successfully meets all the requirements of the Scyther confidentiality and authentication and resists attacks.

5.2. Security Analysis. According to the safety requirements given in the previous chapter, the following safety analysis is given.

- (1) Anonymity: this is an important aspect of vehicle privacy protection. In our proposed scheme, vehicles have communicated through the use of pseudonym $\text{PID}_j = H_1(\text{VID}_j \| s_{TA} \| n_j)$. And in the communication process, we hide the real identity in $A_{j_3} = H_1(A_{j_2} \| T_j \| \text{PID}_j) \oplus (\text{VID}_j \| y_j \| \text{MAC}_j)$, and only by using the secret value s_{TA} can restore the real identity of the vehicle. Therefore, the anonymity of the vehicle can be guaranteed
- (2) Message authentication and integrity: the communication entities in the scheme verify each other's legitimacy by verifying the message authentication code, so the scheme can provide message authentication. Since the generation of the message authentication code is based on the extended Chebyshev polynomial DH problem, the message authentication code is secure. Therefore, the integrity of the message can be verified
- (3) Traceability: once a message is disputed, according to the report message sent by the malicious vehicle and the pseudoidentity, TA can trace back the true identity of the malicious vehicle by calculating $(\text{VID}_j \| y_j \| \text{MAC}_j) = H_1(A'_{j_2} \| T_j \| \text{PID}_j) \oplus A_{j_3}$
- (4) Unlinkability: because the scheme uses random numbers and timestamps, the messages transmitted over the network are different. In addition, since the pseudoidentity of the vehicle is dynamically updated, the attacker cannot confirm that they are from the same sender.
- (5) Resistance to common attacks: the proposed scheme should be able to resist the following common types of attacks:
 - (a) Resistance replay attack: since a timestamp is attached to the message, by checking the validity

Claim	Status	Comments
5G_V2V GV 5G_V2V,GV1 Secret MK	Ok Verified	No attacks.
5G_V2V,GV2 Nisynch	Ok Verified	No attacks.
5G_V2V,GV3 Niagree	Ok Verified	No attacks.
5G_V2V,GV4 Alive	Ok Verified	No attacks.
5G_V2V,GV5 Weakagree	Ok Verified	No attacks.
5GC 5G_V2V,5GC1 Secret MK	Ok Verified	No attacks.
5G_V2V,5GC2 Nisynch	Ok Verified	No attacks.
5G_V2V,5GC3 Niagree	Ok Verified	No attacks.
5G_V2V,5GC4 Alive	Ok Verified	No attacks.
5G_V2V,5GC5 Weakagree	Ok Verified	No attacks.
RSU 5G_V2V,RSU1 Nisynch	Ok Verified	No attacks.
5G_V2V,RSU2 Niagree	Ok Verified	No attacks.
5G_V2V,RSU3 Alive	Ok Verified	No attacks.
5G_V2V,RSU4 Weakagree	Ok Verified	No attacks.

Done.

FIGURE 3: Scyther result.

TABLE 2: Security features comparison.

Functionality	[24]	[29]	[13]	[30]	[35]	[36]	[31]	Our scheme
Anonymous	Yes	No	No	Yes	Yes	Yes	Yes	Yes
Mutual authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Integrity	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Traceability	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Unlinkability	Yes	Yes	No	No	Yes	Yes	No	Yes
Replay attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Man-in-the-middle attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Counterfeit attack	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Batch certification	No	Yes	Yes	Yes	No	No	No	Yes

of the timestamp, the entities participating in the authentication can find out whether message replay has occurred

- (b) Resistance modification attack: in our proposed scheme, the message authentication code is calculated by the secret value held by the corresponding entity. And the secret value is updated dynamically. Therefore, the entity can verify whether the message has been modified
- (c) Resistance man-in-the-middle attack: according to the analysis of the previous message authentication and modification attacks, once an attacker

intercepts and maliciously changes the message in transmission, the entity verifies that the message authentication code in the message cannot be passed. This can be quickly found that the transmission content has been changed

- (d) Resist counterfeit attacks: in order to disguise a legitimate vehicle to send a request message, the adversary needs to send correct $A_{j_3} = H_1(A_{j_2} \| T_j \| \text{PID}_j) \oplus (\text{VID}_j \| y_j \| \text{MAC}_j)$ and $\text{MAC}_j = H_2(\text{VID}_j \| A_{j_2} \| A_{j_1} \| \text{PID}_j \| T_j)$. As analyzed above, it is impossible to extract the true identity of the vehicle from the intercepted

TABLE 3: Computation overhead.

Protocol	Total computation overhead	Total execution time
[33]	$8nT_{\text{ECC}} + 25nT_H + 2nT_{\text{DE}}$	$0.546093n$
[13]	$12nT_{\text{CCM}} + 14nT_H + 2nT_{\text{DE}}$	$0.28025n$
[30]	$9nT_{\text{ECC}} + 13nT_H + 4T_{\text{ECC}} + 7T_H$	$0.582657n + 0.259571$
[31]	$4nT_{\text{ECC}} + 14nT_H$	$0.263078n$
Our scheme	$6nT_{\text{CCM}} + 13nT_H + 4T_{\text{CCM}} + 8T_H$	$0.132411n + 0.08794$

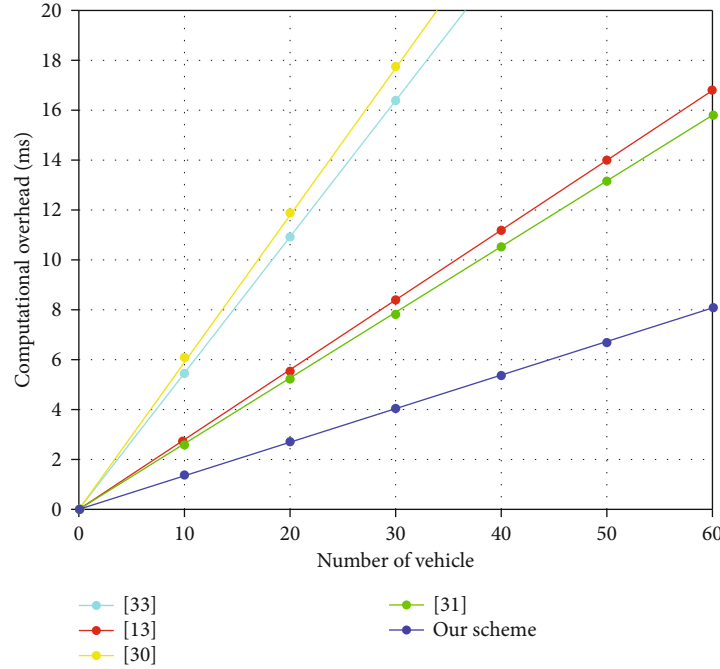


FIGURE 4: Computation overhead between different protocols.

TABLE 4: Communication overhead.

Protocol	Communication overhead
[33]	$2176n$
[13]	$2688n$
[30]	$2272n + 704$
[31]	$2816n + 1024$
Our scheme	$1760n + 1472$

message. Therefore, the scheme in this article can resist this type of attack

5.3. Security Comparison. Through the previous safety analysis, we show the comparison results with other schemes in Table 2. Comparison of the results in the table show that our scheme has better security performance.

6. Performance Analysis

By computation overhead and communication overhead, we evaluate the performance of the scheme. Here, we will

mainly compare the performance of some schemes similar to our proposed scheme, so our main comparison schemes are [13, 30, 31, 33]. Here, n represents the number of vehicles in the group.

6.1. Computation Overhead. In terms of computation overhead, we evaluated the proposed scheme on a laptop. We tested the calculation time of ECC-based scalar multiplication T_{ECC} , hash operation T_H , and Chebyshev mapping operation T_{CCM} , as well as calculation time based on symmetric encryption and decryption T_{DE} . Here, we only calculate some important operations and no longer calculate negligible operations, such as XOR operations. The results of our test are $T_{\text{ECC}} = 0.064016$ ms, $T_H = 0.000501$ ms, $T_{\text{CCM}} = 0.020983$ ms, $T_{\text{DE}} = 0.01072$ ms. As shown in Table 3, we have calculated the computation cost of the related schemes.

As can be seen from Figure 4, compared with other schemes, our scheme has the least computation overhead. When the number of vehicles are increasing, the advantage will be more obvious.

6.2. Communication Overhead. Before analyzing related protocols, we first define the size of relevant parameter in the

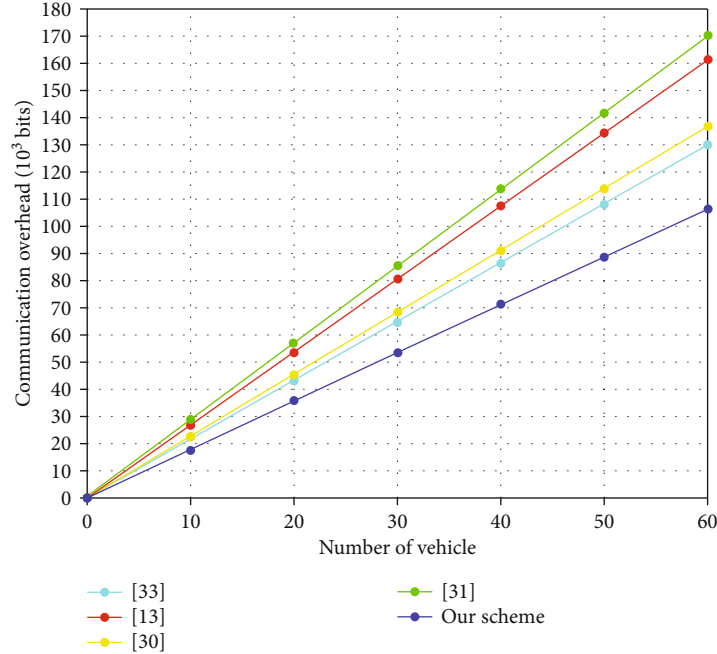


FIGURE 5: Communication overhead between different protocols.

protocol. Assume that the key size based on the ECC algorithm is 256 bits, the size of Chebyshev chaotic map is 128 bits, the size of hash value is 128 bits, the size of identity information is 128 bits, the size of timestamp is 32 bits, and the size of random number is 128 bits [54]. Calculation of the communication overhead for the above schemes is shown in Table 4.

As can be seen from Figure 5, our scheme has obvious advantages in communication overhead by comparing with other schemes [30].

7. Conclusion

As the communication among vehicle groups involves the problems of low delay, safety, and efficiency in the 5G-enabled vehicular networks, we propose a lightweight and secure vehicle group authentication protocol. The scheme is based on the extended chaotic mapping algorithm to achieve authentication, and the group key is distributed through the Chinese remainder theorem, so that the vehicle groups will communicate through the group key. In order to protect the security of RSU, the shared key will be updated. In addition, the security of the scheme is verified by the Scyther tool, and the verification results show that the security of the protocol can be guaranteed. And through the security analysis, the scheme can not only effectively resist all kinds of attacks but also ensure the anonymity, unlinkability, and other security requirements. Finally, by comparing the computation overhead and communication overhead with related schemes, our scheme has less overhead. In the future research work, we will start to study the group management scheme based on aggregation authentication. With the development of 5G communication technology, an effi-

cient scheme is designed to meet the needs of security and privacy.

Data Availability

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

Conflicts of Interest

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

Acknowledgments

This work was supported by the 2020 Industrial Technology Foundation Public Service Platform Project (grant number 2020-0105-2-1).

References

- [1] G. Dimitrakopoulos and P. Demestichas, "Intelligent transportation systems," *IEEE Vehicular Technology Magazine*, vol. 5, no. 1, pp. 77–84, 2010.
- [2] J. Wang, Y. Shao, Y. Ge, and R. Yu, "A survey of vehicle to everything (V2X) testing," *Sensors*, vol. 19, no. 2, p. 334, 2019.
- [3] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.
- [4] S. Zhang, N. Zhang, X. Fang, P. Yang, and X. S. Shen, "Self-sustaining caching stations: Toward cost-effective 5g-enabled vehicular networks," *IEEE Communications Magazine*, vol. 55, no. 11, pp. 202–208, 2017.

- [5] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: the next generation of mobile communication," *Physical Communication*, vol. 18, pp. 64–84, 2016.
- [6] A. Osseiran, F. Boccardi, V. Braun et al., "Scenarios for 5G mobile and wireless communications: the vision of the METIS project," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 26–35, 2014.
- [7] J. Saqlain, *IoT and 5G: History Evolution and Its Architecture Their Compatibility and Future*, [Ph.D. Thesis], Subtitle Metropolia University of Applied Sciences, 2018.
- [8] S. A. Abdel Hakeem, A. A. Hady, and H. W. Kim, "5G-V2X: standardization, architecture, use cases, network-slicing, and edge-computing," *Wireless Networks*, vol. 26, no. 8, pp. 6015–6041, 2020.
- [9] Z. Lin, X. Du, H. H. Chen, B. Ai, Z. Chen, and D. Wu, "Millimeter-wave propagation modeling and measurements for 5G mobile networks," *IEEE Wireless Communications*, vol. 26, no. 1, pp. 72–77, 2019.
- [10] I. Rasheed, F. Hu, Y. K. Hong, and B. Balasubramanian, "Intelligent vehicle network routing with adaptive 3D beam alignment for mmwave 5G-based V2X communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 5, pp. 2706–2718, 2021.
- [11] N. Zhang, S. Zhang, P. Yang, O. Alhusein, W. Zhuang, and X. S. Shen, "Software defined space-air-ground integrated vehicular networks: challenges and solutions," *IEEE Communications Magazine*, vol. 55, no. 7, pp. 101–109, 2017.
- [12] O. Yilmaz and N. Johansson, "5G radio access for ultra-reliable and low-latency communications," *Ericsson Research Blog*, vol. 1, pp. 1184–1189, 2015.
- [13] J. Cui, Y. Wang, J. Zhang, Y. Xu, and H. Zhong, "Full session key agreement scheme based on chaotic map in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 8914–8924, 2020.
- [14] C. Wang, D. Wang, G. Xu, and D. He, *Efficient Privacy-Preserving User Authentication Scheme with Forward Secrecy for Industry 4.0*, Science China: Information Sciences, 2020.
- [15] Z. Li, D. Wang, and E. Morais, "Quantum-safe round-optimal password authentication for mobile devices," *IEEE Transactions on Dependable and Secure Computing*, 2020.
- [16] M. S. Sheikh, J. Liang, and W. Wang, "A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)," *Sensors*, vol. 19, no. 16, p. 3589, 2019.
- [17] C. Wang, D. Wang, Y. Tu, G. Xu, and H. Wang, "Understanding node capture attacks in user authentication schemes for wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2020.
- [18] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 1, pp. 248–262, 2011.
- [19] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "SPACF: a secure privacy-preserving authentication scheme for VANET with cuckoo filter," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10283–10295, 2017.
- [20] P. Vijayakumar, V. Chang, L. Jegatha Deborah, B. Balusamy, and P. G. Shynu, "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," *Future Generations Computer Systems*, vol. 78, Part 3, pp. 943–955, 2018.
- [21] M. Han, L. Hua, and S. Ma, "A self-authentication and deniable efficient group key agreement protocol for VANET," *Ksii Transactions on Internet & Information Systems*, vol. 11, no. 7, pp. 3678–3698, 2016.
- [22] P. Vijayakumar, M. Azees, A. Kannan, and L. Jegatha Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015–1028, 2016.
- [23] 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.
- [24] J. Cui, X. Tao, J. Zhang, Y. Xu, and H. Zhong, "HCPA-GKA: a hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs," *Vehicular Communications*, vol. 14, pp. 15–25, 2018.
- [25] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 722–735, 2021.
- [26] C. Lai, D. Zheng, Q. Zhao, and X. Jiang, "SEGM: a secure group management framework in integrated VANET-cellular networks," *Vehicular Communications*, vol. 11, pp. 33–45, 2018.
- [27] Q. Zhang, X. Wang, J. Yuan et al., "A hierarchical group key agreement protocol using orientable attributes for cloud computing," *Information Sciences*, vol. 480, pp. 55–69, 2019.
- [28] A. Shi, B. Mso, C. Pv et al., "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Generation Computer Systems*, vol. 84, pp. 216–227, 2018.
- [29] I. Gharsallah, S. Smaoui, and F. Zarai, "An efficient authentication and key agreement protocol for a group of vehicles devices in 5G cellular networks," *IET Information Security*, vol. 14, no. 1, pp. 21–29, 2020.
- [30] J. Zhang, H. Zhong, J. Cui, M. Tian, Y. Xu, and L. Liu, "Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7940–7954, 2020.
- [31] M. Ouaisa, M. Houmer, and M. Ouaisa, "An enhanced authentication protocol based group for vehicular communications over 5G networks," in *2020 3rd International Conference on Advanced Communication Technologies and Networking (CommNet)*, pp. 1–8, Marrakech, Morocco, 2020.
- [32] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.
- [33] J. Zhang, H. Zhong, J. Cui, Y. Xu, and L. Liu, "SMAKA: secure many-to-many authentication and key agreement scheme for vehicular networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1810–1824, 2021.
- [34] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, "RSMA: reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6417–6428, 2019.

- [35] J. Huang, Y. Qian, and R. Q. Hu, "Secure and efficient privacy-preserving authentication scheme for 5G software defined vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 8542–8554, 2020.
- [36] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A lightweight privacy-preserving authentication protocol for VANETs," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3547–3557, 2020.
- [37] C. Wang, R. Huang, J. Shen, J. Liu, P. Vijayakumar, and N. Kumar, "A novel lightweight authentication protocol for emergency vehicle avoidance in VANETs," *IEEE Internet of Things Journal*, pp. 1–1, 2021.
- [38] 3rd Generation Partnership Project and Technical Specification Group Services and System Aspects, "System Architecture for the 5G System (Release 16)," in *3GPP Standard TS 33.501, V16.4.0*, pp. 18–46, 3rd Generation Partnership Project (3GPP), 2020.
- [39] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, 2012.
- [40] X. Li, Y. Wang, P. Vijayakumar, D. He, N. Kumar, and J. Ma, "Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11309–11322, 2019.
- [41] O. Mir, T. Weide, and C. C. Lee, "A secure user anonymity and authentication scheme using AVISPA for telecare medical information systems," *Journal of Medical Systems*, vol. 39, no. 9, p. 265, 2015.
- [42] C. T. Li, C. C. Lee, C. Y. Weng, and S. J. Chen, "A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems," *Journal of Medical Systems*, vol. 40, no. 11, article 233, 2016.
- [43] M. S. Hwang, C. C. Lee, and Y. C. Lai, "Traceability on low-computation partially blind signatures for electronic cash," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E85-A, no. 5, pp. 1181–1182, 2002.
- [44] H.-A. Wen, K.-C. Lee, S.-Y. Hwang, and T. Hwang, "On the traceability on RSA-based partially signature with low computation," *Applied Mathematics and Computation*, vol. 162, no. 1, pp. 421–425, 2005.
- [45] C. C. Lee, M. S. Hwang, and W. P. Yang, "A new blind signature based on the discrete logarithm problem for untraceability," *Applied Mathematics & Computation*, vol. 164, no. 3, pp. 837–841, 2005.
- [46] P. Bergamo, P. D'Arco, A. de Santis, and L. Kocarev, "Security of public-key cryptosystems based on Chebyshev polynomials," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 52, no. 7, pp. 1382–1393, 2005.
- [47] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," *Chaos, Solitons & Fractals*, vol. 37, no. 3, pp. 669–674, 2008.
- [48] S. Qiu, D. Wang, G. Xu, and S. Kumari, "Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2020.
- [49] T. T. K. Hue, T. M. Hoang, and A. Braeken, "Lightweight sign-cryption scheme based on discrete Chebyshev maps," in *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 43–47, Cambridge, UK, 2017.
- [50] Y. Ren, V. Oleshchuk, and F. Y. Li, "An efficient Chinese remainder theorem based node capture resilience scheme for mobile WSNs," in *2010 IEEE International Conference on Information Theory and Information Security*, pp. 689–692, Beijing, China, 2010.
- [51] P. Vijayakumar, S. Bose, and A. Kannan, "Chinese remainder theorem based centralised group key management for secure multicast communication," *Information Security*, vol. 8, no. 3, pp. 179–187, 2014.
- [52] J. Cao, Z. Yan, R. Ma, Y. Zhang, Y. Fu, and H. Li, "LSAA: a lightweight and secure access authentication scheme for both UE and mMTC devices in 5G networks," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5329–5344, 2020.
- [53] C. Cremers, *The Scyther Tool*, CISPA Helmholtz Center for Information Security, 2020, <https://people.cispa.io/cas.cremers/scyther/>.
- [54] Y. Sun, J. Cao, M. Ma et al., "EAP-DDBA: efficient anonymity proximity device discovery and batch authentication mechanism for massive D2D communication devices in 3GPP 5G HetNet," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2020.

Research Article

Analyzing the Effectiveness of Touch Keystroke Dynamic Authentication for the Arabic Language

Suliman A. Alsuhibany  and Afnan S. Almuqbil 

Department of Computer Science, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia

Correspondence should be addressed to Suliman A. Alsuhibany; salsuhibany@gmail.com

Received 31 March 2021; Revised 14 July 2021; Accepted 25 August 2021; Published 11 September 2021

Academic Editor: Ding Wang

Copyright © 2021 Suliman A. Alsuhibany and Afnan S. Almuqbil. 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 keystroke dynamic authentication (KDA) technique was proposed in the literature to develop a more effective authentication technique than traditional methods. KDA analyzes the rhythmic typing of the owner on a keypad or keyboard as a source of verification. In this study, we extend the findings of the system by analyzing the existing literature and validating its effectiveness in Arabic. In particular, we examined the effectiveness of the KDA system in Arabic for touchscreen-based digital devices using two KDA classes: fixed and free text. To this end, a KDA system was developed and applied to a selected device operating on the Android platform, and various classification methods were used to assess the similarity between log-in and enrolment sessions. The developed system was experimentally evaluated. The results showed that using Arabic KDA on touchscreen devices is possible and can enhance security. It attains a higher accuracy with average equal error rates of 0.0% and 0.08% by using the free text and fixed text classes, respectively, implying that free text is more secure than fixed text.

1. Introduction

The rapid progress engendered by mobile devices has exponentially accelerated the use of smartphones and other digital devices [1, 2]—owing to the power of networking, mobility sensing, and mobile device computing. According to a cybersecurity statistics report [3], malware variants in mobile crypto-jacking increased from eight in 2017 to a staggering 27 in the first five months of 2018. In March 2020, the new Android malware samples per month were 482,579 [4]. Among them, Trojans are the most popular form of malware affecting Android devices, as reported by the AV-Test [5]. This increment in malware variants demands robust security mechanisms for mitigating the enhanced risk.

Security measures suffer from severe security and usability limitations. Many authentication methods have been used for mobile security, such as personal identification numbers, face recognition, and fingerprint scanning [6]. Although these mechanisms ensure security, they can be easily compromised [7]. For example, passwords can be shoulder-surfed, leaked, or guessed, or other password-defying channels can be used to break-in. Also, passwords can be

shared with friends and written to remember [8, 9]. Similarly, fingerprint authentication is equally susceptible to being spoofed by imitating the fingertip structure, often generated using a concealed fingerprint [10]. The mobile system sometimes fails to recognize the fingertip, requiring multiple attempts. Similar to passwords and fingerprint recognition, facial recognition can be spoofed using a video, photo, or 3D mask to forge the faces of the mobile users [11]. Besides being vulnerable to illegitimate use, these authentication systems require additional hardware to support their services, ultimately adding to the cost of the device.

To investigate security in a mobile environment, this work considers the technology of keystroke dynamics authentication (KDA) in terms of its efficiency for ensuring the required security. In particular, biometric security authentication is divided into two characteristics: physiological and behavioral. Although the fingerprint, face, veins, and iris are all physiological characteristics unique to each user, behavioral characteristics include studying certain behavior-based patterns.

KDA relies on behavior-based authentication characteristics, specifically, the manner and rhythm of users when

typing characters. Every user has a unique behavioral pattern based on typing strength, the interval between characters, finger position, and angle of usage. The classification of keystroke dynamics is accomplished based on the target input of keystrokes in the form of either fixed or free text—the fixed text class refers to predefined text that must be entered every time the user wishes to sign in to the device/system. Alternatively, the free text class does not involve the predefined text requirement and bypasses the memorization requirement for users. Thus, this study considers both free text and fixed text classes of KDA to become the first study to adopt this approach.

Considering the challenges faced by traditional authentication methods, the dynamic behavioral techniques of biometrics have been calibrated and found harder to forge. That is, keystroke dynamics, when applied on keyboards, reveal only timing information or the elapsed time between releasing and pressing a key and the duration for which the key was held down. Based on this, behavioral authentication systems offer several advantages in countering the deficiencies of traditional authentication. First, generating the same pattern of movement is more challenging to imitate. Even when the movement pattern is imitated; differences in body structure, such as finger shape, height, and orientation on the touchscreen, can differ, leading to changes in the movement patterns. Furthermore, the built-in physical sensors in digital devices can easily detect these minor differences and consequently block access. Further, every user has a unique way of inputting data into a device; any unauthorized user can copy a password; however, it is not easy to imitate the touch style, type, and pattern of the authentic user.

Keystroke dynamics has produced substantial research, with the focus being increasingly placed on the keypad area of smartphones. Recently conducted research has reported an error equal rate (EER) of 0% [12].

These promising results are attributed to tools already embedded in keypads, such as the accelerometer, gyroscope, and other sensors, which facilitate accurate pattern information compared to a fixed keyboard. In general, there are differences between the data collected by physical keyboards and touchscreen keyboards [13]. In addition to classical timing features, keystroke dynamics on touchscreen keypads enable additional features for authentication, such as pressure on the screen during typing and the area of keys covered by the fingers [14, 15].

Although Arabic has been analyzed using physical keyboards in [16–18], revealing an efficient performance, it has not been analyzed in touchscreen keyboards. Therefore, this study analyzes the effectiveness of touch KDA for Arabic.

The remainder of this paper is organized as follows. Section 2 discusses related work. Section 3 describes the methodology, including data collection, feature extraction, and classification methods for user verification. Section 4 presents the experimental results, which are further outlined and discussed in Section 5. Finally, Section 6 presents the conclusion with suggestions for future research.

2. Related Works

This section is divided into three parts. First, the literature on the use of KDA systems as a verification tool in touchscreen-based digital devices is reviewed. Second, the application of Arabic in KDA was explored. Finally, studies that have applied the KDA system to other languages are discussed.

2.1. Use of KDA in Touchscreen-Based Digital Devices. This section discusses KDA studies in terms of classes, types of features, and classification methods.

2.1.1. KDA Studies Based on the Classes. To reiterate, keystroke dynamics can be categorized into two classes: free text and fixed text. The free text has the potential to verify the authenticity of users in the log-in process alongside the capacity to continuously monitor users after log-in based on their typing pattern [19]. In contrast, the fixed text is primarily employed to protect valid users from various threats in the log-in process. Based on these characteristics, hard-keyboard-based free KDA has been actively studied [20–23]. Conversely, the utilization of free KDA on smartphone devices has received relatively little research attention.

As shown in Tables 1 and 2, the performance of the free KDA is slightly lower than that of the fixed KDA. This low performance has several limitations. First, its keystroke feature is limited, and the number of keystrokes might not be sufficient, as shown in [24]. Draffin et al. [25] failed to provide adequate information because they only used the time feature. In Gascon et al. [26], the worst performance of non-identifiable users, which can hardly be distinguished from others, managed to have a 58% true positive rate (TPR) and 35% false positive rate (FPR). This is unreasonable for practical authentication systems. The study by Kim and Kang [12] was the only one to use free text, and it managed to obtain good results, scoring 0.07% EER and 0% EER in English and Korean, respectively. Conversely, the fixed text has become a saturated research area, yielding interesting results, such as 0.01% EER in Buriro et al. [27].

2.1.2. KDA Studies Based on the Feature Type. In 2009, the earliest research was conducted to analyze KDA as a verification tool in touchscreen devices. This research was performed by Saevanee and Bhattarakosol [28] and focused on finger pressure on the touchscreen as a biometric source for keystroke dynamics analysis, using laptops as a base. With the release of Android 1.6, many new features were added to digital devices, such as fingertip size, device orientation, and device angle, which broadened the application of the technique. In 2010, a further advancement occurred after Android 2.3, which included a rotation vector, a gyroscope, a linear accelerometer, and gravity, giving new life to studies being conducted in this area. Notably, a study by Zheng et al. [29] researched using KDA on mobile touchscreens specifically. In addition to examining common touchscreen-based features, they studied the efficiency of KDA using accelerometer sensors. Kambourakis et al. [30] used Android devices and proposed two new features to evaluate keystroke dynamics: speed and distance features.

TABLE 1: Recent studies of the free KDA for touchscreen devices.

Study	Year	Number of subjects	Methodology	Features	Classifier	FAR, FRR, or EER
[25]	2013	13	15 keys	Time, pressure, gyroscope, coordination, and size	MLP	14% FAR, 2.2% FRR
[26]	2014	315	Predefined free text (150 keystrokes)	Time, accelerometer, gyroscope, and oriented sensor	SVM	92% FAR, 1% FRR
[24]	2015	35	Predefined free text (3,000 keystrokes)	Time	Statistical method, KNN, Gaussian estimation, Parzen window kernel estimation, and support vector data description (SVDD)	8.99% EER
[12]	2020	50	10 samples of 200 keystrokes each	Time, acceleration, and coordination	TT, R, TTPR, TTMR, <i>Kolmogorov-Smirnov statistic</i> , and <i>Cramér-von Mises criterion (CM)</i>	0% EER
Our study	2021	45	200 keystrokes	Time, acceleration, gyroscope, pressure and coordination	ANN, KNN, SVM, Euclidean distance, Manhattan distance, and random forest	0% EER

Roh et al. [31] also used accelerometer sensors but added four additional features: keystamps, gyroscope sensor, touch size, and touch coordinates. Research on several other features, such as motion data and time interval, was conducted by Lee et al. [32], who evaluated keystroke dynamics features using both motion and motionless data to determine which feature yielded more accuracy—motion data yielded more precise results.

2.1.3. KDA Studies Based on the Classification Methods. Several techniques and methods have been proposed to categorize the typing behavior of users, such as machine learning techniques, distance-based matrices, and statistical mechanisms, which have been rarely implemented.

Many studies have employed distance matrices, such as the Manhattan, Euclidean, and Bhattacharya distances. For example, Lee et al. [32] and Coakley et al. [33] implemented Euclidean and Manhattan distance matrices, which resulted in the Manhattan distance producing better accuracy in both studies.

Some researchers have implemented data preprocessing through scaling [7] and standardization before applying distance matrices. Such preprocessing techniques might be crucial for calculating the similarities between features. Although these techniques have generated satisfactory results in some studies, other studies have deemed the results unacceptable.

Likewise, Lee et al. [32] applied the Manhattan and Euclidean distances with two different scaling techniques: standard and MinMax scaling. The best results were obtained by applying the Manhattan distance with standard scaling. Similarly, Roh et al. [31] used the Manhattan and Euclidean distances with mean, absolute deviation, and standard deviation. Their results suggested that preprocessing might not always be useful since they demonstrated that although the outcome generated by preprocessing was good for the average EER, it was worse for the best EER.

Machine learning techniques have been proposed in various studies, as shown in Table 1. Random forest, k-nearest neighbor (KNN), and multilayer perceptron (MLP) classifiers are the most frequently used machine learning techniques. In Sen and Muralidharan [34], MLP obtained a better accuracy rate than decision trees, naïve Bayes, and KNN. Random forest was considered better than MLP in Salem et al. [35], in which the EER score was 0.45%. In Kambourakis et al. [30], there are three renowned classifiers: MLP, KNN, and random forest. Eventually, MLP was rejected because it was incapable of running with memory restrictions when the classifiers were provided with an upper bound of 512 MB of memory. Moreover, KNN was used in Ehatisham-Ul-Haq et al. [36] in addition to three classifiers: support vector machine (SVM), decision trees, and Bayes net—the Bayes net and SVM classifiers delivered better results.

de Mendizabal-Vazquez et al. [37] used Euclidean distance alongside the MLP classifier, with MLP delivering better performance when the sample was increased and when the correct identification rate was 90%. However, the Euclidean distance performed well despite operating with a smaller sample, reaching an EER of 20%.

Based on the preprocessing using machine learning techniques, three preprocessed sample groups were created by De et al. [37]: (1) a linear discriminant analysis (LDA) group, (2) a principal component analysis (PCA) group, and (3) an original data group. The best results were obtained for the PCA group. It was also argued that a considerable reduction in data size due to PCA eased the implementation of these methods on mobile devices, which tend to have strong limitations because of their processing capacity and battery life.

2.2. KDA Using Other Languages. All previous keystroke dynamics studies conducted on touchscreen-based devices included only English as the input language, excluding one

TABLE 2: Recent studies of the fixed KDA for touchscreen devices.

Study	Year	Number of subjects	Methodology	Features	Classifier	FAR, FRR, or EER
[14]	2013	152	17-digit passphrase 10 times	Time, pressure, size, and coordination	K-means	4.59% FRR 4.19% FAR
[32]	2018	22	6-digit PIN	Accelerometer, gravity, rotation, pressure, time, size, and coordination	Euclidean and Manhattan distances	7.89% EER
[29]	2014	80	4-digit PIN/8-digit PIN	Time, acceleration, pressure, and size	Nearest neighbor distance	3.65% EER
[31]	2016	15	4-digit PIN	Flight time, acceleration, pressure, and size	SVR, scaled Euclidean, scaled Manhattan, KNN, and random forest	8.71% EER
[30]	2014	20	10 alphanumeric characters and 47 characters including spaces	Hold time, intertime, distance, and speed	Random forest, KNN, and MLP	12.5% EER
[27]	2015	12	4-digit PIN	Time, accelerometer, gravity, magnetometer, gyroscope, and orientation	Binary classifiers, Bayes net, and random forest	0.01% FAR 0.01% FRR
[7]	2019	104	4-digit PIN	Flight time, acceleration, pressure, and size	SVR, scaled Euclidean, scaled Manhattan, KNN, and random forest	8.71% EER
[6]	2016	150	4-digit PIN 16-digit PIN	Time and size	Gaussian estimation, z-score, and standard deviation drift	6.26% EER
[35]	2019	7	Static, 8 characters (complex passwords)	Time, pressure, size, and coordination	MLP, decision trees, and random forest	0.45% EER
[36]	2017	10	10 different password templates	Time, accelerometer, gyroscope, and magnetometer	Decision tree, KNN, SVM, and Bayesian network/Bayes net classifier	99.18% accuracy
[33]	2016	52	10-digit PIN	Time, pressure, screen location, accelerometer, and gyroscope	Euclidean distance and Manhattan distance	4.3% EER
[34]	2014	10	4-digit PIN	Time and pressure	Decision tree, naïve Bayes, KNN, and MLP	14.1% FAR 14% FRR
[37]	2014	80	4-digit PIN	Time, accelerometer, gyroscope, pressure, and finger size	Euclidean distance and MLP	20% EER

study that included both Korean and English [12]. This demonstrates a lack of language variation in such systems. However, some experiments have considered other languages in fixed keyboard environments. The first study conducted using another input language was in Gunetti et al. [38], which used Italian. This study demonstrated that KDA works in languages other than English and produces accurate results. Two features were examined in this study: the digraph latency and keystroke duration. The researchers compared the samples typed using English and Italian, providing evidence that keystroke dynamics are useful even when the typing samples are written in different languages. Japanese was also checked for accuracy by Samura and Nishimura [39], who employed the keystroke timing for every single letter and combinations of two letters composed of consonant and vowel pairs in

the text. This experiment was performed on 112 participants divided into three groups, depending on their typing skills. The findings included a recognition accuracy of nearly 100% in the group that could write more than 900 letters in five min.

For generalising the KDA scheme to other language, a study in [12] conducted an experiment using two languages: Korean language, which is the native language of the participants, and the English language. Their results showed that the accuracy was higher when the native language was used. Likewise, studies in [2–4] compared between two languages (Arabic and English) with the Arabic native speakers using fixed keyboard, and the accuracy was higher using Arabic language. Thus, we aim in this paper to analyze the effectiveness of touch KDA for Arabic language with the Arabic native speakers.

2.3. KDA Using Arabic. The first study to consider Arabic in the analysis of the accuracy of keystroke dynamics was performed by Alsultan et al. [16], who used the key pairing approach via an Arabic alphabet keyboard. This study classified every character pair based on its relationship and keyboard location. Five keystroke features were extracted from each key pair. Their findings were extended by Alsuhibany et al. [17], who combined three features: keystroke duration, keystroke latency, and di-graph duration through Euclidean distance classification. This study yielded accurate results retched to 0.1 EER. Moreover, Alsuhibany et al. [18] further broadened this research by applying Bhattacharya and Euclidean distance measures, and the results showed that the Bhattacharyya distance was more accurate for both Arabic and English inputs.

Tables 1 and 2 provide a comparison of the most recent studies on keystroke dynamics for a touchscreen environment. As shown in Table 1, our study is compared with other studies that applied the free text technique [12, 24–26]. The comparison is based on many factors, such as EER, the number of keystrokes used, features, and classifiers. In particular, a study in [12], that achieved the best results compared with other studies, is comparable with our study. Although the best accuracy rate was the same (0.0 EER) reached by both studies, the number of keystrokes in our study was noticeably less, which increased the usability of our system.

3. Methodology

This section explains the typical touch dynamics biometric authentication system and its components. Figure 1 indicates that the system operation largely consists of several functional blocks (architectural components), each performing a well-defined function. These components and their respective operations are described as follows.

3.1. Data Collection. For the data collection, a touch-stroke authentication system was implemented using an Android application, which records raw data when a user touches a key. Moreover, when a user writes text and touches the submission button, a user profile is generated and stored in the local database of the device. This profile comprises five features: time stamps, acceleration, gyroscope, pressure, and coordination. Using an Android device (i.e., Huawei Nova 3i), data from 45 participants were collected. Most participants were in the same age bracket (19-25) and owned Android touch-technology smartphones.

It is important to note that all collected data was used for the pompous of this experiment and will be kept stored on the principal investigator drive with no names and an indemnifier of the participants.

3.2. Feature Extraction. This section describes the features used in the study. Specifically, touchscreen devices are designed to capture more features than traditional keyboards. Therefore, the features used in our study were selected because of their efficient performance in the state-of-the-art for activity recognition. To rephrase, the existing

research [27, 31, 36] has well-established the excellent performance of these features for behavioral authentication.

3.2.1. Timing Features. The timing features of keystroke dynamics were attained from two keyboard actions: depression and release. Depression is the timestamp recorded when a key is held down (D), whereas Release is the timestamp recorded when the key is released (U). Timing features were obtained by capturing the time stamps for every event, as shown in Figure 2. Furthermore, very basic and consecutive events can exist in the following combinations:

- (i) *Keystroke Duration or Hold Time (Down-Up)*. The key is pressed until it is released. Figure 3 shows the hold times for four randomly selected participants. The difference between users' behaviors when pressing the buttons can be seen, and the average hold time is, in most cases, more constant between users
- (ii) *Keystroke Latencies/Flight Time*. This is also identified as Down-Down (DD) or Press-Press (PP)—the time between two consecutive key presses
- (iii) *Di-Graph Duration*. This is the elapsed time between the release of the first key and the depression of the second key. It is known as the Up-Down (UD). Figure 4 shows the digraph duration for four users. Although there exists little difference between users, the rhythm of the digraph is less constant between users, as well as between the actions of individual users

3.2.2. Nontiming Features. Four nontiming features were used in our experiment: coordination, pressure, accelerometer, and gyroscope sensors.

The coordinate values are extracted for the horizontal and vertical axes at the time of the key press on the touchscreen device. These coordinate values are 2-row data, one for the x -axis and another for the y -axis for each action. Figure 5 shows a scatter plot of five users who pressed one key when each user had different C_x and C_y coordinates.

The pressure force is returned when the user presses a key on the touchscreen. The returned pressure measurements are an abstract unit, ranging from 0 (no pressure) to 1 (normal pressure). However, higher than one values can also occur depending on the calibration of the input device. In essence, the pressure values are 1-row data, which is the pressure force for each action. The accelerometer calculates the accelerometer (m/s^2) of the three axes, lateral x -, longitudinal y -, and vertical z -axis, as shown in Figure 6(a), by considering gravity values. Figure 7 shows the visualization of the values of the three axes of acceleration for two randomly chosen participants. The gyroscope measures the rate of rotation (rad/s) of a device using three axes: x - axis (pitch), y -axis (roll), and z -axis (yaw), as shown in Figure 6(b). The accelerometer and gyroscope numbers are uneven by samples and must be reshaped as regular forms. Lee et al. [2] used five formulae for the grouped data: average value (mean), root mean square, the sum of positive values, the

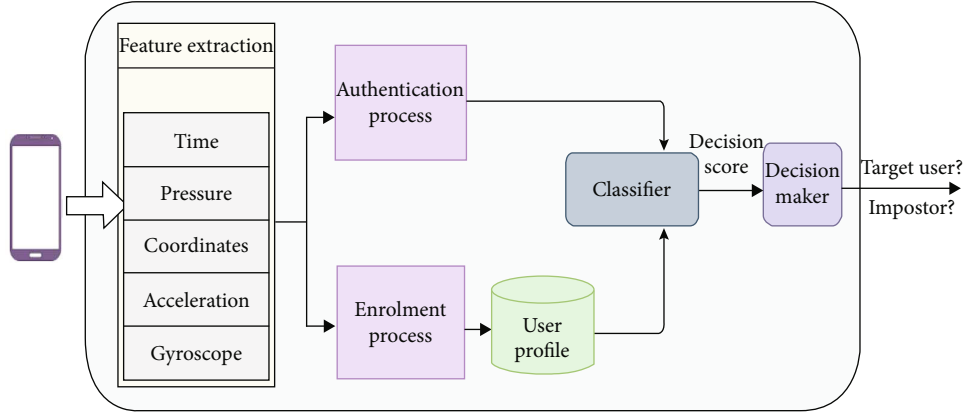


FIGURE 1: Typical touch dynamic biometric authentication system.

Description	Press "a"	Release "a"	Press "b"	Release "b"
Timestamp	000 (ms)	300 (ms)	400 (ms)	650 (ms)

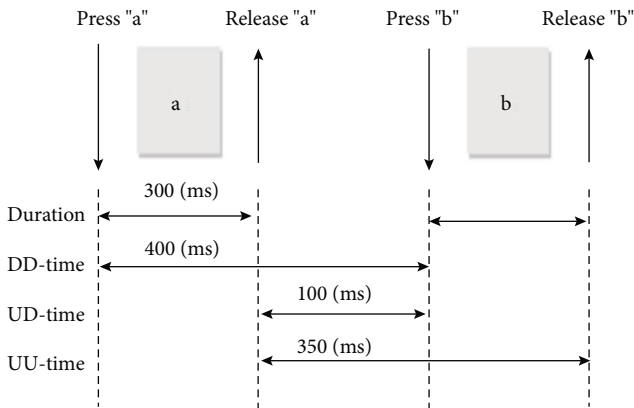


FIGURE 2: Timing features of KDA.

sum of negative values, and standard deviation. Since the error rate was improved when the “mean” formula of motion data was added, we employ the mean formula in our study.

3.3. Preprocessing. Each user has a distinct pattern when typing on a keyboard. However, a user may unintentionally deviate from his or her specific range of data by mistakenly performing an action that does not match the usual pattern. Therefore, outlier data for each participant were detected using an interquartile range. Then, these data were removed before feeding the classifiers to improve classification performance. For features that include more than one dimension, such as acceleration, gyroscope, and coordination, we remove the common value of outliers between these dimensions. For example, the record will be deleted if the three dimensions of acceleration have common outlier values.

Figure 8 graphically illustrates the boxplot for each feature and the removed outlier values.

3.4. Classification. After extracting the users’ typing features and creating their profile templates, a classification process was undertaken to determine the similarities and differences between the users’ templates. In particular, the standardized classifiers were used, including artificial neural network (ANN), KNN, SVM, Euclidean distance, Manhattan distance, and random forest, which were written using Python. Each of these classifiers is explained as follows.

An ANN is a series of algorithms that determine relationships within a dataset through a process that operates similarly to a human brain. Although there are several ANNs, our study utilized MLP owing to its high performance confirmed by recent studies [34].

Moreover, KNN estimates how likely a data point is to be a member of one group based on data points of which groups are nearest to it. SVM is a supervised machine learning algorithm used for both classification and regression. It aims to find a hyperplane in an N -dimensional space, where N is the number of features that distinctly classify the data points. Random forest unsystematically creates and merges multiple decision trees into one “forest.” The goal is not to rely on a single learning model but instead on a collection of decision models for improving accuracy. The Euclidean distance involves calculating the distance between two n -dimensional vectors $p(p_1, p_2, \dots, p_n)$ and $q(q_1, q_2, \dots, q_n)$ in a straight line. Its formula is given by Equation (1):

$$d(p, q) = \sqrt{\sum_{i=1}^n (q_i - p_i)^2}. \quad (1)$$

The Manhattan distance calculates the distance between two n -dimensional vectors, $p(p_1, p_2, \dots, p_n)$ and $q(q_1, q_2, \dots, q_n)$, by subtracting the values and then summing their absolute values, as shown in Equation (2).

$$d(p, q) = \sum_{i=1}^n |q_i - p_i|. \quad (2)$$

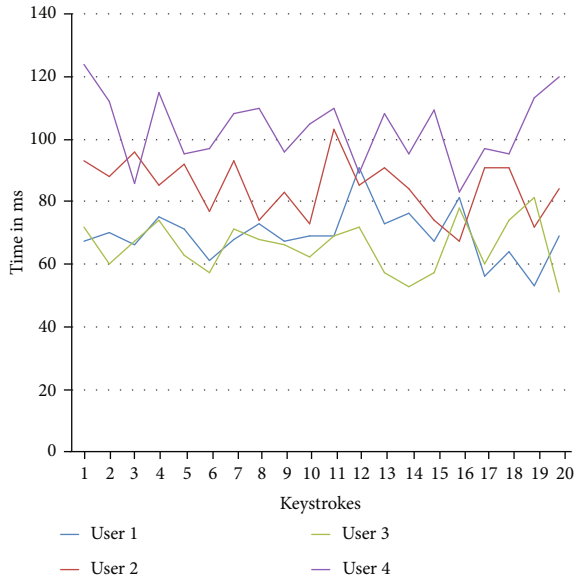


FIGURE 3: Hold time for four users.

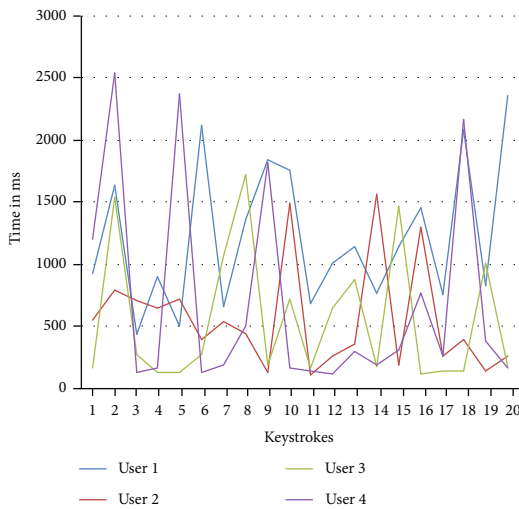


FIGURE 4: Di-graph duration for four users.

4. Evaluation

A controlled laboratory experiment was conducted in which the participants were asked to use the developed application. The following sections present the setup and procedure of the experiment.

4.1. Experimental Setup. This experiment involved various subjects as normal users. In the following section, the design of the experiment is provided, along with a description of the participants, the materials involved, and the systems in the experiment.

4.1.1. Experimental Design. The experiment was conducted in a controlled laboratory so that distributions made no interference, and the desired data could be collected without any biases. The experiment was divided into two sessions. In

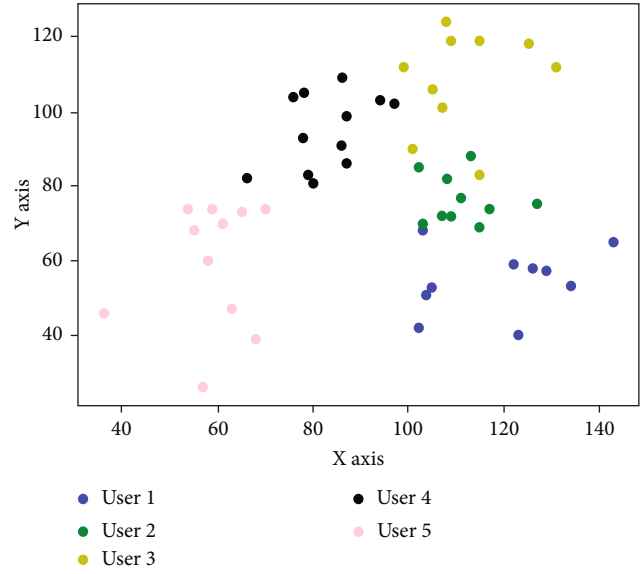


FIGURE 5: C_x and C_y of five users who press one key.

each session, the participants were required to enter one of the two keystroke authentication techniques, namely, fixed text or free text. Each session lasted 15 minutes, and there was a 10-minute break between sessions.

4.1.2. Participants. We recruited 45 participants, and the experiment was conducted for three weeks. The participants had varying typing skills and were between 19 and 25 years of age. All the participants were undergraduate students from different disciplines, and they were all native speakers. Most participants had a technical background. As demonstrated by Lee et al. [32], FAR is reduced in the case of the opposite gender for legitimate users. Therefore, to obtain adequate results, all participants in our experiment were women.

4.1.3. Materials. The stimulus material provided to the participants comprised two texts: a sign-up text and a log-in text. When the fixed text class was used, each participant entered the required phrase at least ten times for the sign-up phase and once for the log-in phase. One sample comprised 20 characters, as suggested by Lee et al. [32]. This study demonstrated that accuracy was the same in the first 20 actions. Subsequently, when the number of user actions was increased from 20 to 40, the user’s input waiting time doubled with minor improvements in accuracy. In contrast, the sign-up text in the free text condition was 200 characters, whereas it was 198 characters in the log-in session. Although many studies have preferred to use a short free text [23, 40], it might not be enough to use only short texts to analyze keystrokes as they may not provide sufficient information for discriminating among users. Other studies [41, 42] have preferred a long free text. Huang et al. [41] argued that the reference profiles required 10,000 keystrokes, whereas a testing sample requires 1,000 keystrokes to produce satisfactory authentication performance. However, users might not find it convenient to enter longer texts. Therefore, an

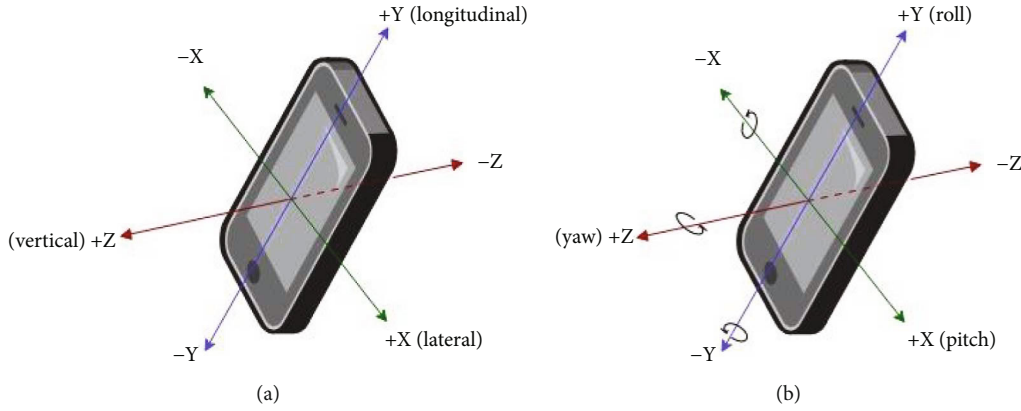


FIGURE 6: Axes of the motion sensors: (a) acceleration; (b) gyroscope.

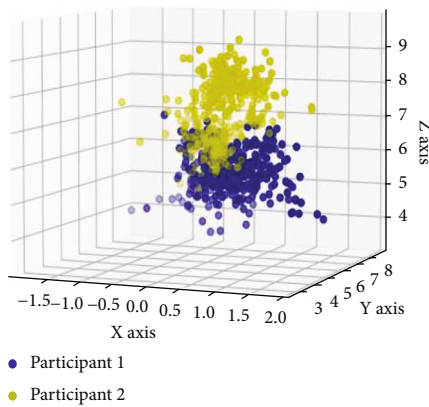


FIGURE 7: Scatter plot of three axes of acceleration data for two participants.

intermediate value was selected to determine the lengths of the characters. Table 3 shows the keystroke data collected during each session.

4.1.4. System. The proposed system was implemented on a Java Android application installed on an Android device. It was designed for users with varying technical experience. The application comprises the main page on which users can select one of the two keystroke biometric classes: free and fixed texts. Both classes are similar in terms of circumstance, which is as follows: after the user has selected the required technique, the page for entering the user's email address will be displayed. This page includes a text box in which the email address can be typed along with a button to check the validity of the email address. When the correct email address is entered, the sign-up page is shown, which has the required text to enter and the textbox to enter this text, as shown in Figure 9. When the user presses the submit button, the written text is matched with the required text; data features and the email address will be saved locally in the database. In contrast, when the text fails to match, an error page will be displayed, after which the user can make another attempt. After the sign-up phase, the user is directed to the log-in page.

Android does not have any mechanism to monitor the keyboard for security purposes, such as implementing a key-

logger [30]. Thus, it was essential to design and implement a custom keyboard, which could be easily installed on each device used to authenticate users. This keyboard was developed for all touchscreen Android mobile devices.

4.1.5. Evaluation Metrics. Three metrics were used to evaluate the accuracy of the biometric authentication system: false rejection rate (FRR), false acceptance rate (FAR), and EER. FAR is the percentage ratio of the number of acceptances of an imposter user as a legitimate user. A low FAR indicates that fewer illegitimate users were falsely accepted, thereby indicating increased security.

FRR is the percentage ratio of rejecting a legitimate user by considering him/her to be an imposter. A low FRR indicates that fewer legitimate users were falsely rejected, thereby indicating the increased usability of the method.

EER is a single-number performance metric used to measure and compare the accuracy of various biometric systems. This metric is obtained by placing a graph, one for FAR and one for FRR, against a matching threshold, and then taking the interception point of the two graphs. The EER formula is given by Equation (3).

$$\text{EER} = \frac{\text{FAR} + \text{FRR}}{2}. \quad (3)$$

Usually, a low FRR and a low FAR result in a lower EER. A lower EER indicates a good performance using a biometric authentication method. However, because FAR and FRR are negatively correlated, it is impractical to lower both metrics.

4.2. Experimental Procedure. This section explains how the experiment was conducted—instructions for the participants, the experimental process, and the data collection procedure.

4.2.1. Instructions to Participants. The participants were initially instructed to type the provided text as normal. All participants were required to switch off their phones (or set them to silent) and avoid chatting with friends. This was done to prevent any interruption during typing. All participants were asked to sit while holding the smartphone in their hands, as this position yielded more accuracy, as stated

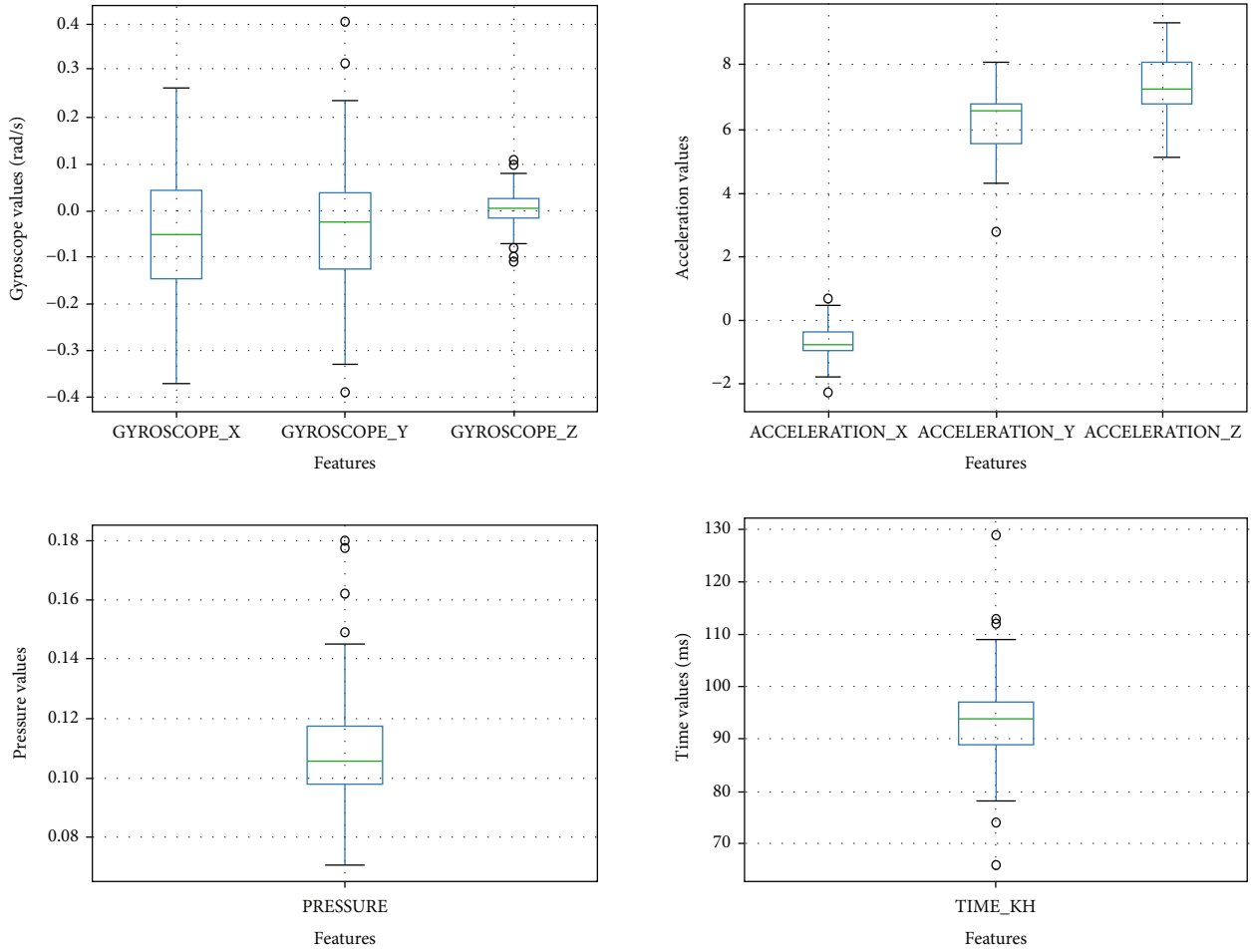


FIGURE 8: Boxplots of the feature data for one user.

TABLE 3: Experimental settings of collected keystroke data.

Session#	Technique type	Number of training samples	Number of testing samples	Number of actions in sign-up phase	Number of actions in log-in phase
First session	Free text	1	1	200	198
Second session	Fixed text	10	1	200	20

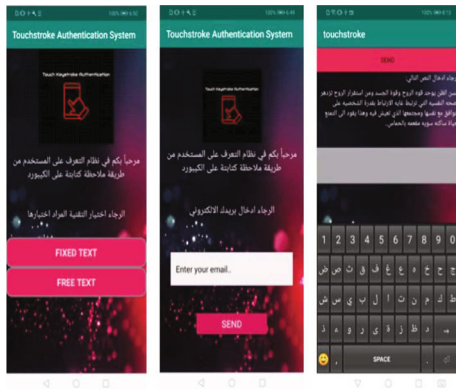


FIGURE 9: Interfaces of an Android-based keystroke collector.

in [31]. Before beginning the experiment, the participants were given some time to test the system by discarding the first trial. During typing, the participants were told that they could use the backspace or spacebar keys when needed. Lastly, a confirmation message was shown, indicating that the experiment has ended.

4.2.2. *Procedure.* The procedure was implemented in two distinct phases to authenticate users using KDA on mobile phones. The first phase of enrolment is also known as profile building. In this phase, the typing rhythm was collected in different trials to select the most similar profiles for the typing behavior of the user. For the second phase, the user was required to enter the log-in text, which was matched and compared with the stored text. Each time, the authenticated

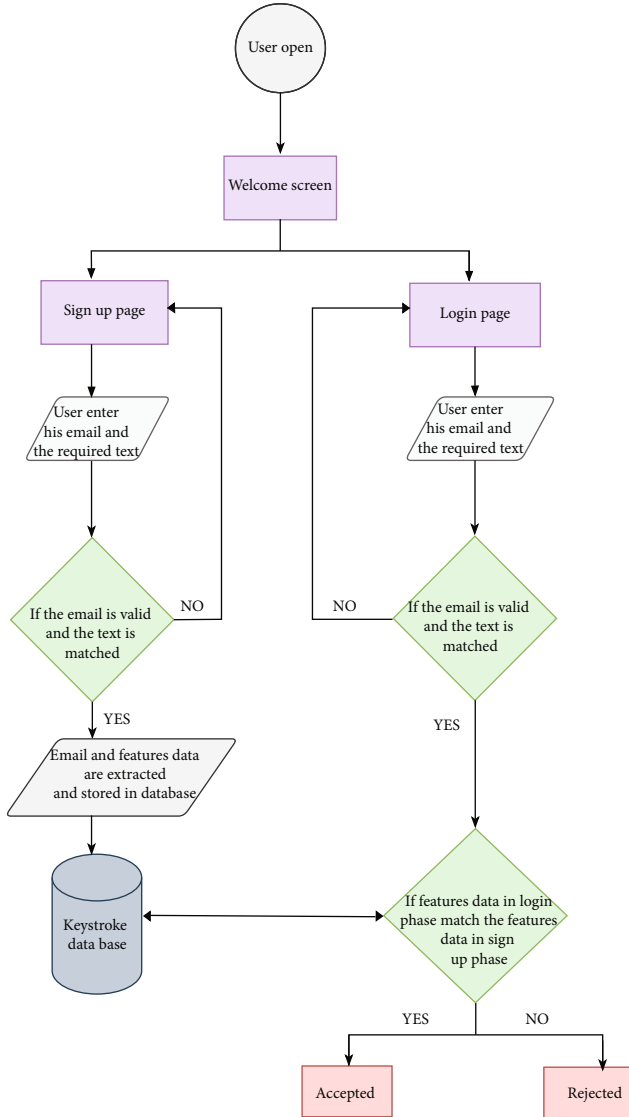


FIGURE 10: Flowchart of the proposed system.

user was required to enroll with the system for comparison with the profile stored in the database. A flowchart is shown in Figure 10.

4.2.3. Collected Data. For every successful attempt, a user profile was created, which included data for time keystrokes, accelerometers, gyroscopes, pressures, and coordinates. Table 4 shows all 13 features for each class; however, the number of dimensions is different. In particular, in a fixed text class, every sample comprises 20 sets of 13 features. Hence, by subtracting three values from DD, PP, and UD features, a single sample comprises 257 fields. Conversely, in the free text class, whenever a participant touched a particular key on the keyboard, it was presented as 13 features, where each feature appears in a single dimension in DB. Subsequently, the mean, maximum, and minimum for each feature are stored in another table.

TABLE 4: Features and dimensions for each KDA class.

Feature set	Description	Number of dimensions	
		1 sample (20 characters) (fixed text)	(Free text)
Time	Hold time	20	1
	Flight time (DD)	19	1
	Flight time (PP)	19	1
Coordination	Di-graph duration	19	1
	At TouchDown	40	2
Pressure	At TouchDown	20	1
	At TouchDown	60	3
Gyroscope	At TouchDown	60	3
	At TouchDown	60	3
# of features		13	13
# of dimensions		257	13

5. Results

All participants successfully completed their tasks in three weeks. The level of accuracy obtained in the research indicates that this approach can improve the performance of touch-based systems when typing in Arabic. Specifically, the combination of the five features, namely, time, acceleration, coordination, pressure, and gyroscope, by applying a random forest classifier yields 0.0% EER using a free text database and 0.086% EER using a fixed text database, as shown in Figures 11 and 12. Although we have compared between our results and prior studies' results in Table 1, Table 5 compares between our approach and the result of [12]. This shows clearly that our approach is more usable due to the less number of keystrokes, though the accuracy rate of both studies was the same (0.0 EER).

This section presents the results, first with machine learning methods and then with distance-based metrics.

5.1. Machine Learning Methods. It is evident from Figures 11 and 12 that the free text class has a low FAR in comparison to the fixed text class. For example, the KNN classifier scored the FAR of 0% with the free class using a combination of features. However, in the fixed text class, the FAR was 0.34%. Notably, applying the coordination feature in the fixed text database yielded a better FRR than that in the free text database. In the fixed text classifier, the best result obtained was 0.18% FRR, whereas in the free text classifier, the FRR reached 0.6% using SVM.

5.2. Distance-Based Metrics. This experiment utilized two popular distance matrices: Manhattan and Euclidean distances. As suggested by Alsuhibany et al. [18], the standard deviation of the user's profile was utilized to set a threshold for the Euclidean distance. Therefore, we used this threshold for both Euclidean

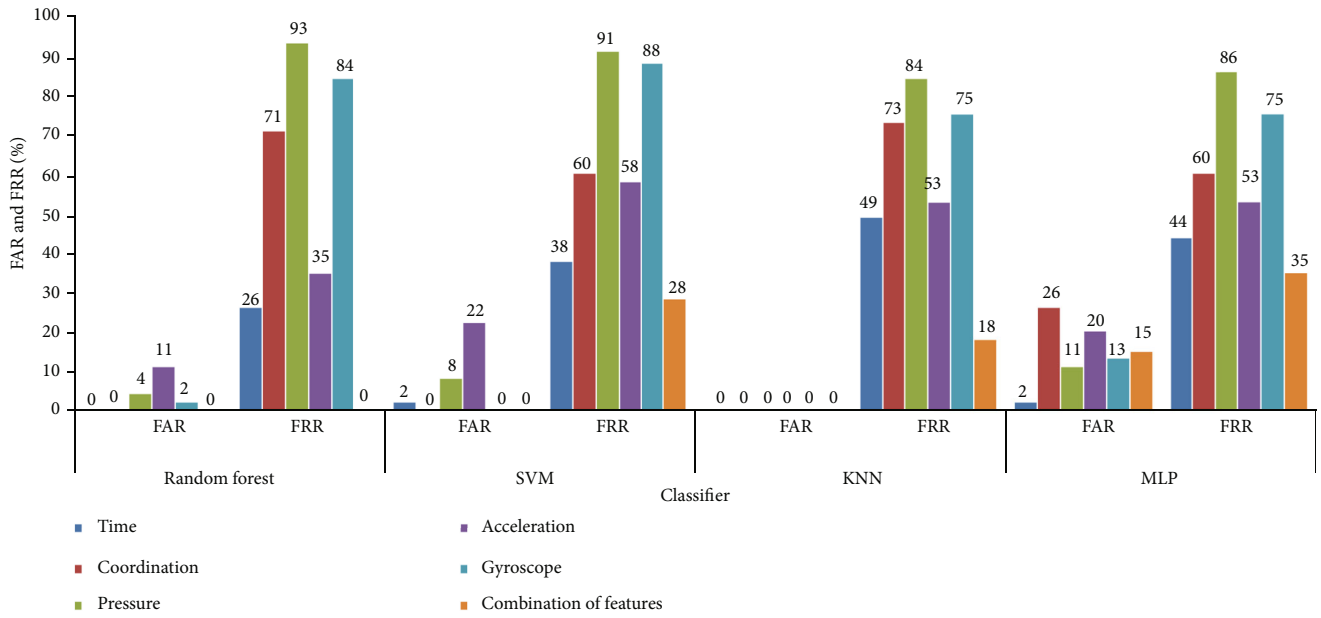


FIGURE 11: FAR and FRR for each supervised classifier using the free text class.

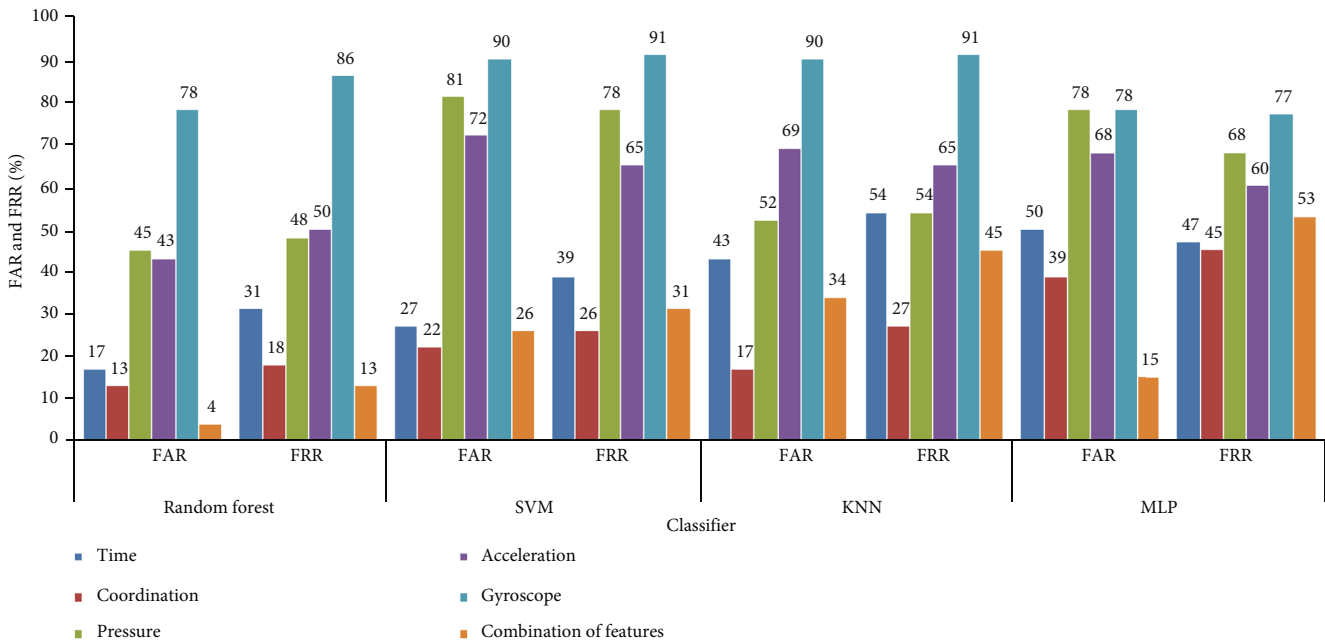


FIGURE 12: FAR and FRR for each supervised classifier using the fixed text class.

TABLE 5: A comparison of our system result and the result of [12].

Study	Methodology	Features	Classifier	EER
[12]	10 samples of 200 keystrokes each	Time, acceleration, and coordination	TT, R, TTPR, TTMR, Kolmogorov-Smirnov statistic, and Cramér-von Mises criterion (CM)	0.0
Our study	200 keystrokes	Time, acceleration, gyroscope, pressure, and coordination	ANN, KNN, SVM, Euclidean distance, Manhattan distance, and random forest	0.0

and Manhattan distances. To enhance the performance of the Manhattan distance, the threshold was changed to the summation of the standard deviations of the two users’ profiles, which

tends to engage in the process of authentication. This result is shown in Table 6, where it is evident that the performance of the Manhattan distance using the free text class has been

TABLE 6: Difference between two thresholds using the Manhattan distance in the free text class.

	Time		Coordination		Pressure		Acceleration		Gyroscope		Combination of features	
	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR
First threshold	10	15	80	5	30	0	10	40	0	90	30	35
Second threshold	0	15	80	0	10	0	25	0	15	10	10	15

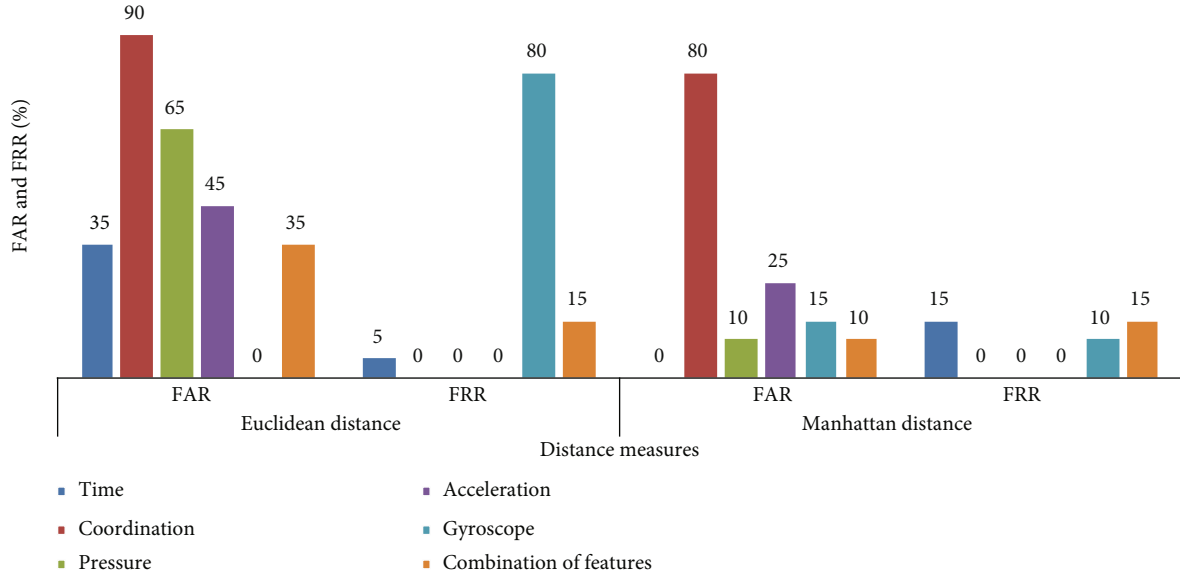


FIGURE 13: FAR and FRR for each distance-based metric using the free text class.

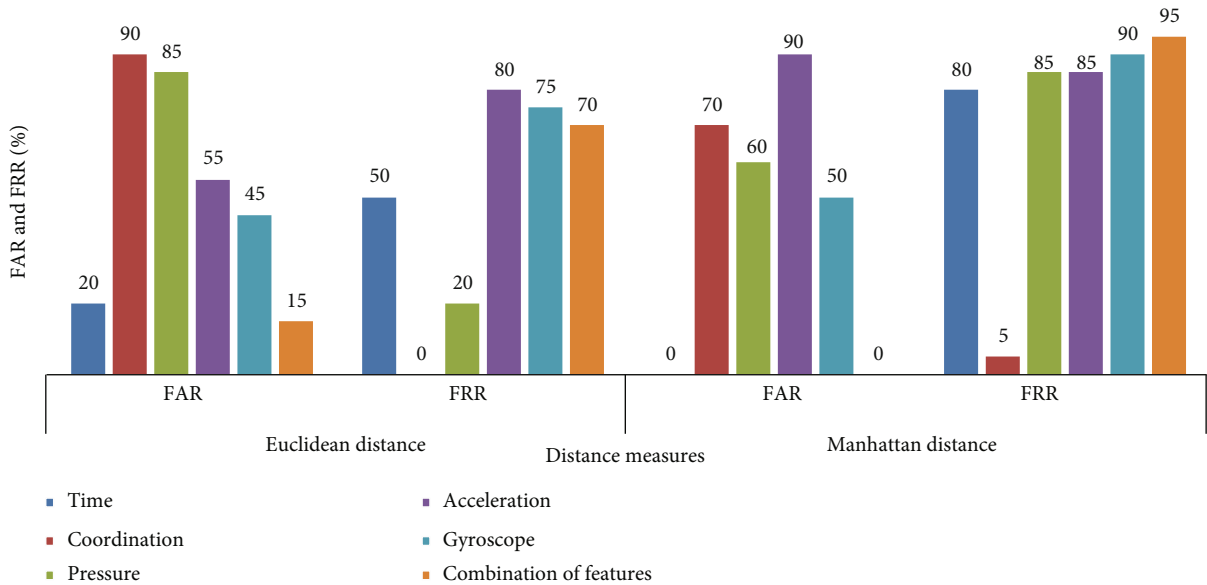


FIGURE 14: FAR and FRR for each distance-based metric using the fixed text class.

significantly increased using the second threshold. In fact, the results of the fixed text class remain unchanged even after setting the new threshold. The results of the two text classes were acceptable, as shown in Figures 13 and 14.

6. Discussion

This section interprets the results obtained using machine learning methods and distance-based metrics.

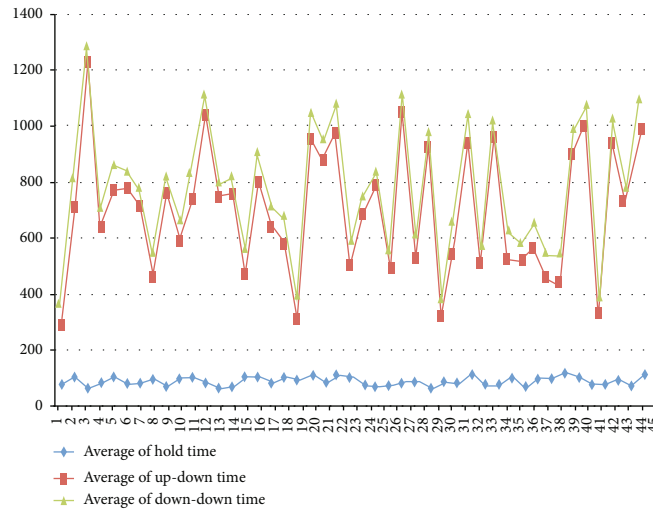


FIGURE 15: Average of the hold time, Up-Down time, and Down-Down time for each user.

6.1. Machine Learning Methods. This section compares the results based on three distinct points: the keystroke dynamic class, method of classification, and features. That is, a low FAR indicates a higher level of security. In this case, since the free text has a low FAR, it indicates that the free text is more secure than the fixed text. This may be attributed to the size of the text, which was provided in the log-in phase of the free text technique because it was longer than that in the fixed text technique. Consequently, it will be challenging for an intruder to imitate the typing pattern of the user for a longer text.

The obtained results are consistent with Alsultan and Warwick [43]—the free text ensures more safety and security than the fixed text from many threats, such as spyware, shoulder surfing, and social engineering. Hence, it can be concluded that as more keystrokes are input in the log-in phase, a more robust authentication model will be achieved. However, from the perspective of system users, inputting considerable keystrokes may be inconvenient.

In contrast, a lower FRR indicates increased usability. Since coordination achieved better FRR through fixed text, it ensures enhanced usability for the fixed text category, implying that every user has a particular coordinate for each button, as shown in Figure 5. Thus, this feature is rendered more convenient in the fixed text class.

Therefore, to determine the most appropriate machine learning method for the classification engine of the proposed system, the study undertook several preliminary classification experiments, which included four popular classifiers: SVM, MLP, k-NN, and random forest. As suggested by Kambourakis et al. [30], k-NN and random forest classifiers were most crucial in performance on mobile devices. This refers to the fact that a user will select not only the most effective algorithm in classification but also the one that promptly executes commands over the handheld device or smartphone, despite limited memory and CPU. In addition to the increased performance of the random forest classifier, it yielded higher accuracy as it outperformed the other three classifiers with the most features. In contrast, in addition to

the less effective result produced by MLP, in Kambourakis et al. [30], the MLP classifier was excluded because it could not run on limited memory capacity. Thus, it can be inferred that random forest is the best option for the KDA system because it can run on low-memory devices.

Furthermore, Figure 11 (free text) clearly indicates that the combination of all features delivers the best results using all four classifiers. When each feature is used independently, time is the best feature, followed by acceleration. Figure 15 depicts the average of the hold-time, UP time, and DD time using the free text class, implying that the time features are unique for each person, except for a few users who can be distinguished by their other features. Figure 12 (fixed text) implies that combining all the features provides better results in two classifiers: random forest and MLP. In contrast, the coordination feature was the highlight feature in the case of SVM and KNN classifiers.

In general, it was observed that the combination of different features delivered highly accurate results in both fixed and free texts. Additionally, time was a crucial feature in the free text technique, whereas coordination was more effective in the fixed text technique.

6.2. Distance-Based Metrics. Two parameters that influence the accuracy of distance-based metrics are the number of keystrokes used in the testing phase and the threshold. In the fixed text technique, the classification is intended to determine whether a user is legitimate by computing the distance between the mean point of reference samples and the one sample used in the log-in phase, comprising merely 20 letters. Conversely, in the free text technique, the distance computes the difference between the mean point of the sign-up data and the mean point of the log-in data, comprising 198 letters. This is an explanation for the higher results obtained using the free text class. Therefore, it is suggested to increase the number of samples entered by the user in the log-in phase in the fixed text class to three samples [31]. When the threshold was altered in the Manhattan distance, there was an increase in performance using the free

text. Hence, notably, the new threshold for the Manhattan distance, the Manhattan distance outperformed the Euclidean distance.

7. Conclusion and Future Works

This research extended the previous studies on KDA that used Arabic with conventional keyboards by investigating KDA in Arabic on soft keyboards. Currently, touchscreen devices are embedded with sensors that can improve the performance of the system. This study extracted five features to determine the keystroke patterns of the users: accelerometer, time, touch coordinates, touch pressure, and gyroscope sensor. The performance of the features was assessed using six methods of validation: SVM, KNN, Euclidean distance, Manhattan distance, random forest, and neural network. The system was analyzed through two keystroke dynamic classes: free text and fixed text, for determining the most effective approach. Subsequently, the results of both techniques were compared.

The results indicate that a verification system using Arabic is possible with touchscreen devices and can enhance security. It exhibits a higher rate of accuracy using the free text class, with an average EER of 0.0%, whereas an average EER of 0.08% can be obtained by using the fixed text class when combining the features and the random forest classifier. Among both KDA classes, the free text class had a lower FAR throughout the entire study, irrespective of the feature set used, thereby implying that the free text is more secure than the fixed text.

To improve our results, the experiments will be carried out on a tablet device to investigate whether the size of the screen has any impact on authentication accuracy. Moreover, additional classifiers, which were not a part of this study, can be included, and advanced scenarios, features, and methodologies can be considered in the future. Lastly, the number and diversity of the participants should be increased in the future experiments to better assess the associated outcomes with this particular behavioral trait.

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

The researchers would like to thank the Deanship of Scientific Research, Qassim University for funding the publication of this project.





References

- [1] "Number of smartphone users in the U.S. 2010-2023," March 2021, <https://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/>.
- [2] "Smartphone users in South Korea 2015-2025," March 2021, <https://www.statista.com/statistics/467171/forecast-of-smartphone-users-in-south-korea/>.
- [3] "Cybersecurity statistics report," March 2021, <https://preyproject.com/blog/en/cybersecurity-statistics/>.
- [4] "Development of Android malware worldwide 2016-2020," March 2021, <https://www.statista.com/statistics/680705/global-android-malware-volume/>.
- [5] "Distribution of Android malware 2019," March 2021, <https://www.statista.com/statistics/681006/share-of-android-types-of-malware/>.
- [6] P. S. Teh, N. Zhang, A. B. J. Teoh, and K. Chen, "TDAS: a touch dynamics based multi-factor authentication solution for mobile devices," *International Journal of Pervasive Computing and Communications*, vol. 12, no. 1, pp. 127–153, 2016.
- [7] Y. Wang, C. Wu, K. Zheng, and X. Wang, "Improving reliability: user authentication on smartphones using keystroke biometrics," *IEEE Access*, vol. 7, 2019.
- [8] J. Han, S. M. Kywe, Q. Yan et al., "Launching generic attacks on iOS with approved third-party applications," in *International Conference on Applied Cryptography and Network Security*, M. Jacobson, M. Locasto, P. Mohassel, and R. Safavi-Naini, Eds., vol. 7954 of Lecture Notes in Computer Science, pp. 272–289, Springer, 2013.
- [9] O. Berkman and O. M. Ostrovsky, "The Unbearable Lightness of PIN Cracking," in *Financial Cryptography and Data Security*, pp. 224–238, Springer, 2007.
- [10] C. Sousedik and C. Busch, "Presentation attack detection methods for fingerprint recognition systems: a survey," *IET Biometrics*, vol. 3, no. 4, pp. 219–233, 2014.
- [11] N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks and anti-spoofing with kinect," in *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pp. 1–8, Arlington, VA, USA, 2013.
- [12] J. Kim and P. Kang, "Freely typed keystroke dynamics-based user authentication for mobile devices based on heterogeneous features," *Pattern Recognition*, vol. 108, 2020.
- [13] M. El-Abed, M. Dafer, and C. Rosenberger, "RHU keystroke touchscreen benchmark," in *2018 international conference on Cyberworlds (CW)*, pp. 363–368, Singapore, 2018.
- [14] M. Trojahn, F. Arndt, and F. Ortmeier, "Authentication with keystroke dynamics on touchscreen keypads-effect of different n-graph combinations," in *3rd International Conference on Mobile Services, Resources, and Users (MOBILITY)*, pp. 114–119, Lisbon, Portugal, 2013.
- [15] P. Gautam and P. R. Dawadi, "Keystroke biometric system for touch screen text input on android devices optimization of equal error rate based on medians vector proximity," in *2017 11th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)*, pp. 1–7, Malabe, Sri Lanka, 2017.
- [16] A. Alsultan, K. Warwick, and H. Wei, "Free-text keystroke dynamics authentication for Arabic language," *IET Biometrics*, vol. 5, no. 3, pp. 164–169, 2016.
- [17] S. A. Alsuhibany, M. Almushyti, N. Alghasham, and F. Alkhudier, "Analysis of free-text keystroke dynamics for Arabic language using Euclidean distance," in *2016 12th International Conference on Innovations in Information Technology (IIT)*, pp. 1–6, Al Ain, United Arab Emirates, 2016.
- [18] S. A. Alsuhibany, M. Almushyti, N. Alghasham, and F. Alkhudier, "Investigating the effectiveness of Arabic

- language for free-text keystroke dynamics authentication,” *International Journal of Computer Science and Software Engineering*, vol. 6, 2017.
- [19] A. Alsultan, K. Warwick, and H. Wei, “Non-conventional keystroke dynamics for user authentication,” *Pattern Recognition Letters*, vol. 89, pp. 53–59, 2017.
- [20] X. Lu, S. Zhang, P. Hui, and P. Lio, “Continuous authentication by free-text keystroke based on CNN and RNN,” *Computers & Security*, vol. 96, 2020.
- [21] B. Ayotte, J. Huang, M. K. Banavar, D. Hou, and S. Schuckers, “Fast continuous user authentication using distance metric fusion of free-text keystroke data,” in *2019 IEEE/CVF conference on computer vision and pattern recognition workshops (CVPRW)*, pp. 2380–2388, Long Beach, CA, USA, 2019.
- [22] C.-J. Tsai and K.-J. Shih, “Mining a new biometrics to improve the accuracy of keystroke dynamics-based authentication system on free-text,” *Applied Soft Computing*, vol. 80, pp. 125–137, 2019.
- [23] A. A. Ahmed and I. Traore, “Biometric recognition based on free-text keystroke dynamics,” *IEEE Transactions on Cybernetics*, vol. 44, no. 4, pp. 458–472, 2014.
- [24] P. Kang and S. Cho, “Keystroke dynamics-based user authentication using long and free text strings from various input devices,” *Information Sciences*, vol. 308, pp. 72–93, 2015.
- [25] B. Draffin, J. Zhu, and J. Zhang, “Keysens: Passive User Authentication through Micro Behavior Modeling of Soft Keyboard Interaction,” in *International Conference on Mobile Computing, Applications, and Services*, pp. 184–201, Springer, 2013.
- [26] H. Gascon, S. Uellenbeck, C. Wolf, and K. Rieck, “Continuous authentication on mobile devices by analysis of typing motion behavior,” in *Schutz und Zuverlässigkeit*, pp. 1–12, Gesellschaft für Informatik e.V., 2014.
- [27] A. Buriro, B. Crispo, F. Del Frari, and K. Wrona, “Touchstroke: smartphone user authentication based on touch-typing biometrics,” in *New Trends in Image Analysis and Processing – ICIAP 2015 Workshops*, pp. 27–34, Springer, 2015.
- [28] H. Saevanee and P. Bhattarakosol, “Authenticating user using keystroke dynamics and finger pressure,” in *2009 6th IEEE Consumer Communications and Networking Conference*, pp. 1–2, Las Vegas, NV, USA, 2009.
- [29] N. Zheng, K. Bai, H. Huang, and H. Wang, “You are how you touch: user verification on smartphones via tapping behaviors,” in *2014 IEEE 22nd International Conference on Network Protocols*, pp. 221–232, Raleigh, NC, USA, 2014.
- [30] G. Kambourakis, D. Damopoulos, D. Papamartzivanos, and E. Pavlidakis, “Introducing touchstroke: keystroke-based authentication system for smartphones,” *Security and Communication Networks*, vol. 9, no. 6, 554 pages, 2016.
- [31] J.-H. Roh, S.-H. Lee, and S. Kim, “Keystroke dynamics for authentication in smartphone,” in *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 1155–1159, Jeju, Korea (South), 2016.
- [32] H. Lee, J. Y. Hwang, D. I. Kim, S. Lee, S.-H. Lee, and J. S. Shin, “Understanding keystroke dynamics for smartphone users authentication and keystroke dynamics on smartphones built-in motion sensors,” *Security and Communication Networks*, vol. 2018, Article ID 2567463, 10 pages, 2018.
- [33] M. J. Coakley, J. V. Monaco, and C. C. Tappert, “Keystroke biometric studies with short numeric input on smartphones,” in *2016 IEEE 8th International Conference on Biometrics The-ory, Applications and Systems (BTAS)*, pp. 1–6, Niagara Falls, NY, USA, 2016.
- [34] S. Sen and K. Muralidharan, “Putting ‘pressure’ on mobile authentication,” in *2014 Seventh International Conference on Mobile Computing and Ubiquitous Networking (ICMU)*, pp. 56–61, Singapore, 2014.
- [35] A. Salem, A. Sharieh, A. Sleit, and R. Jabri, “Enhanced authentication system performance based on keystroke dynamics using classification algorithms,” *KSII Transactions on Internet and Information Systems*, vol. 13, no. 8, p. 8, 2019.
- [36] M. Ehatisham-Ul-Haq, M. A. Azam, J. Loo et al., “Authentication of smartphone users based on activity recognition and mobile sensing,” *Sensors*, vol. 17, no. 9, p. 2043, 2017.
- [37] I. de Mendizabal-Vazquez, D. de Santos-Sierra, J. Guerra-Casanova, and C. Sanchez-Avila, “Supervised classification methods applied to keystroke dynamics through mobile devices,” in *2014 International Carnahan Conference on Security Technology (ICCST)*, pp. 1–6, Rome, Italy, 2014.
- [38] D. Gunetti, C. Picardi, and G. Ruffo, “Keystroke Analysis of Different Languages: A Case Study,” in *International Symposium on Intelligent Data Analysis*, pp. 133–144, Springer, 2005.
- [39] T. Samura and H. Nishimura, “Keystroke timing analysis for individual identification in Japanese free text typing,” in *2009 ICCAS-SICE*, pp. 3166–3170, Fukuoka, Japan, 2009.
- [40] F. Monroe and A. Rubin, “Authentication via keystroke dynamics,” in *CCS '97: Proceedings of the 4th ACM conference on Computer and communications security*, pp. 48–56, New York, NY, USA, 1997.
- [41] J. Huang, D. Hou, S. Schuckers, and Z. Hou, “Effect of data size on performance of free-text keystroke authentication,” in *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015)*, pp. 1–7, Hong Kong, China, 2015.
- [42] J. Huang, D. Hou, and S. Schuckers, “A practical evaluation of free-text keystroke dynamics,” in *2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*, pp. 1–8, New Delhi, India, 2017.
- [43] A. Alsultan and K. Warwick, “Keystroke dynamics authentication: a survey of free-text methods,” *International Journal of Computer Science Issues*, vol. 10, 2013.

Research Article

Enabling Efficient Decentralized and Privacy Preserving Data Sharing in Mobile Cloud Computing

Jiawei Zhang ¹, Ning Lu ^{2,3}, Teng Li ¹ and Jianfeng Ma ¹

¹School of Cyber Engineering, Xidian University, Xi'an, China

²School of Computer Science and Technology, Xidian University, Xi'an, China

³College of Computer Science and Engineering, Northeastern University, Qinhuangdao, China

Correspondence should be addressed to Ning Lu; luning@neuq.edu.cn

Received 2 July 2021; Revised 31 July 2021; Accepted 10 August 2021; Published 2 September 2021

Academic Editor: Weizhi Meng

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

Mobile cloud computing (MCC) is embracing rapid development these days and able to provide data outsourcing and sharing services for cloud users with pervasively smart mobile devices. Although these services bring various conveniences, many security concerns such as illegally access and user privacy leakage are inflicted. Aiming to protect the security of cloud data sharing against unauthorized accesses, many studies have been conducted for fine-grained access control using ciphertext-policy attribute-based encryption (CP-ABE). However, a practical and secure data sharing scheme that simultaneously supports fine-grained access control, large universe, key escrow free, and privacy protection in MCC with expressive access policy, high efficiency, verifiability, and exculpability on resource-limited mobile devices has not been fully explored yet. Therefore, we investigate the challenge and propose an Efficient and Multiauthority Large Universe Policy-Hiding Data Sharing (EMA-LUPHDS) scheme. In this scheme, we employ fully hidden policy to preserve the user privacy in access policy. To adapt to large scale and distributed MCC environment, we optimize multiauthority CP-ABE to be compatible with large attribute universe. Meanwhile, for the efficiency purpose, online/offline and verifiable outsourced decryption techniques with exculpability are leveraged in our scheme. In the end, we demonstrate the flexibility and high efficiency of our proposal for data sharing in MCC by extensive performance evaluation.

1. Introduction

As an emerging paradigm, mobile cloud computing (MCC) is growing exponentially and facilitates the deployment of enormous mobile devices covering public and private sectors [1]. The MCC systems provide not only strong mobility but also abundant computing and storage capacity for these resource-limited devices which prefer to outsource their data to MCC for cost saving [2]. Moreover, assisted by the data sharing service of MCC, users are able to conveniently enjoy various applications, such as smart home, smart office, and intelligent transportation, with pervasive and smart mobile devices [3]. In particular, this trend is being accelerated with the implementation of 5G communication network offering massive high-speed access capacity [4]. As shown in Figure 1, users

can share their data in MCC conveniently with different kinds of mobile devices, e.g., laptops, cellphones, through gNBs (i.e., next generation NodeB) of 5G network, or even satellites receiving station on various sites (e.g., home, hotel, plain, or car). Although MCC, such as iCloud and OneDrive, can provide a variety of benefits to mobile users, the data security issues, i.e., data confidentiality and fine-grained access control, have become important stumbling blocks for the usage of MCC [5]. The data outsourced to MCC may contain numerous sensitive information or significant assets relevant to mobile users and terminates [6]. Thus, the most critical data security concern is the data access control issues that allows only authorized users while prevents unauthorized ones from accessing the shared data in MCC as it will cause severe consequences if the private information is leaked.

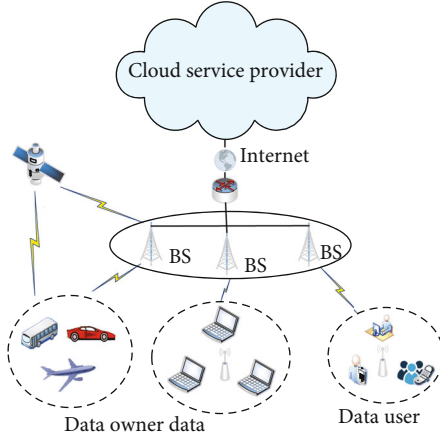


FIGURE 1: The architecture of mobile cloud computing.

Therefore, how to protect these sensitive data outsourced in MCC remains an urgent challenge. As a promising technique, ciphertext-policy attribute-based encryption (CP-ABE) [7–9] can be adopted to provide fine-grained data access control when user data is shared with multiple users. Nevertheless, the conventional CP-ABE schemes are unsuitable to be directly utilized in secure data sharing of the MCC system as there still exist several issues. First of all, in general CP-ABE schemes, ciphertexts are stored in Cloud Service Provider (CSP) and shared with multiple users together with the access policies which are in plaintext and may cause user privacy leakage [7]. Moreover, a MCC system involves large amount of mobile devices and users, and standard CP-ABE schemes with bounded attribute universe and single attribute authority are no longer satisfactory due to their inflexibility, key escrow, and single-point failure problems [10]. Furthermore, as the CSPs are untrusted in terms of users, they may misbehave in outsourced decryption by returning previous results or even random and false results to users [2]. In addition, the low efficiency in encryption and decryption is an inferior drawback for traditional CP-ABE schemes when used in MCC with enormous resource-limited mobile devices. Thus, it is urgent to design a practical data access control scheme for data sharing in MCC that can address these issues.

To find out a solution, many works have made great progresses. The scheme in [11] solves the problem of bounded attribute universe, key escrow, and single-point failure problem while it cannot support policy privacy preserving and decryption verifiability. Meanwhile, the schemes in [12, 13] support efficient encryption and exculpable decryption as well as multiauthority and policy hidden, respectively. Recently, the authors in [6, 7] proposed two CP-ABE schemes with privacy preserving and expressive policy, but both of them do not support large attribute universe and exculpability of decryption. Then, the scheme in [1] provides features of multiauthority, large attribute universe, and high efficiency to resist key escrow problem, but it cannot satisfy policy preserving and verifiability with exculpability. Besides, such schemes do not consider the issue of exculpability as in some cases, and CSP acts honestly may be

framed by users. Although the scheme in [14] fixed this problem, it fails to protect the user privacy in policies. Hence, it is urgent to devise a significant data sharing scheme that is addressing all these drawbacks in traditional CP-ABE schemes at the same time when used in MCC, including key escrow resistance, large attribute universe, privacy preserving, expressive policy, and efficiency.

1.1. Our Contributions. Confronting the above problems, we propose an Efficient and Multiauthority Large Universe Policy-Hiding Data Sharing (EMA-LUPHDS) scheme to achieve key escrow resistance, expressive access policies, and high efficiency for data sharing of MCC with resource-limited mobile devices by extending the decentralized CP-ABE scheme [15]. In particular, our main contributions are listed as follows:

- (i) *Single-Point Failure and Key Escrow Free.* To adapt to decentralized environment of the MCC system, EMA-LUPHDS introduces the architecture of multiple authority for user key distribution so as to prevent single-point failure and key escrow problem in a centralized single authority.
- (ii) *Hidden Access Policy over Large Attribute Universe.* EMA-LUPHDS leverages fully hidden access policy to solve the user privacy leakage problem in most of current CP-ABE schemes with cleartext access policy shared with the ciphertexts in CSP which may lead to private information leakage. To be flexible in the setup of large-scale MCC systems, EMA-LUPHDS supports large attribute universe with constant size of system parameter.
- (iii) *Cost Saving in Encryption and Decryption.* To save the computation cost in both encryption and decryption, online/offline technique is introduced into EMA-LUPHDS for efficient data encryption. Moreover, EMA-LUPHDS achieves outsourced decryption in order to improve efficiency by moving a majority of computation cost of mobile devices with poor resources to CSP.
- (iv) *Verifiability and Exculpability.* To guarantee the correctness of outsourced decryption executed by CSP, EMA-LUPHDS can check the result of partially decrypted ciphertext transformed by untrusted CSP with a data verification approach. For the exculpability of CSP, it achieves a commitment mechanism using Pedersen commitment approach.
- (v) *Security and Efficiency.* We present security analysis and performance evaluation of the proposed scheme. The result demonstrates that our proposal is secure and efficient, which is extremely practicable and suitable for MCC systems.

1.2. Organization. The remainder of the article is outlined below. Some relevant studies are reviewed in Section 2, and the preliminaries including related definitions and notations

are introduced in Section 3. In Section 4, we give the system model, threat model, and design goals of our scheme together with the system definition. Based on this, we describe in detail the constructions of the proposal in Section 5. Section 6 follows this to discuss the security of the scheme, and its performance evaluation is conducted in Section 7. Finally, Section 8 makes a conclusion for the work in this article.

2. Related Work

Mobile cloud computing (MCC) is widely utilized in various applications in which huge number of data plays an important role. Thus, how to protect the security of such large volume data is a big challenge for MCC [3]. CP-ABE is a promising technique for data confidentiality and fine-grained access control which is first introduced in [16] based on the scheme in [17] aside from the user authentication protocols [18–21] as user-centric access control. Due to the data-centric and flexible access control, CP-ABE has been broadly studied and applied [8, 9, 22–26]. However, MCC is a large scale and distributed system involving mobile and resource-limited user devices with much privacy in their data, and the standard CP-ABE schemes cannot be directly employed in MCC applications due to their high cost in computation and dependence on centralized authority.

To confront the bottleneck of single authority, the study in [15] designed a scheme based on [27, 28] with fully multi-authority, but it is inefficient and cannot resist collusion attack. As a solution, borrowing the idea of outsourced decryption proposed in [29–33] based on [34], the scheme in [29] improved the decryption efficiency and the DACC in [35] utilized Key Distribution Centres (KDC) for user key generation across multiple groups to resist collusion attack. Later, the proposals in [30, 36] enhance the DACC scheme in addressing both user collusion and revocation problems. Recently, to solve the problem of deploying CP-ABE in MCC applications for data access control, the schemes in [2] proposed a solution based on [37] and outsourced decryption with anonymous techniques to achieve high decryption efficiency in distributed MCC systems, but it only improves efficiency in decryption and cannot support large attribute universe. Thus, motivated by online/offline CP-ABE proposed in [14, 38, 39] based on [40–42], De and Ruj [1] designed a multiauthority CP-ABE with outsourced decryption to achieve high efficiency in both encryption and decryption, whereas it fails to protect user privacy in access policy which is important for MCC applications containing massive private data.

To protect user privacy in plaintext access policy of standard CP-ABE schemes, the research in [43] first presents the idea of partial hidden-policy CP-ABE, but it only supports AND gate policy with weak security. Later, the study in [44] devised a fully secure and partial hidden-policy CP-ABE, but it still suffers from restricted expressiveness in access policy. Then, the scheme in [45] improves its expressiveness, and the work in [46] introduces decryption testing and large universe to improve efficiency and flexibility, but it is computation consuming with composite order groups. To

solve this problem, the studies in [47, 48] design two efficient and partial hidden-policy CP-ABE schemes based on prime order groups that support expressive access policy and verifiable outsourced decryption. However, they are weak in the protection of access policy due to their partially hidden policies. As a solution, the research in [49] proposed fully hidden policy for CP-ABE, but it incurs high computation cost. Then, the work in [50] proposed an efficient fully hidden-policy CP-ABE scheme, while it only supports restricted access policy. Recently, the studies in [6, 7] devise two efficient CP-ABE schemes that support fully hidden and expressive access policy, but both schemes do not overcome the efficiency issue in encryption and small attribute universe. Moreover, these schemes fail to support exculpability which guarantees an authorized user has no way to accuse the cloud of outputting incorrect results in outsourced decryption while it was not the case. As a whole, these schemes cannot be used in MCC applications.

To seek a better solution, we propose EMA-LUPHDS for data access control in MCC applications. We make a function comparison in Table 1 between our scheme and several related state-of-the-art schemes in [1, 2, 6, 7, 10, 12–14] in the functionalities of access policy, large attribute universe, multiauthority, hidden access policy, efficient encryption, efficient decryption, verifiability, and exculpability. This demonstrates that our EMA-LUPHDS is more versatile and flexible than other schemes with richer advantages and satisfies the requirements of data access control in MCC applications.

In Table 1, the schemes are compared from the features of access policy, attribute universe, authority, policy hidden, encryption, and decryption efficiency as well as verifiability and exculpability. First of all, from Table 1, we note that the majority of schemes support expressive LSSS access policy which are flexible and expressive in access policy design. Only two schemes in comparison support “AND” threshold access policy which are lack in expressiveness and flexibility. Moreover, from the aspect of attribute universe, the schemes in [1, 7, 10, 14] and ours all support large universe, while only our scheme and the schemes in [6, 7, 13] provide the features of multiple authorities and hidden policy, which can prevent sensitive information leakage from access policy and resist single authority failure. Furthermore, from the aspect of efficiency, it is well accepted to adopt outsourced encryption and decryption in CP-ABE schemes. And we conclude that most of the schemes in Table 1 support outsourced decryption and verifiability simultaneously, while only our scheme and the schemes in [1, 2, 14] also improve the efficiency in encryption by introducing online/offline technique. In addition, to support a strong verifiability and exculpability for outsourced decryption, we also note that the feature of exculpability is only supported by our scheme and those in [12, 14], while the scheme in [12] does not support expressive policy and the scheme in [14] failed to protect sensitive data in policy and is lack of large attribute universe. In general, our proposal can simultaneously support all the features mentioned above.

TABLE 1: Function comparison.

Scheme	Access policy	Large universe	Multiple authority	Policy hidden	Efficient encryption	Outsourced decryption	Strong verifiability	Exculpability
Scheme in [12]	AND gate	×	×	×	×	√	×	√
Scheme in [11]	LSSS	√	√	×	×	×	×	×
Scheme in [13]	AND gate	×	√	√	×	×	×	×
Scheme in [7]	LSSS	√	√	√	×	√	×	×
Scheme in [1]	LSSS	√	√	×	√	√	×	×
Scheme in [14]	LSSS	√	×	×	√	√	√	√
Scheme in [6]	LSSS	×	√	√	×	√	×	×
Scheme in [2]	LSSS	×	√	×	√	√	×	×
EMA-LUPHDS	LSSS	√	√	√	√	√	√	√

3. Preliminaries

This section provides several notions and definitions in our proposal including access structure and bilinear maps.

3.1. Notations. In our work, $[l1, l2]$ is used to denote the set $\{l1, l1 + 1, \dots, l2\}$ and $[n]$ is the set $1, 2, \dots, n$, where $n \in \mathbb{Z}_p^*$, while $|S|$ denotes the length of a string S .

3.2. Access Structure

Definition 1 (Access structures [8]). Let $E = E_1, \dots, E_n$ be a entity collection. Given a set $C \subseteq 2^E \setminus \emptyset$, it is monotonic if $\forall D, F : D \subseteq F \cap D \in C \implies F \in C$. Then, the set C is also a monotonic access structure, and the subsets in C are called the authorized sets, otherwise the unauthorized sets.

3.3. Linear Secret Sharing Schemes (LSSSs)

Definition 2 (LSSS [25]). Given the attribute universe U_a , an LSSS on it involves (B, δ) , where B is an $l \times n$ share-generating matrix on \mathbb{Z}_p and the function δ maps a row of B into an attribute in U_a . There are two algorithms: Share and Reconstruction in an LSSS. The former is to create the shares for a secret value s based on B with $\vec{b} = (s, b_2, \dots, b_n)^T$, where $b_2, \dots, b_n \in_R \mathbb{Z}_p$ by $\lambda_x = B_x \cdot \vec{b}$ as a share of the secret s , while the latter reconstructs s with the secret shares of an authorized set E by finding $I = \{i \mid \delta(i) \in E\} \subseteq \{1, 2, \dots, l\}$ and constances $\omega_i \in \mathbb{Z}_p$ to make $\sum_{i \in I} \omega_i B_i = (1, 0, \dots, 0)$ hold and compute $\sum_{i \in I} \omega_i \lambda_i = s$.

3.4. Cryptographic Background

Definition 3 (Bilinear maps [9]). Given p -ordered cyclic groups G and G_T with a generator $w \in G$, where p is a big

prime, if a map $\hat{e} : G \times G \longrightarrow G_T$ is bilinear, it must satisfy the following: (1) bilinearity: $\hat{e}(u^e, h^f) = \hat{e}(w, h)^{ef}$, $\forall e, f \in \mathbb{Z}_p$, $u, h \in G$, (2) nondegeneracy: $\hat{e}(w, w) \neq 1$, and (3) computability: $\hat{e}(u, h)$ which can be efficiently computed by an algorithm $\forall u, h \in G$.

4. System Model and Design Goals

This section presents the system model, threat model, and design goals of our proposed system before giving the formal definition and security model for EMA-LUPHDS.

4.1. System Model. As detailed in Figure 2, our system involves Cloud Service Provider (CSP), trusted authority (TA), attribute authorities (AAs), data owner (DO), and data user (DU).

- (i) CSP provides users with data outsourcing, sharing, and outsourced decryption services as well as unlimited storage and computational resources
- (ii) TA is responsible for initiating whole system by generating global public parameters for the whole system and its master keys
- (iii) AA takes charges of managing a disparate set of attributes and generating and distributing secret key and transformation key of the authenticated cloud users. The attribute sets managed by any two or more AAs are different from each other
- (iv) DO collects important information from mobile devices in MCC and uploads the massive data to CSP. Before outsourcing, DO converts the data with symmetric algorithm and a symmetric key encrypted by a fully hidden access policy for fine-

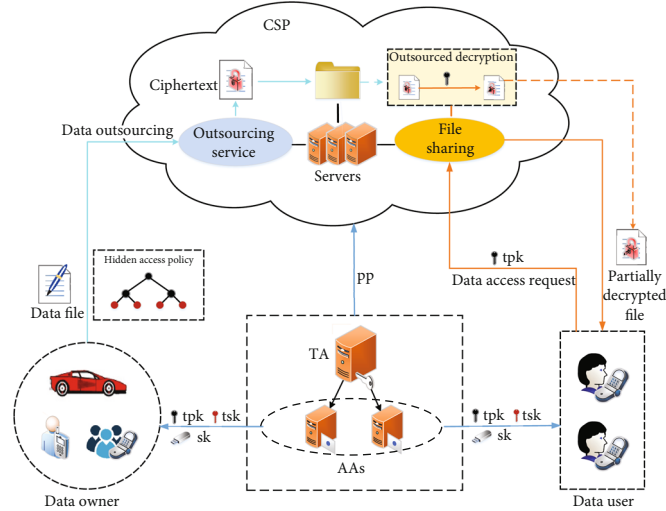


FIGURE 2: The system model of our EMA-LUPHDS.

grained access control and user privacy preserving. Besides, DO prepares ciphertext components while accessing the power source offline to save computational resource of mobile devices

- (v) DU accesses the shared data in CSP on demand with his transformation key for outsourced decryption and recovers the symmetric key if authorized to further decrypt the partially decrypted ciphertext from CSP after verifying its correctness

Based on the above system model, we design our data sharing scheme suitable for the MCC system involving four phases as below.

- (i) *Initialization*. TA creates the system global public parameters and master key at the first. All entities can obtain the global public parameters with which each AA can generate their public and secret key pair.
- (ii) *User Enrollment*. Each AA issues a secret key and a pair of transformation key for DUs after receiving the joining requests from these DUs. Each AA manages the enrolled DUs as well as their attribute sets.
- (iii) *Encryption*. DO encrypts the data (usually in form of files) collected from the smart mobile devices in MCC systems based on a designated access policy and outsources the final ciphertext with fully hidden policies to CSP for data sharing.
- (iv) *Decryption*. DU downloads ciphertexts from CSP with his transformation public key for outsourced decryption by CSP. After receiving the partially decrypted data, the DU decrypts it based on transformation private key and checks its correctness.

4.2. Threat Model and Design Goals. In our EMA-LUPHDS, TA, AA, and DO are trusted entities while CSP is deemed to

be a semihonest entity which is willing to act with honesty but may leak the private information in an “honest-but-curious” manner. In supplying the outsourced decryption service, CSP may misbehave in returning the result of the partially decrypted ciphertext to DU, such as returning false results or be lazy to return previous results. DUs are regarded as untrusted as they may illegally access the shared data in CSP without authorization or try to break the data security and privacy. Due to these threats on data sharing in MCC, we have the following design goals for our system:

- (i) *Data Confidentiality*. The proposed scheme should protect sensitive information in the outsourced data from being leaked or eavesdropped during data sharing and outsourced decryption in CSP and the communication between DU and CSP.
- (ii) *Fine-Grained Access Control and Collusion Resistance*. Malicious users who are unauthorized or intend to collude with each other in data access should have no way to recover the ciphertext by aggregating their keys while anyone of them is unauthorized to decrypt the ciphertext alone.
- (iii) *Access Policy Hiding*. On account of the access policy shared with ciphertext, those sensitive or privacy-aware information contained and exposed in access policies should be concealed for the purpose of user privacy preserving
- (iv) *Verifiability and Exculpability*. Due to the misbehaving CSP, the correctness of outsourced decryption by CSP should be verified. Also, any DU with authorized secret key cannot accuse the CSP of performing incorrectly in outsourced decryption while it acts honestly.
- (v) *Efficient Encryption and Decryption*. With respect of resource-limited mobile devices in the MCC system, the computation should be as little as possible for

DU by moving a majority of preparation work off-line and offloading the highly operations in decryption to CSP.

4.3. System Definition. We present the definition of our proposed EMA-LUPHDS scheme with the following algorithms:

- (i) $Setup_{Global}(\lambda)$. The global setup algorithm is executed by TA. On inputting the security parameter λ , it outputs the global public parameters pp and master key msk
- (ii) $Setup_{AA}(pp)$. The authority setup algorithm is in the charge of each AA AA_i managing a disparate set of attributes. It takes as input system global public parameters and outputs their public and secret key pair (pk_{AA_i}, sk_{AA_i}) .
- (iii) $KeyGen(pp, sk_{AA_i}, GID, S_{i,GID})$. The key generation algorithm is executed by each attribute authority AA_i . It takes as input system global public parameters pp , their secret key sk_{AA_i} , the global identity GID , and an attribute set $S_{i,GID}$ of each cloud user. Then, AA_i outputs $sk_{i,GID}$ as the secret key associated with the DU identified by GID and their attribute set $S_{i,GID}$.
- (iv) $TKeyGen(pp, sk_{i,GID})$. The transformation key generation algorithm is run by each attribute authority AA_i . It takes the global public parameters pp and the secret key $sk_{i,GID}$ of DU identified by GID and outputs the transformation key pair tk of the DU identified by GID .
- (v) $Encrypt_{off}(pp)$. The offline encryption algorithm is executed by DO. On inputting the system global public parameters pp , DO generates offline ciphertext component Key_{off} and VC_{off} .
- (vi) $Encrypt_{on}(pp, M, (A, \rho))$. The online encryption algorithm is run by DO. On inputting the system global public parameters pp , the specific message M , and the designated access policy (A, ρ) , DO generates the final ciphertext CT and outsources it to CSP
- (vii) $Decrypt_{OUT}(pp, tpk_{i,GID}, CT)$. The outsourced decryption algorithm is executed by CSP. It takes as input system global public parameters pp , transformation public key $tpk_{i,GID}$, and ciphertext CT and then outputs the partial decrypted ciphertext CT^* .
- (viii) $Decrypt_U(pp, tsk_{i,GID}, CT^*)$. The user decryption algorithm is run by DU. It takes the system global public parameters pp , transformation private key $tsk_{i,GID}$, and partially decrypted ciphertext CT^* as input and outputs the recovered ciphertext components R^* and key^* .

- (ix) $DecVerify(pp, \bar{C}, V_m, key^*, R^*)$. The user decryption verification algorithm is executed by DU. Given the recovered random element R^* and encapsulated key key^* , the DU checks if the session key and encrypted data are valid and output the plaintext M .

5. The Proposed EMA-LUPHDS Scheme

In this section, we describe the overview of our EMA-LUPHDS scheme and its concrete construction.

5.1. Overview. To adapt to the large-scale MCC system, we first design a large universe multiauthority hidden-policy CP-ABE scheme with verifiable and exculpable outsourced decryption to realize efficient data sharing in MCC. Each user in such a distributed architecture is bound up with a global identity (GID) [51] to avoid collision. Moreover, we introduce online/offline technique to further reduce the overhead in data encryption. Before displaying the detailed construction of EMA-LUPHDS scheme, we define that in our EMA-LUPHDS, U_a is the attribute universe which contains arbitrary string, U_A is the authority universe with N different AAs and a public function $F : U_a \rightarrow U_A$, which maps each attribute $j \in U_a$ to a specific authority $AA_i \in U_A$, denoting that the attribute j is managed by authority AA_i , and I_{AA} is the index of relevant authorities of a user. For simplicity, here we introduce another symbol $\delta(j) = F(j)$, $j \in U_a$.

5.2. Construction of EMA-LUPHDS. Here, the detail of each phase and corresponding algorithms in the formal definition of our proposal are given.

5.2.1. Initialization Phase. In this phase, TA generates system global public parameters and master key and each AA generates their public and secret key pair by the following steps.

- (i) $Setup_{Global}(\lambda)$. Given the security parameter λ , TA generates groups G and G_T of prime order p with a bilinear map $\hat{e} : G \times G \rightarrow G_T$. Then, it chooses random generators $g, g_1, g_2 \in G$ and four collision-resistant hash functions $H : \{0, 1\}^* \rightarrow Z_p^*$, $H_0 : U_a \rightarrow G$, $H_1 : \{0, 1\}^* \rightarrow G$, $H_2 : G_T \rightarrow \{0, 1\}^{n_1}$, $H_3 : \{0, 1\}^* \rightarrow \{0, 1\}^{n_2}$, where M is the message universe and n_1 and n_2 are output sizes of H_2 and H_3 hash functions, respectively. Next, TA creates a \mathcal{L} -length key derivation function (KDF) K , where $\mathcal{L} = |\text{key}| + |p|$ and set the global public parameters as follows:

$$pp = \{G, G_T, H, H_0, H_1, H_2, H_3, F, K, \mathcal{L}, \hat{e}, g, g_1, g_2\}. \quad (1)$$

Finally, TA publishes the global public parameters pp .

- (ii) $Setup_{AA}(pp)$. Each AA AA_i manages a set of attributes S_{AA_i} . As to each attribute authority AA_i , it

chooses two random number $y_i, \alpha_i, \beta_i, t_i \in Z_p^*$ for itself. Thus, each attribute authority AA_i generates its key pair as follows:

$$\text{sk}_{AA_i} = (y_i, \alpha_i, \beta_i, t_i), \text{pk}_{AA_i} = (g^{y_i}, g^{\alpha_i}, g^{\beta_i}). \quad (2)$$

Finally, the attribute authority AA_i outputs their public and secret key pair $(\text{pk}_{AA_i}, \text{sk}_{AA_i})$.

5.2.2. User Enrollment Phase. Upon receiving the enrollment request from DU with their global identities and attribute sets, attribute authorities generate a secret key and a transformation key pair for DU based on the following algorithms.

- (i) *KeyGen*($pp, \text{sk}_{AA_i}, \text{GID}, S_{i,\text{GID}}$). If a DU has a global identity GID and a set of attributes $S_{i,\text{GID}}$ which is related to an attribute authority AA_i , the AA_i chooses

a random number $t \in Z_p^*$ and computes the secret key $\text{sk}_{i,\text{GID}}$ for the DU as follows:

$$\begin{aligned} \text{sk}_{i,\text{GID}} &= \{K_{1,j}, K_{2,j}, K_3\}_{j \in S_{i,\text{GID}}} \\ &= \left\{ g^{\alpha_i} H_1(\text{GID})^{y_i} H_0(j)^{\beta_i}, H_0(j)^{t_i}, g^{\beta_i} \right\}_{j \in S_{i,\text{GID}}}. \end{aligned} \quad (3)$$

Finally, the attribute authority AA_i outputs $\text{sk}_{i,\text{GID}}$ and sends it to the DU identified by GID through secure channel.

- (ii) *TKeyGen*($pp, \text{sk}_{i,\text{GID}}$). The authority AA_i generates transformation key for DU identified by GID on giving the DU's secret key $\text{sk}_{i,\text{GID}}$. We assume that as for each attribute $j \in S_{i,\text{GID}}$, if $F(j) = i$, the attribute set $S_{i,\text{GID}}$ of DU with GID is managed by AA_i . The authority AA_i chooses a random number $\mu \in Z_p^*$ and computes the transformation key $\text{tk} = (\text{tpk}, \text{tsk})$ as follows:

$$\begin{aligned} \text{tpk}_{i,\text{GID}} &= \{\text{TK}_{1,j}, \text{TK}_{2,j}, \text{TK}_3, \text{TK}_4, \text{TK}_5\}_{j \in S_{i,\text{GID}}} \\ &= \left\{ K_{1,j}^{1/\mu}, K_{2,j}^{1/\mu}, K_3^{1/\mu}, g^{1/\mu}, H_1(\text{GID})^{1/\mu} \right\}_{j \in S_{i,\text{GID}}} \\ &= \left\{ g^{\alpha_i/\mu} H_1(\text{GID})^{y_i/\mu} H_0(j)^{\beta_i/\mu}, H_0(j)^{t_i/\mu}, g^{\beta_i/\mu}, g^{1/\mu}, H_1(\text{GID})^{1/\mu} \right\}_{j \in S_{i,\text{GID}}} \\ \text{tsk}_{i,\text{GID}} &= \{\mu\}. \end{aligned} \quad (4)$$

Finally, AA_i outputs transformation key $\text{tk} = (\text{tpk}, \text{tsk})$ for DU with identity GID .

5.2.3. Encryption Phase. On input globally public parameters pp and public key of AA_i , the encryption process contains the following three steps:

- (i) *Encrypt_{off}*(pp). DO selects a random secret $s \in_R Z_p$ to compute the encapsulated key key . Then, the DO generates the corresponding session key ssk for data encryption/decryption and the commitment \bar{C} (e.g., Pedersen commitment algorithm) for key verification. The algorithm is executed as follows:

$$\text{key} = \prod_{i \in I_{AA}} \tilde{e}(g, g)^{\alpha_i s} = \tilde{e}(g, g)^{\sum_{i \in I_{AA}} \alpha_i s}, \quad (5)$$

$$\text{KDF}(\text{key}, \mathcal{L}) = \text{ssk} \| d, \bar{C} = g_1^{H(\text{ssk})} g_2^{H(d)}.$$

As a result, the DO sets $\text{Key}_{\text{off}} = (s, \text{key}, \text{ssk}, \bar{C})$ and creates a pool of offline keys. Next, the DO picks a random element $R \in G_T$ and computes $R' = H_2(R)$. Finally, the DO sets $\text{VC}_{\text{off}} = (R, R')$ and constructs a pool of offline verification code.

- (ii) *APTransform*. To achieve access policy anonymity, the DO first designates an original access policy (A_o, ρ) , where A_o is a $l \times n$ matrix and ρ is a function that maps each row of A_o to an attribute. Then, the DO selects a random value $a \in Z_p^*$ and computes $m_x = \tilde{e}((g^a)^{A_o}, H_0(\rho(x)))$, where $x \in [l]$ is each row of access policy (A_o, ρ) and l is the number of rows in A_o . To preserve the privacy of access policy, the data owner replaces each attribute $\rho(x)$ in A_o with m_x , and then, the original access policy (A_o, ρ) can be transformed to LSSS access policy matrix $(A_{l \times n}, \rho)$ which can be denoted by (A, ρ) for simplicity.

- (iii) *Encrypt_{on}*($pp, M, (A, \rho)$). DO chooses any one pair of offline components $\text{Key}_{\text{off}} = (s, \text{key}, \text{ssk}, \bar{C})$ and $\text{VC}_{\text{off}} = (R, R')$ to encrypt the data M gathered from smart devices to generate encrypted data C $T_s = E_{\text{symm}}(M, \text{ssk})$ with the symmetric encryption algorithm and the symmetric key ssk and compute the verification code $V_m = H_3(R' \| CT_s)$ for CT_s . With the specific access policy (A, ρ) , where A is a $l \times n$ matrix and ρ is a mapping from each row A_x to a certain attribute att_x , DO picks $p_x \in_R Z_p^*$ for each row A_x of A and computes $\lambda_x = A_x$

$\cdot \gamma$, where $\gamma = \{\gamma_1, \gamma_2, \dots, \gamma_l\} \in_R Z_p^l$ and $\theta_x = A_x \cdot \nu$, where $\nu = \{\nu_1, \nu_2, \dots, \nu_l\} \in_R Z_p^l$. Next, DO outputs ciphertext $CT = \{(A, \rho), \bar{C}, CT_s, V_m, C', C_0, \{C_{1,x}, C_{2,x}, C_{3,x}, C_{4,x}\}_{x \in [l]}\}$, where

$$\begin{aligned} C' &= g^a, C_0 = R \cdot \text{key}, C_{1,x} = g^{\alpha_{\delta(x)} \lambda_x} g^{\alpha_{\delta(x)} \rho_x}, \\ C_{2,x} &= g^{\rho_x}, C_{3,x} = (H_0(\rho(x)))^{\rho_x}, C_{4,x} = g^{\gamma_{\delta(x)} \rho_x} g^{\theta_x}. \end{aligned} \quad (6)$$

Finally, the DO uploads the ciphertext CT to CSP.

5.2.4. Decryption Phase. After DU requesting for specific data CT with his transformation public key (tpk), the CSP executes outsourced access policy recovery operations and sends back the intermediate anonymous attributes to the DU. Then, the CSP executes outsourced decryption with the recovered index of access policy received from the DU. Next, with the partially decrypted ciphertext from CSP, the DU can get decrypted plaintext at the end. Finally, with verification execution, the DU can verify whether the ciphertext and session key is valid. The phase involves the following algorithms:

- (i) *APRecover*. First of all, the CSP computes $m_x' = \hat{e}(C', H_0(\rho(x))^{t_i/\mu})$, where $x \in S_{i, \text{GID}}$ with the DU's tpk and sends the m_x' together with access policy of CT, i.e., (A, ρ) , to the DU. Then, the DU replaces the attribute x with $(m_x')^{\text{tsk}}$, and the result attribute set $S_{i, \text{GID}}'$ is constructed, and the attribute index set is $I_s' = \{x : (\rho(x) \cap S_{\text{GID}}')_{x \in [l]}\}$. Then, the DU sends I_s' to CSP for outsourced decryption.
- (ii) *Decrypt_{OUT}*($pp, tpk_{i, \text{GID}}, CT$). Let each matrix row A_x of access policy (A, ρ) correspond to an attribute $\rho(x)$, and CSP executes as follows:

$$\begin{aligned} C_{\delta(x)}^* &= \frac{\hat{e}(\text{TK}_4, C_{1,x}) \hat{e}(\text{TK}_5, C_{4,x}) \hat{e}(\text{TK}_3, C_{3,x})}{\hat{e}(\text{TK}_{1,x}, C_{2,x})} \\ &= \frac{\hat{e}(g^{1/\mu}, C_{1,x}) \hat{e}(H_1(\text{GID})^{1/\mu}, C_{4,x})}{\hat{e}(g^{\alpha_{\delta(x)}/\mu} H_1(\text{GID})^{\gamma_{\delta(x)}/\mu} H_0(\rho(x))^{\beta_{\delta(x)}/\mu}, C_{2,x})} \\ &\quad \cdot \frac{\hat{e}(g^{\beta_{\delta(x)}/\mu}, H_0(\rho(x))^{\rho_x})}{\hat{e}(g^{\alpha_{\delta(x)}/\mu} H_1(\text{GID})^{\gamma_{\delta(x)}/\mu} H_0(\rho(x))^{\beta_{\delta(x)}/\mu}, C_{2,x})} \\ &= (e\wedge(g, g)^{\alpha_{\delta(x)} \lambda_x} e\wedge(H_1(\text{GID}), g)^{\theta_x})^{1/\mu}. \end{aligned} \quad (7)$$

Then, as mentioned before, $\lambda_x = A_x \cdot \gamma$, where $\gamma = \{\gamma_1, \gamma_2, \dots, \gamma_l\} \in Z_p^l$ and $\theta_x = A_x \cdot \nu$, where $\nu = \{\nu_1, \nu_2, \dots, \nu_l\} \in Z_p^l$, we note that there exists coefficients $\omega_x \in Z_p$ where $x \in I_s'$ such that $\sum_{x \in I_s'} \omega_x A_x = (1, 0, \dots, 0)$. Thus, we have $\sum_{x \in I_s'} \omega_x \lambda_x = s$ and $\sum_{x \in I_s'} \omega_x \theta_x = 0$.

Subsequently, the DU can compute $\prod_{x \in I_s'} (C^*)^{\omega_x}$, so that,

$$\begin{aligned} CT_{\delta(x)}' &= \prod_{x \in I_s'} (C_{\delta(x)}^*)^{\omega_x} = \prod_{x \in I_s'} (e\wedge(g, g)^{\alpha_{\delta(x)} \omega_x \lambda_x} e\wedge(H_1(\text{GID}), g)^{\omega_x \theta_x})^{1/\mu} \\ &= \left(e\wedge(g, g)^{\alpha_{\delta(x)} \sum_{x \in I_s'} \omega_x \lambda_x} \right)^{1/\mu} \cdot \left(e\wedge(H_1(\text{GID}), g)^{\sum_{x \in I_s'} \omega_x \theta_x} \right)^{1/\mu} \\ &= \hat{e}(g, g)^{\alpha_{\delta(x)} s/\mu}. \end{aligned} \quad (8)$$

Let $i = \delta(x)$, and we have the following equation:

$$CT' = \prod_{i \in I_{AA}} CT'_i = \prod_{i \in I_{AA}} \hat{e}(g, g)^{\alpha_i s/\mu} = \hat{e}(g, g)^{\sum_{i \in I_{AA}} \alpha_i s/\mu}. \quad (9)$$

Finally, the CSP returns partially decrypted ciphertext $CT^* = \{C_0, \bar{C}, CT', CT_s, V_m\}$ to the DU.

- (i) *Decrypt_U*($pp, tsk_{i, \text{GID}}, CT^*$). After receiving the partially decrypted ciphertext CT^* , the DU recovers the random element R and the encapsulated key key used for generating symmetric session key as follows:

$$\begin{aligned} \text{key}^* &= (CT')^{\text{tsk}} = \left(e\wedge(g, g)^{\sum_{i \in I_{AA}} \alpha_i s/\mu} \right)^\mu = \hat{e}(g, g)^{\sum_{i \in I_{AA}} \alpha_i s}, \\ R^* &= \frac{C_0}{\text{key}^*} = \frac{R \cdot \hat{e}(g, g)^{\sum_{i \in I_{AA}} \alpha_i s}}{\hat{e}(g, g)^{\sum_{i \in I_{AA}} \alpha_i s}}. \end{aligned} \quad (10)$$

Finally, DU outputs the recovered random element R^* and encapsulated key key^* .

- (ii) *DecVerify*($pp, \bar{C}, V_m, \text{key}^*, R^*$). On input recovered encapsulated key key^* and random element R^* , the DU computes as follows:

$$\begin{aligned} \text{KDF}(\text{key}^*, \mathcal{L}) &= \text{ssk}^* \| d^*, \bar{C}^* = g_1^{H(\text{ssk}^*)} g_2^{H(d^*)}, \\ \bar{R}^* &= H_2(R^*), V_m^* = H_3(\bar{R}^* \| CT_s). \end{aligned} \quad (11)$$

Then, the DU checks if the following equations

$$\begin{aligned} \bar{C} &\stackrel{?}{=} \bar{C}^*, \\ V_m &\stackrel{?}{=} V_m^*. \end{aligned} \quad (12)$$

hold, and it outputs $M = D_{\text{symm}}(CT_s, \text{ssk}^*)$, otherwise \perp .

6. Security Analysis

In this section, we present a brief security analysis of our proposed EMA-LUPHDS scheme concerning the design goals mentioned in Section 4.2.

Theorem 1. *The proposed scheme satisfies the properties of correctness.*

Proof. We can prove the correctness of outsourced decryption in our scheme by the following equation:

$$\begin{aligned}
CT_{\delta(x)}' &= \prod_{x=1}^l (C_{\delta(x)}^*)^{\omega_x} = \prod_{x=1}^l \left(\frac{\tilde{e}(\text{TK}_4, C_{1,x}) \tilde{e}(\text{TK}_5, C_{4,x}) \tilde{e}(\text{TK}_3, C_{3,x})}{\tilde{e}(\text{TK}_{1,x}, C_{2,x})} \right) \\
&= \prod_{x=1}^l \left(\frac{e\Lambda(g^{1/\mu}, C_{1,x}) e\Lambda(H_1(\text{GID})^{1/\mu}, C_{4,x})}{e\Lambda(g^{\beta_{\delta(x)}/\mu} H_1(\text{GID})^{\gamma_{\delta(x)}/\mu} H_0(\rho(x))^{\beta_{\delta(x)}/\mu}, C_{2,x})} \right. \\
&\quad \left. \cdot \frac{e\Lambda(g^{\beta_{\delta(x)}/\mu}, H_0(\rho(x))^{P_x})}{e\Lambda(g^{\alpha_{\delta(x)}/\mu} H_1(\text{GID})^{\gamma_{\delta(x)}/\mu} H_0(\rho(x))^{\beta_{\delta(x)}/\mu}, C_{2,x})} \right)^{\omega_x} \\
&= \prod_{x=1}^l \left(\frac{e\Lambda(g^{1/\mu}, g^{\alpha_{\delta(x)} \lambda_x} g^{\alpha_{\delta(x)} P_x})}{e\Lambda(g^{\alpha_{\delta(x)}/\mu} H_1(\text{GID})^{\gamma_{\delta(x)}/\mu} H_0(\rho(x))^{\beta_{\delta(x)}/\mu}, g^{P_x})} \right. \\
&\quad \left. \cdot \frac{e\Lambda(H_1(\text{GID})^{1/\mu}, g^{\gamma_{\delta(x)} P_x} g^{P_x})}{e\Lambda(g^{\alpha_{\delta(x)}/\mu} H_1(\text{GID})^{\gamma_{\delta(x)}/\mu} H_0(\rho(x))^{\beta_{\delta(x)}/\mu}, g^{P_x})} \right. \\
&\quad \left. \cdot \frac{e\Lambda(g^{\beta_{\delta(x)}/\mu}, H_0(\rho(x))^{P_x})}{e\Lambda(g^{\alpha_{\delta(x)}/\mu} H_1(\text{GID})^{\gamma_{\delta(x)}/\mu} H_0(\rho(x))^{\beta_{\delta(x)}/\mu}, g^{P_x})} \right)^{\omega_x} \\
&= \prod_{x=1}^l \left(e\Lambda(g, g)^{\alpha_{\delta(x)} \lambda_x} e\Lambda(H_1(\text{GID}), g)^{\theta_x} \right)^{\omega_x / \mu} \\
&= \prod_{x=1}^l \left(e\Lambda(g, g)^{\alpha_{\delta(x)} \omega_x \lambda_x} e\Lambda(H_1(\text{GID}), g)^{\omega_x \theta_x} \right)^{1/\mu} \\
&= \left(e\Lambda(g, g)^{\alpha_{\delta(x)} \sum_{x=1}^l \omega_x \lambda_x} e\Lambda(H_1(\text{GID}), g)^{\sum_{x=1}^l \omega_x \theta_x} \right)^{1/\mu} \\
&= \tilde{e}(g, g)^{\alpha_{\delta(x)} S / \mu}.
\end{aligned} \tag{13}$$

□

Theorem 2. *The proposed scheme satisfies the properties of data confidentiality.*

Proof. In our scheme, the data is first encrypted using a symmetric encryption algorithm, and the key is encapsulated by access policy. As for the data confidentiality, the symmetric encryption algorithm, such as AES, can guarantee the feature. With respect to the fine-grained data access control, for the transformation public key tpk of a unauthorized DU whose attribute set does not satisfy the access policy, CSP cannot get an authorized index set I_s' so as to calculate the correct constants $\{\omega_x\}$ to make the equation $\sum_{x \in I_s'} \omega_x A_x = s$ holds. Thus, the CSP will fail to return a correct par-

tially decrypted ciphertext, and the DU also cannot obtain the encapsulated symmetric key to further get the plaintext of data. Moreover, in outsourced decryption, the CSP also cannot get the symmetric key from partially decrypted ciphertext to recover plaintext of data because it cannot get the transformation secret key tsK of the DU to further decrypt the partially decrypted ciphertext. Furthermore, the secret key of each DU is embedded with his unique global identity, and the transformation public key of each DU is also confused with his unique transformation secret key tsK which is secret by the DU himself, and any two or more DUs have no way to collude for data access. □

Theorem 3. *The proposed scheme satisfies the properties of access policy hiding.*

Proof. In our scheme, when the DO encrypts the symmetric key used in symmetric encryption based on a designated access policy, he first transforms each attribute in access policy according to the one-way anonymous key agreement protocol in [52] by computing $m_x = \tilde{e}((g^{t_i})^a, H_0(\rho(x)))$ for each row x of access policy, where a is a random number. Then, DO replaces each attribute in access policy by m_x , which can obfuscate each attribute $\rho(x)$ in access policy. In decryption phase, the DU cannot compute m_x only if he has the key component $H_0(\rho(x))^{t_i}$. Otherwise, DU cannot distinguish m_x from x . Therefore, malicious DU cannot infer the access policy, and thus, the attribute information in access policy is protected. □

Theorem 4. *The proposed scheme satisfies the properties of collusion resistance.*

Proof. The malicious users may collude to combine their secret keys and transformation keys to access the shared data which they cannot access individually. In our scheme, different attribute authority generates secret keys for different users, and the secret keys are associated with users' GID, specific attribute set and random, which are uniquely related to each user and make the combination of attributes in different secret keys useless. As a result, collusive users cannot compute $\text{key}^* = \tilde{e}(g, g)^{\sum_{i \in I_{AA}} \alpha_i S}$ cooperatively in the outsourced decryption even if the combined attributes of these users satisfy the access policy. Thus, our scheme is collision-resistant. □

Theorem 5. *The proposed scheme satisfies the properties of verifiability.*

Proof. Suppose that KDF is secure and H , H_2 , and H_3 are three collision-resistant hash functions. Thus, the output of KDF is indistinguishable from a random string. In the encryption phase of our scheme, $\text{KDF}(\text{key}, \mathcal{L}) = \text{ssk} \| d$ and $\bar{C} = g_1^{H(\text{ssk})} g_2^{H(d)}$. As it is difficult to distinguish the output of KDF from a random string and H is a deterministic collision-resistant hash function, the untrusted CSP has no way to guess the random $H(d)$, $H(\text{ssk})$ and thus fails to tamper the Pedersen commitment \bar{C} which is

computationally hiding. Moreover, since H_2 and H_3 are two collision-resistant functions, it is hard to guess a random R^* to construct $H_3(R^* || CT_s) = H_3(R || CT_s)$, which is in negligible probability. Therefore, the validity of key and ciphertexts CT_s can be guaranteed. \square

Theorem 6. *The proposed scheme satisfies the properties of exculpability.*

Proof. Suppose that KDF is secure and H is a deterministic collision-resistant hash functions. Thus, the output of KDF is indistinguishable from a random string. If a malicious DU with transformation secret key tsk wants to accuse CSP of returning incorrect results, he has to have the ability of forging a fake transformation secret key tsk^* that can generate the same commitment. Suppose that $g_1 = g^p$, $g_2 = g^y$ and the malicious DU constructs $KDF(key, \mathcal{L}) = ssk || d$ and $KDF(key^*, \mathcal{L}) = ssk^* || d^*$, where key and key^* are partially decrypted results with tsk and tsk^* , respectively. The commitment must be equal, that is, $g_1^{H(ssk)} g_2^{H(d)} = g_1^{H(ssk^*)} g_2^{H(d^*)}$. Then, the malicious DU can get $\varphi = \psi(H(d^*) - H(d)) / H(ssk) - H(ssk^*)$, which means that the malicious DU can solve DL problem. However, it is of negligible probability according to DL assumption. Therefore, our scheme is exculpable for decryption. \square

7. Performance Evaluation

This section evaluates the performance by comparing our EMA-LUPHDS scheme with several existing schemes in efficiency aspects. We give the comparison in computation and space complexity in theoretical aspects between our scheme and the schemes in [6, 7]. Furthermore, we focus on experiment implementation to precisely evaluate the efficiency of EMA-LUPHDS. By comparing with several excellent similar schemes, we demonstrate that our scheme is more efficient and practicable for data sharing in MCC.

7.1. Theoretical Analysis. We thoroughly analyzes the computation and space complexity by comparing our EMA-LUPHDS and other schemes [2, 6, 7] in detail from the aspects of public parameter size (pp size), user key size (UKey size), transformation key size (TKey size), ciphertext size (ciphertext size), encryption cost, user decryption cost, and outsourced decryption cost (out decryption cost), as the former four metrics measure the space complexity of each scheme and the remains are used to evaluate the computation cost in execution of each scheme. The comparison result is summarized in Table 2.

Here, we first stipulate some denotions in the theoretical analysis. E_G, E_{G_T} denotes the exponentiation operations in G, G_T , M_G, M_{G_T} denotes the multiplication operations in G, G_T , P denotes the pairing operation \hat{e} , H denotes the computation cost of a hash function and Enc_{sym}, Dec_{sym} denotes the computation costs of symmetric encryption and decryption. In addition, l denotes the number of attributes in access structure, $|S|$ denotes the number of attributes owned by DU, $|G|, |G_T|$ denotes the length of elements in group $G,$

G_T , $|A|$ denotes the number of attributes managed by each authority, $|V|$ denotes the length of verification code, and $|CT_{sym}|$ denotes the length of symmetric encrypted ciphertext.

In Table 2, we first analyze the space complexity comparison. First of all, the pp size of schemes in [2, 6, 7] are $|G| + 1 + (2 + |G_T| + |G|)|A|$, $|A| (|G| + 1) + |G_T| + 1$, and $|G| + |G_T| + 2 + (3 + |G_T| + |G|)|A|$, respectively. We note that these sizes are all growing with the increase of access policy number. However, the pp size in our scheme is $3|G| + 4$, which shows that our scheme can support large attribute universe because the public parameter size is constant and very small. Moreover, the transformation key sizes of the four schemes are $|G|(2 + |S|)$, $2|G|(|S| + 1)$, $2|G|(|S| + 3/2) + 1$, and $2|G|(|S| + 1) + 1$, respectively. This means that the transformation key sizes in four related schemes are of the same case. Furthermore, we analyze the ciphertext size. In schemes [2, 7], the ciphertext sizes are $(3|G| + 4)l + |G| + |G_T|$ and $|G_T| + |V| + |G| + (3|G| + |G_T|)l$, while the sizes in our scheme and the scheme [6] are $2|G|(1 + 2l) + |CT_{sym}| + |V| + |G_T|$ and $|G|(3l + 1) + |G_T| + |V| + |CT_{sym}|$. We note that the former two schemes support smaller ciphertext. However, as the latter two schemes are suitable for scalable plaintext encryption, the ciphertext size may be larger. Later, we will analyze the experiment result and use the base ciphertext size to compare the practical result.

Then, we analyze the computation complexity comparison. First, as for encryption time, the complexity in scheme is [2] while in our scheme and the schemes [6, 7] are $(5E_G + 2M_G)l + E_G + P + M_{G_T} + H + Enc_{sym}$, $2M_{G_T} + H + E_G + (5E_G + 2M_G + E_{G_T})l$, and $E_G + M_{G_T} + (6E_G + 2M_G)l + Enc_{sym} + H$. We can infer that the computation complexity in [2] is a little less while the other three schemes cost more. Moreover, the user decryption in schemes [2, 7] is $E_{G_T} + M_{G_T}$ and $E_{G_T} + M_{G_T} + H$, while the schemes in [6] and our scheme cost $E_{G_T} + M_{G_T} + Dec_{sym} + 2H$ and $E_{G_T} + M_{G_T} + Dec_{sym} + 2H + 2E_G + M_G$. We note that the latter two schemes cost more than the former two schemes because the latter two schemes support large plaintext encryption and decryption, which means that the user needs to decrypt the symmetric ciphertext after obtaining encapsulated symmetric key. In our scheme, we need more computation for commitment recover and add more computation overhead. Furthermore, as for out decryption, we infer from Table 2 that the four schemes outsource similar workload to third party.

In conclusion, we know that although in our scheme, the transformation key is a little larger than other schemes in Table 2, and it has far smaller public parameters in constant size. Also, our scheme supports scalable ciphertext though it may take up a lot of space. As our scheme supports flexible functions, to increase the efficiency, we also introduce online/offline and outsourced computing techniques. We note that from Table 2, the computation cost in encryption and user decryption of our scheme is greatly reduced and approaches other schemes in Table 2. In general, our scheme can achieve more reasonable computation complexity compared with other relevant schemes in theoretical analysis.

TABLE 2: Computation complexity comparison.

Scheme	pp size	TKey size	Ciphertext size	Encryption cost	User decryption cost	Our decryption cost
Scheme in [6]	$ G + 1 + (2 + G_T + G) A $	$2 G S $	$ G (3 I+1 + G_T + V + CT_{\text{sym}})$	$(5E_G + 2M_G)I + E_G + P + M_{G_T} + H + \text{Enc}_{\text{sym}}$	$E_{G_T} + M_{G_T} + \text{Dec}_{\text{sym}} + 2H$	$(3P + 2M_{G_T} + E_{G_T}) S $
Scheme in [2]	$ A + (G + 1) + G_T + 1$	$ G (2 + S)$	$(3 G + 4)I + G + G_T $	$M_{G_T} + E_{G_T} + E_G + 2I$	$E_{G_T} + M_{G_T}$	$(2E_G + 3M_{G_T}) S + P + (2P + M_{G_T} + E_{G_T}) S $
Scheme in [7]	$ G + G_T + 2 + (3 + G_T + G) A $	$2 G (S + 1) + 1$	$ G_T + V + G + (3 G + G_T)I$	$2M_{G_T} + H + E_G + (5E_G + 2M_G + E_{G_T})I$	$E_{G_T} + M_{G_T} + H$	$(4P + 3M_{G_T} + 2E_{G_T}) S + P + M_{G_T} + H$
Our scheme	$3 G + 4$	$2 G \left(\frac{3}{2} + S + 1 \right) + 1$	$2 G (1 + 2 I + CT_{\text{sym}} + V + G_T)$	$E_G + M_{G_T} + (6E_G + 2M_G)I + \text{Enc}_{\text{sym}} + H$	$E_{G_T} + M_{G_T} + \text{Dec}_{\text{sym}} + 2H + 2E_G + M_G$	$(4P + 3M_{G_T} + E_{G_T}) S $

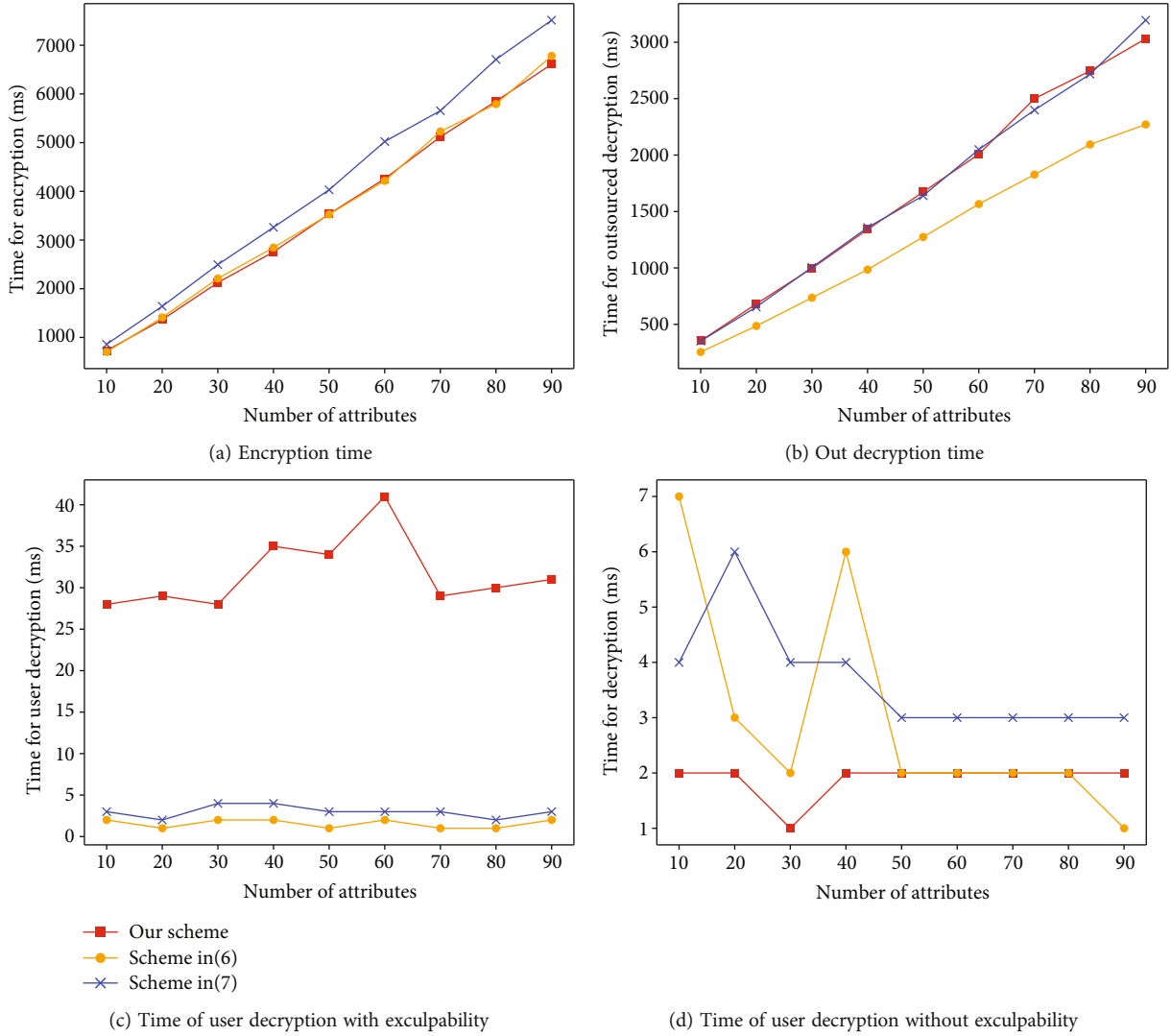


FIGURE 3: Comparison of the computation cost.

7.2. Experimental Analysis. To precisely evaluate the performance of EMA-LUPHDS, we implement our scheme and the schemes in [6, 7] and compare their actual computation and space cost with EMA-LUPHDS, and the result of which is summarized in Figures 3 and 4.

We implement and develop these schemes using Java Programming Language with the Java Pairing-Based Cryptography library (JPBC) [53] for various operations in finite field and groups. Type A pairing is adopted in our implementations which is defined over a 160-bit elliptic curve group over 512-bit finite field, that is, the supersingular elliptic curve $E(F_p): y^2 = x^3 + x$ with embedding degree 2, where p is a 512-bit Solinas prime. Moreover, our simulation experiments are run on Windows10 system with Intel Core i5 CPU 2.13 GHz and 8.00 GB RAM. In addition, we use SHA256 algorithm to generate the V_m for correctness verification of ciphertext in our experiments.

Figure 3 shows the computation comparison from the point of the time cost in encryption, outsourced decryption,

and user decryption. We note that in Figure 3(a), our scheme performs approximate to that of schemes in [6] and is superior to the scheme in [7] in encryption. From Figure 3(b), we know that the computation cost of outsourced decryption for our scheme is a little larger than that of [6] and nearly the same as that of [7]. Figures 3(c) and 3(d) present the computation cost of Pedersen commitment for supporting exculpability. We note that in Figure 3(d), the three schemes perform similarly, and in Figure 3(c), the computation cost of our scheme is larger than the other two schemes, which shows the trade-off between the function of exculpability and efficiency cost.

From Figure 4, we note that the storage complexity of our scheme is approximate to that in [6, 7] while takes only constant-sized public parameters that are far smaller than that in [6, 7]. We can infer from Figure 4(a) that the size of public parameters in our scheme is very small and constant. Thus, in Figure 4(b), the public parameter size of our scheme is nearly invisible. In Figure 4(c), we

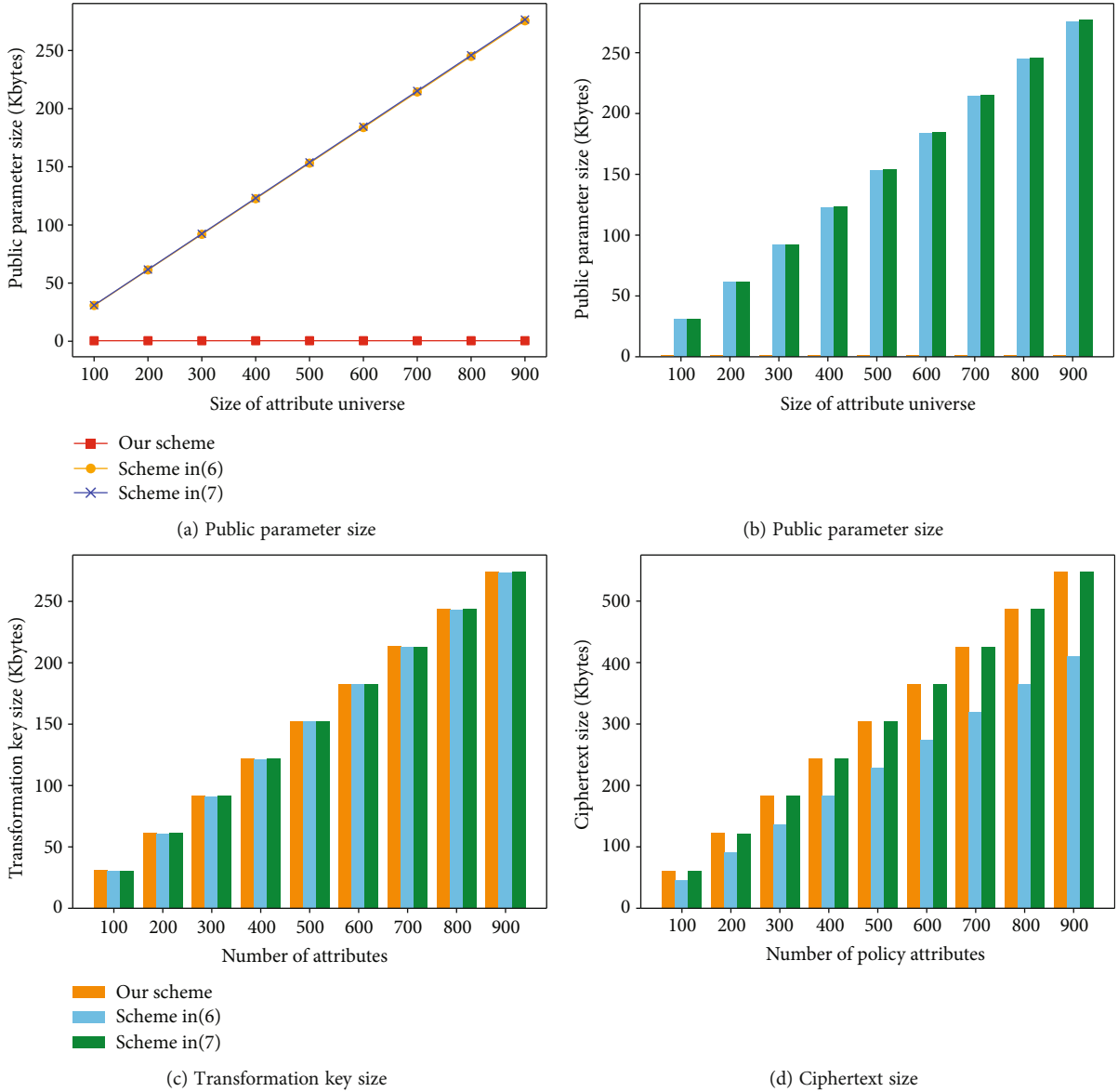


FIGURE 4: Comparison of the storage cost.

know that the three schemes take up similar size in transformation key. Figure 4(d) shows that our scheme takes up a little larger space for ciphertext as we support exculpability and flexible policy hiding. We also note that the ciphertext size is approximate to that of the scheme in [7] which is not flexible as our scheme. And both the scheme in and our scheme can support scalable ciphertext, which means that the user does not need to map plaintext to the bilinear group.

It is obvious that the results of our experiment simulation indicate that our scheme is flexible and versatile. It is also efficient in encryption cost, user decryption cost, and out decryption cost and has far smaller and constant public parameter size. Therefore, we argue that EMA-LUPHDS proposed in our work is more suitable for resource-constraint mobile devices in MCC system.

8. Conclusion

In this paper, we propose an Efficient and Multiauthority Large Universe Policy-Hiding Data Sharing (EMA-LUPHDS) scheme to achieve key escrow resistance, expressive access policies without user privacy leakage, and high efficiency for data sharing of MCC with resource-limited mobile devices. In our proposal, we adopt fully hidden strategy to protect sensitive information about attributes of users and access policy. To achieve high efficiency, we introduce outsourced decryption to reduce the computational cost and the online/offline technique to trade off the overhead in encryption operation. In addition, we add into the ciphertext with verification code and Pedersen commitment to ensure the correctness of the partially decrypted result got from misbehaving CSP and the exculpability for CSP

accused by DU maliciously. Moreover, the security analysis and thorough performance evaluation show that our proposal is practicable for resource-restraint mobile devices in the MCC system.

In our future work, we would dedicate into the efficient attribute and user revocation in data sharing scheme for mobile cloud environment.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research is funded by the National Natural Science Foundation of China (Nos. 62072093, 62072092, 61601107, and U1708262), the China Postdoctoral Science Foundation (No. 2019M653568), the Fundamental Research Funds for the Central Universities (No. N2023020), and the Natural Science Foundation of Hebei Province of China (No. F2020501013).

References

- [1] S. J. De and S. Ruj, "Efficient decentralized attribute based access control for mobile clouds," *IEEE Transactions on Cloud Computing*, vol. 8, no. 1, pp. 124–137, 2020.
- [2] M. Lyu, X. Li, and H. Li, "Efficient, verifiable and privacy preserving decentralized attribute-based encryption for mobile cloud computing," in *2017 IEEE Second International Conference on Data Science in Cyberspace (DSC)*, pp. 195–204, Shenzhen, China, 2017.
- [3] Y. Wu, X. Wang, W. Susilo et al., "Efficient server-aided secure two-party computation in heterogeneous mobile cloud computing," *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2021.
- [4] H. Riasudheen, K. Selvamani, S. Mukherjee, and I. Divyasree, "An efficient energy-aware routing scheme for cloud-assisted MANETs in 5G," *Ad Hoc Networks*, vol. 97, p. 102021, 2020.
- [5] Y. Xie, H. Wen, B. Wu, Y. Jiang, and J. Meng, "A modified hierarchical attribute-based encryption access control method for mobile cloud computing," *IEEE Transactions on Cloud Computing*, vol. 7, no. 2, pp. 383–391, 2019.
- [6] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "Phoabe: securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted iot," *Computer Networks*, vol. 133, pp. 141–156, 2018.
- [7] K. Fan, H. Xu, L. Gao, H. Li, and Y. Yang, "Efficient and privacy preserving access control scheme for fog-enabled IoT," *Future Generation Computer Systems*, vol. 99, pp. 134–142, 2019.
- [8] N. Zhang, Q. Jiang, L. Li, X. Ma, and J. Ma, "An efficient three-factor remote user authentication protocol based on BPV-FourQ for internet of drones," *Peer-to-Peer Networking and Applications*, 2021.
- [9] J. Zhang, T. Li, M. S. Obaidat, C. Lin, and J. Ma, "Enabling efficient data sharing with auditable user revocation for IoV systems," *IEEE Systems Journal*, pp. 1–12, 2021.
- [10] K. Zhang, H. Li, J. Ma, and X. Liu, "Efficient large-universe multiauthority ciphertext-policy attribute-based encryption with white-box traceability," *Science China Information Sciences*, vol. 61, no. 3, 2018.
- [11] P. Zhang, Z. Chen, J. K. Liu, K. Liang, and H. Liu, "An efficient access control scheme with outsourcing capability and attribute update for fog computing," *Future Generation Computer Systems*, vol. 78, pp. 753–762, 2018.
- [12] J. Li, F. Sha, Y. Zhang, X. Huang, and J. Shen, "Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length," *Security and Communication Networks*, vol. 2017, Article ID 3596205, 11 pages, 2017.
- [13] J. Li, X. Chen, S. S. M. Chow, Q. Huang, D. S. Wong, and Z. Liu, "Multi-authority fine-grained access control with accountability and its application in cloud," *Journal of Network and Computer Applications*, vol. 112, pp. 89–96, 2018.
- [14] H. Ma, R. Zhang, Z. Wan, Y. Lu, and S. Lin, "Verifiable and exculpable outsourced attribute-based encryption for access control in cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 6, pp. 679–692, 2017.
- [15] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Advances in Cryptology – EUROCRYPT 2011*, vol. 6632 of Lecture Notes in Computer Science, pp. 568–588, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.
- [16] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security - CCS '06*, pp. 89–98, New York, NY, USA, 2006.
- [17] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 457–473, Springer, Berlin, Heidelberg, 2005.
- [18] D. Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 1–722, 2016.
- [19] Z. Li, D. Wang, and E. Morais, "Quantum-safe round-optimal password authentication for mobile devices," *IEEE Transactions on Dependable and Secure Computing*, 2020.
- [20] S. Qiu, D. Wang, G. Xu, and S. Kumari, "Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Transactions on Dependable and Secure Computing*, 2020.
- [21] C. Wang, D. Wang, Y. Tu, G. Xu, and H. Wang, "Understanding node capture attacks in user authentication schemes for wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, 2020.
- [22] Y. Rouselakis and B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security - CCS '13*, pp. 463–474, New York, NY, USA, 2013.
- [23] G. Zhao, Q. Jiang, X. Huang, X. Ma, Y. Tian, and J. Ma, "Secure and usable handshake based pairing for wrist-worn smart devices on different users," *Mobile Networks and Applications*, 2021.

- [24] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K.-K. R. Choo, "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9390–9401, 2020.
- [25] J. Zhang, J. Ma, Z. Ma et al., "Efficient hierarchical data access control for resource-limited users in cloud-based e-health," in *2019 International Conference on Networking and Network Applications (NaNA)*, pp. 319–324, Daegu, Korea (South), 2019.
- [26] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, Berkeley, CA, USA, 2007.
- [27] M. Chase, "Multi-authority attribute based encryption," in *Theory of Cryptography Conference*, pp. 515–534, Springer, 2007.
- [28] M. Chase and S. S. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in *Proceedings of the 16th ACM conference on Computer and communications security - CCS '09*, pp. 121–130, New York, NY, USA, 2009.
- [29] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of abe ciphertexts," *USENIX Security Symposium*, vol. 2011, no. 3, 2011.
- [30] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1735–1744, 2014.
- [31] K. Yang and X. Jia, "Attributed-based access control for multi-authority systems in cloud storage," in *2012 IEEE 32nd International Conference on Distributed Computing Systems*, pp. 536–545, Macau, China, 2012.
- [32] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp. 1343–1354, 2013.
- [33] Baodong Qin, R. H. Deng, Shengli Liu, and Siqi Ma, "Attribute-based encryption with efficient verifiable outsourced decryption," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 7, pp. 1384–1393, 2015.
- [34] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Public-Key Cryptography - PKC 2013*, pp. 162–179, Springer, Berlin, Heidelberg, 2013.
- [35] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: distributed access control in clouds," in *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 91–98, Changsha, China, 2011.
- [36] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: effective data access control for multi-authority cloud storage systems," in *2013 Proceedings IEEE INFOCOM*, pp. 2895–2903, Turin, Italy, 2013.
- [37] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 384–394, 2014.
- [38] S. Hohenberger and B. Waters, "Online/offline attribute-based encryption," in *Public-Key Cryptography - PKC 2014*, vol. 8383, pp. 293–310, Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.
- [39] P. Datta, R. Dutta, and S. Mukhopadhyay, "Fully secure online/offline predicate and attribute-based encryption," in *Information Security Practice and Experience*, vol. 9065, pp. 331–345, Springer International Publishing, 2015.
- [40] S. Even, O. Goldreich, and S. Micali, "On-line/off-line digital signatures," *Journal of Cryptology*, vol. 9, no. 1, pp. 35–67, 1996.
- [41] A. Shamir and Y. Tauman, "Improved online/offline signature schemes," in *Advances in Cryptology - CRYPTO 2001*, pp. 355–367, Springer Berlin Heidelberg, Berlin, Heidelberg, 2001.
- [42] F. Guo, Y. Mu, and Z. Chen, "Identity-Based Online/Offline Encryption," in *Financial Cryptography and Data Security*, vol. 5143 of Lecture Notes in Computer Science, pp. 247–261, 2008.
- [43] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in *Applied Cryptography and Network Security*, pp. 111–129, Springer, Berlin, Heidelberg, 2008.
- [44] J. Lai, R. H. Deng, and Y. Li, "Fully Secure Ciphertext-Policy Hiding CP-ABE," in *Information Security Practice and Experience vol. 6672*, pp. 24–39, Springer, Berlin, Heidelberg, 2011.
- [45] J. Lai, R. H. Deng, and Y. Li, "Expressive CP-ABE with partially hidden access structures," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security - ASIACCS '12*, ACM: New York, 2012.
- [46] Y. Zhang, X. Chen, J. Li, D. S. Wong, and H. Li, "Anonymous attribute-based encryption supporting efficient decryption test," in *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security - ASIA CCS '13*, pp. 511–516, ACM: New York, 2013.
- [47] H. Cui, R. H. Deng, G. Wu, and J. Lai, "An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures," in *Provable Security, vol. 10005*, pp. 19–38, Springer, Cham, 2016.
- [48] H. Cui, R. H. Deng, J. Lai, X. Yi, and S. Nepal, "An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures, revisited," *Computer Networks*, vol. 133, pp. 157–165, 2018.
- [49] Z. Zhou, D. Huang, and Z. Wang, "Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption," *IEEE Transactions on Computers*, vol. 64, no. 1, pp. 126–138, 2015.
- [50] T. V. X. Phuong, G. Yang, and W. Susilo, "Hidden ciphertext policy attribute-based encryption under standard assumptions," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 35–45, 2016.
- [51] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology - CRYPTO 2001*, pp. 213–229, Springer, 2001.
- [52] A. Kate, G. M. Zaverucha, and I. Goldberg, "Pairing-based onion routing," in *Privacy Enhancing Technologies*, pp. 95–112, Springer, Berlin, Heidelberg, 2007.
- [53] A. De Caro and V. Iovino, "JPBC: Java pairing based cryptography," in *2011 IEEE Symposium on Computers and Communications (ISCC)*, pp. 850–855, Kerkyra, Greece, 2011.

Research Article

Multiagent Minimum Risk Path Intrusion Strategy with Computational Geometry

Jianguo Sun , Zining Yan , and Sizhao Li 

College of Computer Science, Harbin Engineering University, Harbin 150001, China

Correspondence should be addressed to Sizhao Li; sizhao.li@hrbeu.edu.cn

Received 19 March 2021; Revised 26 May 2021; Accepted 21 June 2021; Published 9 July 2021

Academic Editor: Ding Wang

Copyright © 2021 Jianguo Sun 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 wireless sensor networks (WSNs), inefficient coverage does affect the quality of service (QoS), which the minimum exposure path (MEP) is traditionally used to handle. But intelligent mobile devices are generally of limited computation capability, local storage, and energy. Present methods cannot meet the demand of multiple target intrusion, lacking the consideration of energy consumption. Based on the Voronoi diagram in computational geometry, this paper proposed an invasion strategy of minimum risk path (MRP) to such a question. MRP is the path considered both the exposure of the moving target and energy consumption. Federated learning is introduced to figure out how to find the MRP, expressed as $C(t_i, t_j) = f(E, e)$. The value of $C(t_i, t_j)$ can measure the success of an invasion. At the time when a single smart mobile device invades, horizontal federated learning is taken to partition the path feature, and a single target feature federated (SPF) algorithm is for calculating the MRP. Moreover, for multi smart mobile device invasion, it has imported the time variable. Vertical federated learning can partition the feature of multipath data, and the multi-target feature federated (MFF) algorithm is for solving the multipath MRP dynamically. The experimental results show that the SPF and MFF have the dominant advantage over traditional computational performance and time. It primarily applies the complex conditions of a massive amount of sensor nodes.

1. Introduction

Wireless sensor networks (WSNs) composed of many sensors are widely used in many fields, such as building monitoring, intelligent transportation system (ITS), and enemy status report [1, 2]. What mainly affects network quality is coverage, especially the WSN barrier coverage problem [3]. According to the coverage classification, barrier coverage is one of the three coverage strategies to detect unauthorized intruding behaviour in monitored areas. Moreover, its quality measurement factors are mainly breaching, supporting, or exposure of the penetration path [4]. To reduce the risks of being found, invaders can make effective path planning and minimize the exposure [5] through intelligent algorithm.

Minimum exposure path (MEP) [6] is a significant way that assesses the coverage effect of WSN to optimize the management of WSN. By finding out the MEP, the defender can estimate where the sensor network coverage is weak because the invader crossed the sensing field along this path is the most difficult to detect [7]. Therefore, this paper will study

how to find an optimal invasion path from the perspective of intruders.

Meguerdichian et al. [8] put forward the Voronoi diagram numerical solution combined with WSN and solved the MEP problem by the shortest path algorithm. Chechik et al. [9] defined the exposure by the number of nodes adjacent to the moving target, considering single-path connectivity to solve the MEP problem.

In this paper, considering the perspective from invaders, the monitoring area is modelled by the Voronoi diagram that divided the field into undirected graphs that are a set of segmented linear components to limit the optimal searching space.

Previous studies have shown that for intruders, the threat can be viewed as the probability of being detected by the sensor nodes when passing through the WSN, namely, the exposure. Exposure is the expected average ability of intrusion targets moved in the monitored area. Mathematically, the invader's exposure time and sensor field intensity should be taken into account when calculating the exposure degree.

Exposure can be formulated as a path integral when the sensor field intensity is accumulated along a path from the source point to the destination point during a time interval.

According to the Cannikin Law [10], the reliability of the penetration path depends not only on its total exposure degree but also on the exposure of the discrete edges that make up the path. And when the invader passes through the monitoring area in some circumstances, it will be limited by time, distance, exposure, and energy consumption. Therefore, it is not accurate to find the path with the minimum total exposure degree. It is necessary to find an approach that is more in line with actual needs. The minimum risk path (MRP) is called to sum up the above paths in this paper.

However, most of the researchers consider only one single intruder when solving the intrusion path. In actual situations, such as the Underwater Listening Network, a system collects underwater sounds and tracks and monitors the Navy's passing ships and submarines. Underwater listeners are installed on the seafloor and act as sensor nodes. The moving target is an autonomous underwater vehicle (AUV) that needs to pass through the monitoring area. Multiple AUV intruders cross the sensing field simultaneously and cooperate with each other, as shown in Figure 1. Invader 1 and invader 2 need to walk along two different paths to collect more information as far as possible, which will add to the complexity of path planning.

By contrast with the traditional method, federated learning allows multiple data owners to establish a shared model [11] with the protection of local data. It is conducive for updating the global data model dynamically to path planning. Yang et al. [12] introduced a federated learning framework of comprehension and security in 2019. Zhu and Jin [13] optimized the structure of neural network models by multiobjective evolutionary algorithms while minimizing communication costs and global model testing errors. Sodhro et al. [14] proposed a dynamic method of forward-center by adjusting the running time of the sensing and transmission process in the Internet of Things devices, which allocates resources with effectiveness and fairness.

The horizontal federated learning applies to that the data features of participants overlap more, and the sample IDs are less. For a single intrusive target, the edges of the Voronoi diagram generated of WSN can be seen as a data set. The evaluation indicators of exposure and energy consumption can be regarded as a feature space. The intersection of the feature space is massive between the data sets. Hence, a data set can be divided into horizontal sections. It aggregates different data in the same feature space to train a model for the ideal path of the moving target. The above single intrusion target pathfinding algorithm combined with federated learning is called SPF.

The vertical federated learning is suitable to the case of the ID of the training samples of participants overlap more and the data features less. Moving intrusion targets can be considered as data sets of this time. The feature space is the exposure and the energy consumption, which is the current position of the moving target location at the moment. Consequently, the different features of the common samples of multiple participants (intrusion targets) can be trained by vertical federated learning, which increased the feature

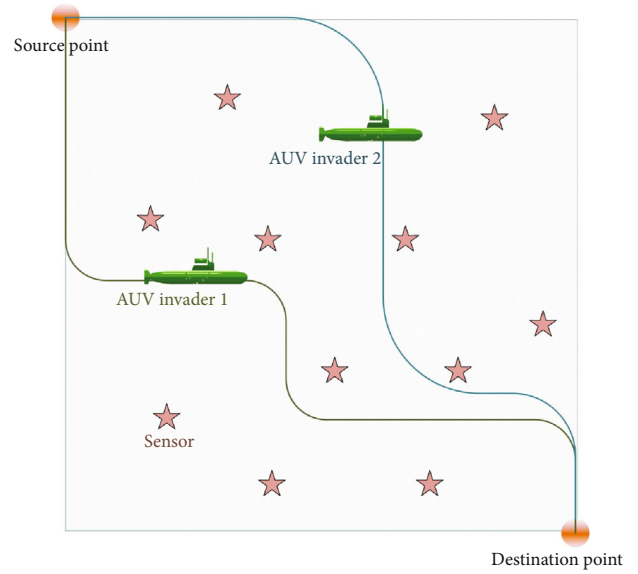


FIGURE 1: Multitargets: AUVs.

dimensions of samples to build a multiobjective path planning model. The dynamic pathfinding algorithm for multiple intrusion targets based on federated learning is called MFF.

In summary, the main contributions of this paper are as follows.

- (1) Considering the influence of various factors on the path, propose the concept of a minimum risk path
- (2) Innovatively combine federated learning with path planning to build an intrusion algorithm and find out the MRP
- (3) The optimal path is worked out through a dynamically segmented solution of the generated model. Experimental results show that the SPF algorithm can reduce computational complexity and improve performance
- (4) Based on the vertical federated learning, it established a dynamic path planning model and MFF algorithm for multiple intrusion targets that make full use of multiobjective programming characteristics. Augmenting additional requirements can work out diverse path combinations

The rest part of this paper is as follows. The second part is the model building process. The detail of the proposed algorithm is described in the third section. In the fourth section, the experimental results are discussed. We formulate the evaluation indexes of the intrusion path planning algorithm in the fifth section. The final part is the summary of the whole paper.

2. Model Aggregation Based on Feature-Partitioned

2.1. Preliminaries. The sensing model determines the scope, and monitoring capability can be a usage of abstracting the

sensing range of the same class nodes. In a bounded region F , presumed n active sensor nodes s_1, s_2, \dots, s_n would be deployed in predetermined locations. They can detect the target T appearing in any point within the sensing field. The detected sensing signal attenuates with the increasing Euclidean distance between the sensor node $s_i (i = 1, \dots, n)$ and the target T . The specific *sensing model* for detecting the target T signal can determine the exposure of the target which moves along the path.

With the increasing transmission distance, the practically environmental noise interference and signal strength will attenuate. The detection probability of the node tapers as the distance grows between the moving target and the sensor node [15]. The detection capability of sensor nodes shows the uncertainty that attenuated disk perception model reflected.

On this basis, Rai and Daruwala [16] studied the coverage problem under the attenuated disk perception model. The detection probability $p(u, s_i)$ of s_i against the point u in region F can be expressed as in equation (1). In this paper, we selected the order type attenuated disk perception model.

$$p(u, s_i) = \lambda \cdot d(u, s_i)^{-K}. \quad (1)$$

Euclidean distance between u and s_i is $d(s_i, u)$. λ and K are the positive parameters relevant to the sensing capability. λ depicts the energy factor transmitted or reflected by the target, and K represents the path attenuation exponent. In standard conditions, the value of K is in a range of constant between 2 and 5.

In region F , u is at any point, and s_m is the sensor node with the shortest Euclidean distance to point u . The maximum-sensor intensity function $I_C(F, u)$ indicates the effective sensing measurement of s_m to u . Function I_C value of point P can be expressed as in (2) while the freely moving target P runs to the situation of u .

$$\begin{aligned} s_{\min} &= s_m \in S | d(s_m, u) \leq d(s, u) \forall s \in S, \\ I_C(F, u) &= p(u, s_{\min}). \end{aligned} \quad (2)$$

t is the time variable. When the target P is moving at a constant speed v , (2) can be converted into

$$E(t_i, t_j) = v \cdot \int_{t_i}^{t_j} I(F, u) dt. \quad (3)$$

Exposure is a quantitative expression of network coverage performance, and the definition varies with the changing of application environments. Binh et al. [17] reckoned that exposure is the ability of WSN to detect objects passing through the sensing region. Aravinth et al. [18] defined exposure as the probability of detecting a target in the sensing region.

This paper endues two factors to explicate exposure: target moving time and induction intensity. It is noticeable that time accumulation affects induction intensity as the target passing through the sensor area. In the sensor region F , targets moving along the path over a while, its exposure degree can be described as (4).

$$E(t_i, t_j) = \int_{t_i}^{t_j} I(F, u) \left| \frac{du}{dt} \right| dt. \quad (4)$$

The threat model in this paper is a quantitative description of the optimal invasion path for intruders. The model can analyze the situation of the WSN, quantify the capability of the sensor nodes, and plan the invasion path of the adversary to the whole WSN reasonably. Specifically speaking, we firstly simulate the distribution of sensor network nodes to generate the network topology, and then, the intrusion path is planned according to the quantized threat data. A definition for the threat model is determined.

Definition 1. Given the overwhelming probability that an intruder can successfully penetrate the entire network if the value of $E(t_i, t_j)$ is as small as possible.

The concept of the Voronoi diagram is derived from computational geometry. It divides a plane into multiple regions by a collection of points called generators [19]. Considering a convex Euclidean domain F and a set Q of points q_0, q_1, \dots, q_n in F , Voronoi regions related to set Q are defined as (5) where $d(p, q)$ is the Euclidean distance between p and q .

Equation (5) means that a point $p \in F$ belongs to the Voronoi region $V(q_i)$, if the distance between p and q_i is the shortest distance between p and any other point $q_j \in Q$. The point $q_j \in Q$ is generating points or generators of the Voronoi partition.

$$V(q_i) = \bigcap_{j \neq i} \left\{ p \in F | d(p, q_i) < d(p, q_j), \forall q_j \in Q \right\}, \forall q_i \in Q. \quad (5)$$

In this paper, specific partitions (Voronoi diagram) can be produced according to the position of generating points (sensor nodes) in mission space (WSN) which separates sensor region F into multiple convex polygons. Each one contains a sensor node that its edge is called the *Voronoi edge*, and the intersection of *Voronoi edge* is the *Voronoi vertex*.

The characteristics of the Voronoi diagram played a key role. As a result, the minimum exposure path is right on the *Voronoi edge* precisely, under the maximum-sensor intensity. The Voronoi diagram or Voronoi partition that was generated via WSN consists of all the Voronoi cells of sensors.

Two types of methods can generate the Voronoi diagram. One is direct method that Voronoi diagram is generated from a set of points, such as half plane method, incremental construction method, divide and conquer method, plane scanning line method. Another is indirect which it takes the relationship between Voronoi diagram and the dual diagram of Delaunay triangle network. The point set is firstly subdivided to generate Delaunay triangle network and then to construct the Voronoi diagram.

If the corresponding Voronoi cells of sensor q_i and q_j have a same boundary, they become Delaunay neighbours and all the ones gathered to be an edge set of the Delaunay graph. Delaunay graph is dual to the Voronoi diagram, and consequently, one graph can be drawn from its dual counterpart. According to Table 1, triangulation generation method

TABLE 1: Comparison of Delaunay generation algorithms.

Algorithm	General condition	Worst condition
Lewis and Robinson	$O(n \log n)$	$O(n^2)$
Lee and Schachter	$O(n \log n)$	$O(n \log n)$
Dwyer	$O(n \log \log n)$	$O(n \log n)$
Chew	$O(n \log n)$	$O(n \log n)$
Lawson	$O(n^{4/3})$	$O(n^2)$
Lee and Schachter	$O(n^{3/2})$	$O(n^2)$
Bowyer	$O(n^{3/2})$	$O(n^2)$
Watson	$O(n^{3/2})$	$O(n^2)$
Sloan	$O(n^{5/4})$	$O(n^2)$
Green and Sibson	$O(n^{3/2})$	$O(n^2)$
Brassel and Reif	$O(n^{3/2})$	$O(n^2)$
McCullagh and Ross	$O(n^{3/2})$	$O(n^2)$
Improved point-by-point insertion method (IPI)	$O(n \log n)$	$O(n \log n)$

is at the lowest time efficiency, point-by-point insertion method the middle, and divide-and-conquer algorithm the highest. The point-by-point insertion algorithm that owned high time efficiency can implement simply, occupying less space in operation.

The first part of the table from top to bottom is divide-and-conquer algorithm, the second part is point-by-point insertion algorithm, and the third part is triangulation generation method. This paper considering time and space efficiency, with the improved point-by-point insertion method (IPI), constructs Delaunay triangulation. The Voronoi diagram is structured upon the Delaunay triangle. By contrast to the point-by-point insertion algorithm, it can diminish the number of relevant point judgment and the computational complexity by arranging points first x and then y .

The specific construction process is shown in Algorithm 1.

$V(WSN)$ is specific Voronoi diagram generated upon sensor network node distribution. Vertex corresponding of $V(WSN)$ has a one-to-one relationship to each *Voronoi vertex* of the general Voronoi diagram $V(A)$. Vertexes in $V(WSN)$ include the vertexes of $V(A)$ and other points intersected the edges of $V(A)$ and boundary of region F , as shown in Figure 2. The process of constructing $V(WSN)$ is shown in Algorithm 2.

2.2. Parameter Calculation. The network flow is a specific flow solution that is closely related to linear programming [20]. This paper presents a new idea that edges have been defined as *Voronoi edges* and the flow as the moving target passed by this edge. The capacity can be considered as the maximum number of moving targets that each *Voronoi edge* can hold. Each node (not a source point or a sink point) is like an analogy to a *Voronoi vertex*, while the capacity is not limited.

Definition 2. The capacity network $D = (V, A)$ (V is the vertex of an undirected graph and A is the arc), and each arc (V_i, V_j) endues the transmission cost per unit moving $b_{ij} \geq 0$, denoted as

$$D = (V, A, B), b_{ij} \in B. \quad (6)$$

The maximum flow from source to sink can be found in the cost network D , and the total transfer cost of the stream is at a minimum.

Definition 3. If the moving target velocity was a constant v , the time increment dt would have a significant linear correlation between the unit length ds defined as

$$ds = v \cdot dt. \quad (7)$$

The energy consumption is defined below.

Definition 4. Supposing q is the energy consumption of unit length while target moving, the time variable is t and the time interval from V_i to V_j is $[t_i, t_j]$. In the sensor region F , the energy consumption of the target which moves along the path $r(t)$ at a constant speed v , is defined as

$$e(t_i, t_j) = \int_{t_i}^{t_j} v q dt. \quad (8)$$

The analytic discrete method can work out this problem, using a variational method to obtain the analytical solution to the risk optimization problem. Such a method simplifies original question to a set of differential equations about the optimal trajectory coordinates. How the trajectory is defined will make the complexity of the system.

```

Input: Vertex list (Vertices)
Output: A list of determined triangles (Triangles)
1: Initialise the Vertices
2: Create an index list indices
3: Sort the indices bases on the x-coordinates of Vertices
4: Get the super triangle (A super triangle means that the triangle contains all the points in the point set)
5: Save the duper triangle to the temp triangles list
6: Push the super triangles into Triangles list
7: for Each sample point in the Vertices list sorted by indices do
8:   Initialize the edge buffer
9:   for Each triangle in temp triangles do
10:    Calculate the center and radius of the triangle
11:    if The point is on the right side of the circumcircle then
12:      This triangle is a Delaunay triangle, save it in Triangles
13:      Remove the triangle from temp triangles list
14:      Skip
15:    else if The point is outside the circumcircle then
16:      This triangle is uncertain
17:      Skip
18:    else The point lies on the inside of the circumcircle
19:      This triangle is not a Delaunay triangle, add the three triangle edges to edge buffer
20:      Remove the triangle from temp triangles list
21:    end if
22:  end for
23:  Delete all repetitive edges in edge buffer
24:  Combine the edges in the edge buffer with the current point, and save these triangles into temp triangles
25: end for
26: Combine the temp triangles and Triangles
27: Remove triangles associated with super triangles vertices from Triangles list

```

ALGORITHM 1: IPI algorithm.

Presuming the coordinate of Voronoi vertex V_k is (x_{V_k}, y_{V_k}) , and $t(p)$ is the path crossing time. The length of the edge $\langle V_i, V_j \rangle$ is expressed as $l_{V_i V_j}$.

The travel time along the edge $\langle V_i, V_j \rangle$ of the moving target is indicated by $t_{V_i V_j}$. $I_{V_i V_j}$ is the induction intensity of the nearest sensor nodes $s_1(s_2)$ when the target moves along the edge. $|d_{s_i V_k}|$ is the distance from the sensor node $s_1(s_2)$ to the point V_k , and $\theta_{s_i V_i V_j}$ is the angle of $\angle V_i s_1 V_j$. The coordinates of s_1 is (x_1, y_1) ; hence, $t_{V_i V_j}$ can be expressed as

$$t_{V_i V_j} = \frac{l_{V_i V_j}}{v} = \frac{\sqrt{(x_{V_j} - x_{V_i})^2 + (y_{V_j} - y_{V_i})^2}}{v}. \quad (9)$$

Analyzing the cost solution, suppose a sensor of Voronoi cells located in the coordinate system origin point, using the polar coordinate system. The relationship between Cartesian coordinate x, y , polar radius ρ , and polar angle Ψ is as in (10).

$$\begin{aligned} x(s) &= \rho(s) \cos \Psi(s), \\ y(s) &= \rho(s) \sin \Psi(s). \end{aligned} \quad (10)$$

For points V_i and V_j , polar radius ρ and angle θ can be expressed as in (11) and (12)

$$\rho_i = \sqrt{x_i^2 + y_i^2}, \quad (11)$$

$$\rho_j = \sqrt{x_j^2 + y_j^2},$$

$$\theta = \arccos \left(\frac{x_i x_j + y_i y_j}{\rho_i \rho_j} \right). \quad (12)$$

To derive the formula for the exposure index, it calculates the cumulative exposure of a moving target affected by s_1 from V_i to V_j . λ is the induction parameter determined by the sensor node hardware, and K is the distance impact factor with its value in common between 2 and 5. It has presumed $\lambda = 1, K = 2$ and induction intensity expressed as in (13)

$$\begin{aligned} v \cdot \int_{t_{V_a}}^{t_{V_b}} d^{-2} \left| \frac{dp}{dt} \right| dt &= \int_{V_a}^{V_b} d^{-2} dp = \int_{x_{V_a}}^{x_{V_b}} \frac{\sqrt{1 + (y'_x)^2}}{(x - a_i)^2 + (y - b_i)^2} dx \\ &= \frac{(\arctan(y_{V_b} - b_i/x_{V_b} - a_i) - \arctan(y_{V_a} - b_i/x_{V_a} - a_i)) \cdot l_{V_a V_b}}{(x_{V_a} - a_i)(y_{V_b} - b_i) - (x_{V_b} - a_i)(y_{V_a} - b_i)}. \end{aligned} \quad (13)$$

Vector $(x_{V_k} - x_1, y_{V_k} - y_1)$ can be indicated by $d_{s_i V_k}$, and the angle between vector $d_{s_i V_i}$ and $d_{s_i V_j}$ can be indicated by $\theta_{s_i V_i V_j}$ that meets the condition $0 \leq \theta_{s_i V_i V_j} \leq \pi$. So, it can be simplified to (14)

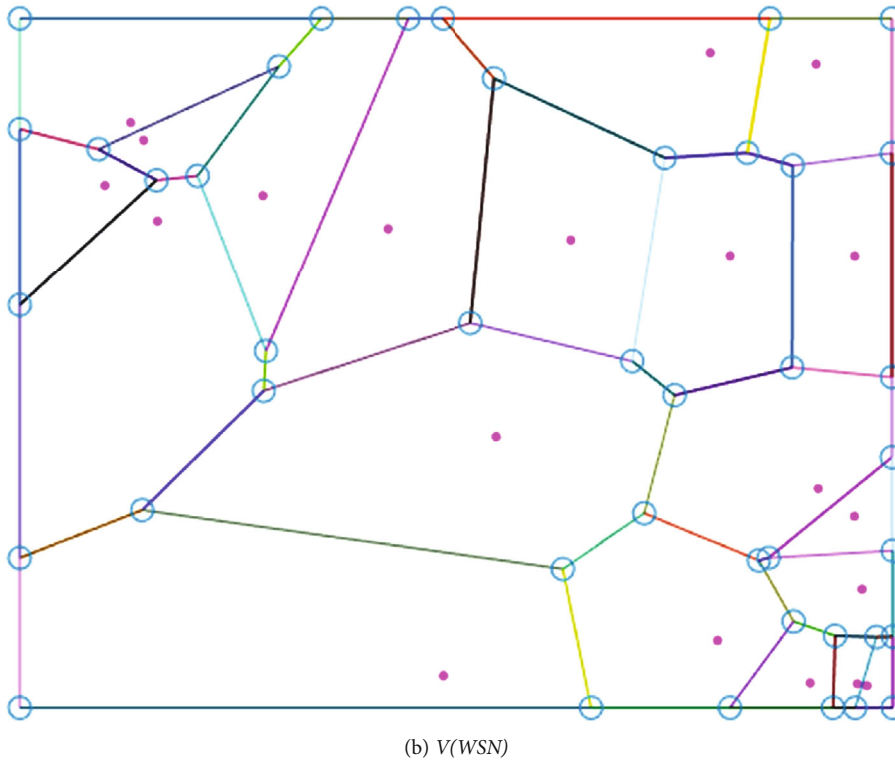
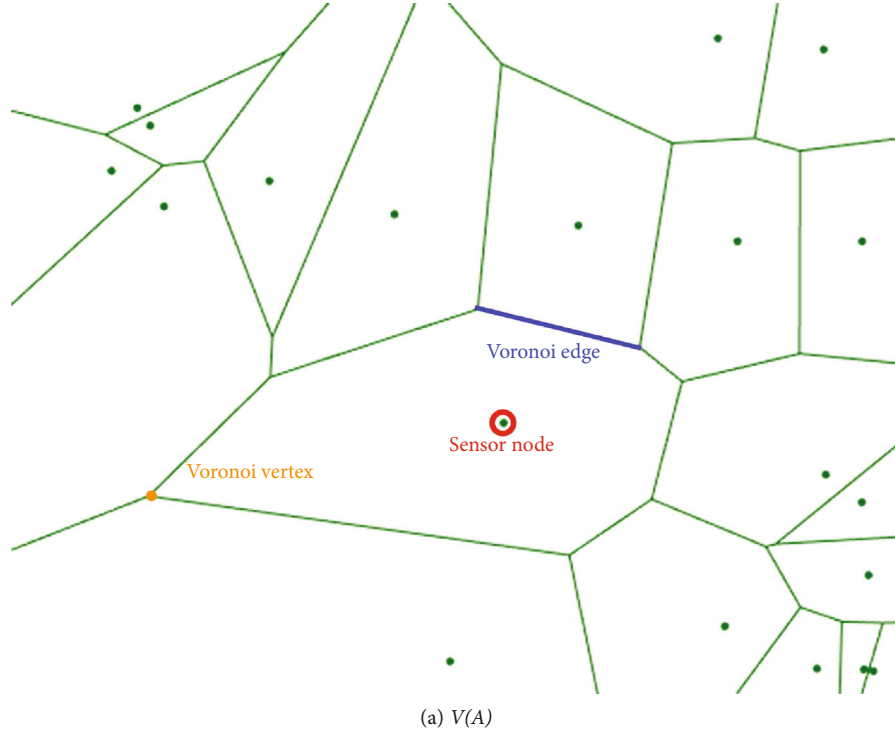


FIGURE 2: Voronoi diagram of WSN.

$$v \cdot \int_{t_{V_i}}^{t_{V_j}} d^{-2} \left| \frac{ds}{dt} \right| dt = \frac{\theta_{s,V_i V_j}}{\sin \theta_{s,V_i V_j}} \cdot \frac{l_{V_i V_j}}{|d_{i,V_i}| \cdot |d_{i,V_j}|}. \quad (14)$$

sure can be calculated by (16), and the target moving total exposure $E(p)$ is (17).

$$I_{s,V_i V_j} = \frac{\theta_{s,V_i V_j}}{\sin \theta_{s,V_i V_j}} \cdot |d_{s,V_i}|^{-1} |d_{s,V_j}|^{-1}, \quad (15)$$

The induction intensity is transformed into (15). The expo-

Input: Vertex list (*Vertices*), Region *F*
Output: $V(\text{WSN})$

- 1: Initialize the *Vertices*
- 2: Create an edge list *Voronoi edge*
- 3: Use IPI algorithm to construct Delaunay triangular network based on *Vertices*
- 4: Number the discrete points and formed them into triangles. Then record three discrete points composed of each triangle
- 5: Calculate the center of each circumcircle of triangle and record it
- 6: for The *triangle* list do Find adjacent triangles *TriA*, *TriB*, and *TriC* that share side with the current triangle *tempTri*
- 7: if Three adjacent triangles are found then
- 8: Connect the outer center of *TriA*, *TriB*, and *TriC* to the outer center of *tempTri*. Put the connected edge into *Voronoi edge* list
- 9: else Three adjacent triangles are not found
- 10: Find the outermost midperpendicular ray and put it into *Voronoi edge* list
- 11: end if
- 12: end for
- 13: Calculate the point of intersection between *Voronoi edge* and region *F*
- 14: Connect *intersection point* according to *F* (acquire *line of intersection*)
- 15: $V(\text{WSN})$ is constructed by *Voronoi edge* and *line of intersection*

ALGORITHM 2: Construction of $V(\text{WSN})$.

$$E_{s,V_i V_j} = I_{s,V_i V_j} \cdot l_{V_i V_j}, \quad (16)$$

$$E(p) = \sum_{i=c}^{j=f} E_{V_i V_j}. \quad (17)$$

3. Find the MRP Using Dynamic Programming and Federated Learning

For the intrusion path selected, the primary goal is to avoid being detected by WSN. It is essential of thinking about how to select a path according to topology of WSN that meets the demands of the actual path seeking process. Therefore, the network topology data preprocessing is a very critical step. We can learn from federated learning, divide, and conquer.

The main idea of federated learning is to build machine-learning models based on data sets distributed over multiple devices [21]. Hao et al. [22] proposed an efficient scheme to solve sensitive data-driven industrial scenarios, and Lu et al. [23] formulate the data-sharing problem into a machine-learning problem via incorporating privacy-preserved federated learning. WSN can generate a significant amount of data [24]. According to the federated learning framework, we can perform data preprocessing on the WSN network topology. It should be noted that the research object of this paper is the static network, only using federated learning methodology, and there is no actual learning process.

Compared to the traditional method, federated learning is beneficial for dynamically updating the global data model on path planning. Thus, federated learning can deal with the MRP problem.

3.1. Single Mobile Device

3.1.1. The Calculation Model Established by Feature-Partitioned. Let matrix D_i denote data onto each *Voronoi edge*. Each row of the matrix represents a sample, and every column marks a feature. The feature space X includes exposure (E) and energy consumption (e), defining I the sample

ID space (*Voronoi edge* number). The feature FE and sample Ids SI constitute the entire training data set (SI, FE).

Horizontal federated learning, also sample-based federated learning, was introduced in that data sets shared the same space in feature but distinct space in samples [25]. Horizontal federated learning is summarized as

$$FE_i = FE_j, SI_i \neq SI_j, \forall D_i, D_j, i \neq j. \quad (18)$$

The intersection of feature space is enormous between the data set of *Voronoi edges*. Then, the data set can be horizontally segmented, and varied data onto the same feature space can be aggregated. Consequently, it trains the model to solve a selection of the optimal path while the target is moving.

Step 1. Participants compute exposure locally with encryption and send results to the server.

Step 2. The server performs secure aggregation without learning information about any participant and calculates the average value of exposure.

Step 3. The server sends back the aggregated results to participants.

Step 4. Participants update their respective model with the decrypted results.

The primary goal of intrusion path is avoiding detection by WSN and then considering over the influence of energy consumption. In Step 2, the method of calculating the average exposure value of the entire network is as shown in (19), and l_{all} is the length of path.

$$E' = \frac{E_1 + E_2 + \dots + E_n}{l_{\text{all}}}. \quad (19)$$

Therefore, the predicted exposure value $E_{\text{pre}}(V_i, V_j)$ from point V_i to point V_j can be expressed as (20)

$$E_{\text{pre}}(V_i V_j) = d_{V_i V_j} \cdot E'. \quad (20)$$

Because the length is the fundamental dimension of quantity, we can describe them by length L . According to (15) and (16), E is dimensionless parameter because the dimension of I is $1/L$ and the dimension of $l_{V_i V_j}$ is L . So, the dimension of E_{pre} is L . The dimension of e can be computed according to (8) in the same way. L is the dimension of e , too.

The time complexity of Voronoi graph generation was $O(n \log n)$ [26]. With Voronoi diagram $(3n - 6)$ edges, accordingly it takes no more than $O(n)$ to calculate the exposure of all *Voronoi edges*. Based on dimensional analysis, the judgment function $C(t_i, t_j)$ can be defined as shown in (21). The value of $C(t_i, t_j)$ can measure the successfulness of an invasion.

$$C(t_i, t_j) = \left(\int_{t_i}^{t_j} E' \left| \frac{dp}{dt} \right| dt \right) + \left(\int_{t_i}^{t_j} q \left| \frac{dp}{dt} \right| dt \right). \quad (21)$$

3.1.2. The Flow of Algorithm and the Procedure of Realization. In actual path planning, combinations of edges that are possibly feasible flows can be various. Hence, it has to dynamically update the priority to the selected edges keeping the searching direction under control in planning an optimal path. Furthermore, the cost is optimal for each extended path. The valuation function of moving target from the starting node s via current node $X(x, y)$ to the end node f can be defined.

Definition 5. $G(X)$ is the total exposure value from the start node to the current node, which can be obtained by adding up the weights of any neighboring edge of the path that traveled. $H(X)$ is the heuristic estimated cost function (included exposure and energy consume) which is only as a judgment, not as a part of cost calculation. The total cost value $F(X)$ can be expressed as

$$F(X) = G(X) + H(X). \quad (22)$$

Considering an ideal condition that the target in motion is supposed to be increasingly closer towards the destination, according to the feature-partitioned of federated learning, $H(X)$ could be accordingly expressed as

$$H(X) = E' \cdot d_{Y,f} + e(t_X, t_Y). \quad (23)$$

Y is the antecedent node of X . $d_{Y,f}$ is the Euclidean distance from Y to the end node s , and $E' \cdot d_{Y,f}$ expressed the exposure estimation from Y to f .

Define an empty table named *NotVis* and another *Been Vis*: nodes that have not been visited (need to be examined) are stored in the *NotVis* table, and nodes that have been visited are stored in the *BeenVis* table. The single intrusion target pathfinding algorithm combined with federated learning (SPF algorithm) is as Algorithm 3.

The SPF algorithm can output an optimal path by inputting the $V(\text{WSN})$ generated by the Voronoi diagram that con-

tains the connected edges and the position coordinates of each node and the point identifier from the source point s to final point f .

3.2. Multiple Mobile Devices

3.2.1. The Calculation Model Established by Feature-Partitioned. It is sometimes a practical demand to transfer multiple moving targets over a time interval. The vertical federated learning is suitable for the ID of the training samples of participants overlap more and the data features less. The moving target is deemed to be a sample set SI . The feature space FE is formed into the moving target position, the moment of the current position, and exposure degree. Vertically federated learning is a process aggregating different features above, in which a model can be built with data from moving targets in cooperation. Under such assumption, (24) can be got.

$$FE_i \neq FE_j, SI_i = SI_j, \forall D_i, D_j, i \neq j. \quad (24)$$

Training the model can solve the multi-optimal path of the moving target. Specific steps are as follows.

Step 1. Participants locally compute exposure and time and send masked results to the server.

Step 2. The server performs secure aggregation without learning information about any participant.

Step 3. The server sends back the aggregated results to participants.

Step 4. Participants update their respective model with the decrypted results.

Whereas varied positions of moving target A as time running would decide the direction of moving target B , time variable was imported over multi-objective path judgment. The probability of being detected by the sensor would be increasing (like a traffic problem [27]) as two moving targets on the same *Voronoi edge*. The presumption is that when target A is at *Voronoi edge* $V_i V_j$, if target B passing by edge $V_i V_j$, the heuristic estimated cost $H(B)$ of target B would be $H'(B)$.

$$H'_B = k \cdot H_B (k > 1). \quad (25)$$

The Underwater Sensor Network is a system that collects underwater sounds and tracks and monitors the Navy's passing ships and submarines. The underwater acoustic detectors (UADs) are installed on the seafloor and act as sensor nodes. The moving target is an autonomous underwater vehicle (AUV) that needs to pass through the monitoring area. For more information gathering and security reasons, it is a method to keep the AUV from going the same path as much as possible by adjusting the k value in (25).

3.2.2. The Algorithm Flow and the Procedure of Realization. When multiple intrusion targets need to be transmitted, a

```

Input: Graph  $V(\text{WSN})$ ;  $s$ ;  $f$ 
Output: optimal path
1:  $\text{NotVis} = [s]$ ;  $\text{BeenVis} = []$ ;
2: while The  $\text{NotVis}$  table is not empty do
3:   Select  $V_i$  with the lowest total proxy value  $F$  from  $\text{NotVis}$ . Then delete  $V_i$  from  $\text{NotVis}$  and insert  $V_i$  into  $\text{BeenVis}$ .
4:   if  $V_i$  is the end node  $f$  then
5:     Return path
6:   else
7:     Extend node  $V_i$ 
8:     for Each adjacent node  $V_j$  of  $V_i$  do
9:       Calculate the exposure  $E_{V_i, V_j}$ .
10:      if  $V_j$  is not in neither the  $\text{NotVis}$  or  $\text{BeenVis}$  table then
11:        Calculate  $F(V_j)$ 
12:        Insert  $V_j$  into the  $\text{NotVis}$  table. And add it a pointer variable pointing to node  $V_i$ .
13:      else if  $V_j$  is in the  $\text{NotVis}$  table then
14:        if  $F(V_j)$  is less than the estimated value  $F'(V_j)$  in  $\text{NotVis}$  table then
15:          Update  $F'(V_j)$  ( $F'(V_j) = F(V_j)$ ).
16:          Change the node pointer in the  $\text{NotVis}$  table to point to the current node  $V_i$ 
17:        else
18:          if  $F(V_j)$  is less than the estimates value  $F'(V_j)$  in  $\text{BeenVis}$  table then
19:            Update  $F'(V_j)$  ( $F'(V_j) = F(V_j)$ ).
20:            Delete  $V_j$  from  $\text{BeenVis}$  table and insert  $V_j$  into  $\text{NotVis}$  table
21:          end if
22:        end if
23:      end if
24:      Insert  $V_j$  into  $\text{BeenVis}$  table
25:    end for
26:  end if
27: end while
28: From  $f$  backtrack to  $s$ . Return path.

```

ALGORITHM 3: SPF algorithm.

time-variable is introduced in this paper to conduct dynamic pathfinding of multiple intrusion targets based on federated learning feature (MFF). Assuming that multiple moving targets M_1, M_2, \dots, M_n start from s every time interval T , the $H(X)$ value is updated according to the formula (25) and the location of the moving target at different times. Based on the SPF algorithm, we need to create some new data structures to store variables in the MFF algorithm, as shown in Table 2.

The specific algorithm flow is as Algorithm 4. By contrast to the SPF algorithm for a single intrusion target, the MFF algorithm sets a time variable to record the positions of distinct targets moving every period, which position relationship can update data onto the model.

4. Experiment

In this section, the performance of the SPF and MFF algorithm is validated through simulation experiments. It analyzed the condition that finding MRP was influenced by distinct node quantities and various distributed modes in the sensing area and whether the algorithms are effective against different network topologies.

It is assumed that the network topology application scenario is an Underwater Sensor Network in this paper.

The experimental environment is in an ideal state, as shown in Figure 3. The UADs are deployed on the seabed to form a monitoring area, and the AUVs move at a uniform speed in the same horizontal plane. From the starting point, the AUVs pass through the monitoring area to the endpoint to perform the underwater penetration mission of the submarine.

We plan to use underwater acoustic communication technology to solve information transmission and sharing among unmanned underwater clusters. In a multiagent case, clock synchronization between two agents is generally calculated by multi-round communication to calculate the deviation and offset rate between clocks. According to the research of Liu et al. [28], several particular nodes named anchors are selected among all moving targets in this paper to aid the localization process.

The anchors are clock synchronized that the moving target achieves clock synchronization by communicating with anchors and estimating the message propagation time. The targeted target broadcasts the location demand, and the anchor reveals the location message containing the sending time and location information after receiving the location request. When the targeted target receives the location message, the transmission delay of the message can be calculated based on the local clock and the sending time in the news. Then, the distance to the anchor can be estimated [29].

TABLE 2: Comparison of Delaunay generation algorithms.

DetCost_Lines	The exposure value of each <i>Voronoi edge</i>
DetTime_Lines	The time required for the moving target to move along each <i>Voronoi edge</i> (V_iV_j)
Path_Cost	The respective cost and total cost of all departing moving targets at a given time
Path_FCost	The respective projected cost values of all departing moving targets at a given time
Path_Record_CurrentPoint	The name of the current point
Path_Record_PreviouPoint	The previous node name

```

Input: Graph  $V(WSN)$ 
Output: optimal path
1:  $NotVis=[s]; BeenVis=[]$ 
2: while The  $NotVis$  table is not empty do
3:   Select the path with the lowest total proxy value  $F$  from  $NotVis$ . And record the corresponding moving target serial number  $i$ .
4:   if All moving targets are the end node  $f$  then
5:     Return  $path$ 
6:   end if
7:   Update DetCost_line according to (25) and path
8:   Sort Path_Time_CurrentPoint in ascending order, and record the moving target serial number respectively. (Determine the moving target  $M_j$  that reaches the next Voronoi vertex first)
9:   for All moving targets do
10:    if  $M_j$  reaches the end point then
11:      Calculate path of  $M_j$ 
12:    elseBreak;
13:    end if
14:  end for
15:  Make path prediction for  $M_i$  which has minimum value of Path_Time_CurrentPoint by SPF algorithm
16:  Update Path_Record_CurrentPoint
17:  Update Path_Time_CurrentPoint
18:  Goto line 7
19: end while

```

ALGORITHM 4: MFF algorithm.

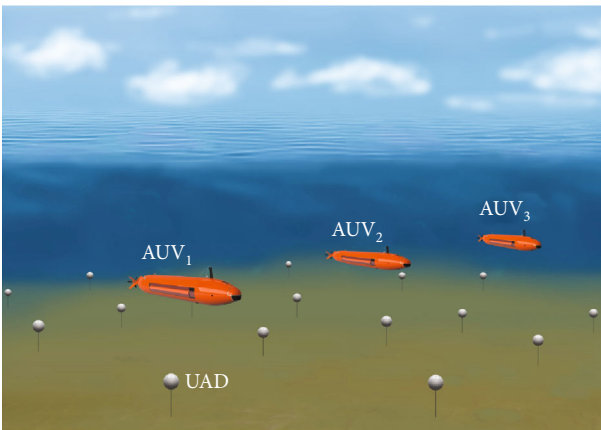


FIGURE 3: Underwater Sensor Network.

4.1. Single Mobile Device. To verify the accuracy of the model and algorithm, we can figure out the minimum exposure path via the topology in [6]. The data manifested in Table 3 are the parameters in the experiment. And the results can

TABLE 3: Experimental parameters (1).

Parameter	Value
Monitoring area	300 * 300
λ	1
K	2
q	0
k	2
n	32
Starting point	(0,120)
Ending point	(300,195)

be found in Figure 4. The number of sensor nodes is expressed by variable n .

Thirty-two sensors are deployed on a 300 * 300 monitoring field. We used the HGA-NFE method [6] and SPF algorithm in this paper for path planning, respectively, as shown in Figure 4. Figure 4(a) reveals the MEP found based on the HGA-NFE method in [6]. The Voronoi nodes of the

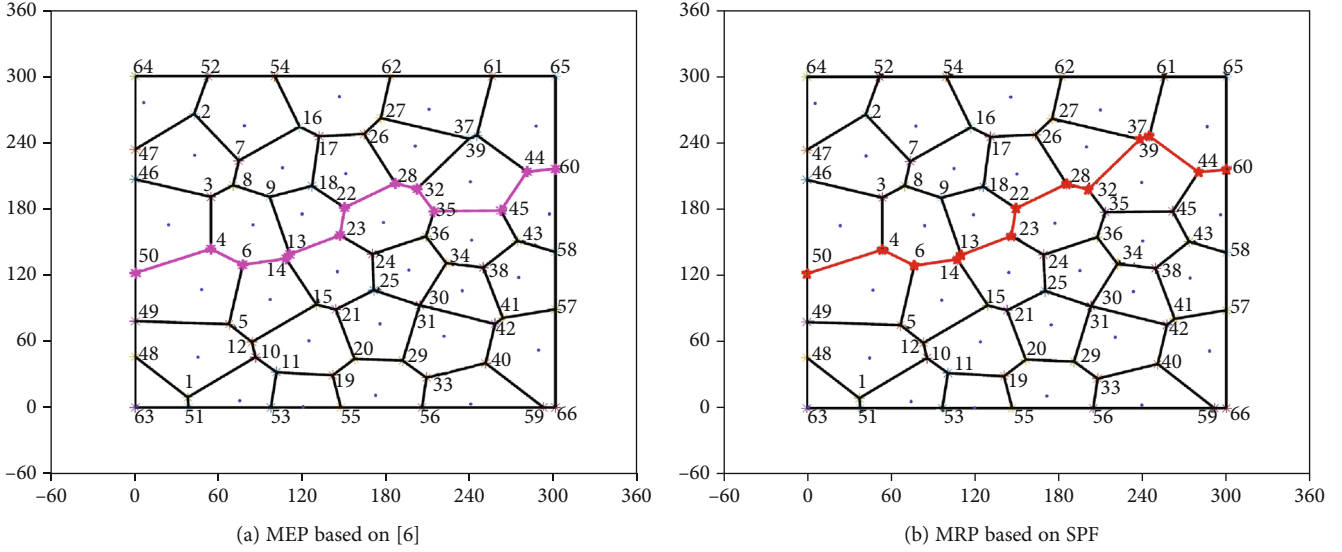


FIGURE 4: Minimum exposure path.

path passed are [50,4,6,14,13,23,22,28,32,35,45,44,60], and the exposure value of this path is 104.1807. Figure 4(b) displays the MRP found based on the SPF algorithm. The Voronoi nodes of the path passed are [50,4,6,14,13,23,22,28,32,37,39,44,60], and the exposure value of this path is 104.1459. The lengths of MRP and MEP are both 379.07, but MRP has a smaller exposure value than the MEP, which is computed by the HGA-NFE method. It indicates that the SPF algorithm is more accurate than the HGA-NFE method [6].

Network topologies can be divided into three different network types according to the deployment of sensors. They are the uniform distribution method, Gaussian distribution method, and exponential distribution method [17]. We limited the distance relationship between nodes in the experiment to achieve all kinds of distribution. For studying the efficiency of the SPF, topologies were randomly generated according to the three network types mentioned. The calculation time of SPF under different topologies is shown in Figure 5.

The total computation time of MRP falls into two parts. One is the time to construct the Voronoi diagram, and the other is the time to find the path. We can find that the total computation time of MRP increases as the number of nodes increases because the time complexity of constructing the Voronoi diagram is related to the number of nodes. The total computation time comparison of the SPF algorithm under the three topologies is shown in Figure 5(d). It is no doubt that the SPF algorithm is more efficient under the topology of uniform distribution.

Binh et al. [17] proposed the GA-MEP algorithm for intrusion path planning. It is difficult to compare the time complexity of the SPF algorithm with the genetic algorithm GA-MEP [17] because the complexity of GA-MEP is not related to the number of sensor nodes. Hence, to test the efficiency of SPF, the calculation time of SPF and GA-MEP was compared. Figure 6 displays the results.

The computing time of the SPF algorithm grows slowly with the increase of sensor nodes in this area, which is better than the GA-MEP algorithm. It indicates that the SPF algorithm is more suitable for the condition of a large number of sensors. The calculation time of SPF is shorter than that of GA-MEP, and the SPF algorithm is more stable for different network topologies. In the case of the same intrusion path exposure, the efficiency of the algorithm proposed in this paper is far better than the GA-MEP algorithm [17].

To explore path-finding law limited by various constraints, experiments have been done on the uniform distribution network topology where $n = 20$ and $n = 40$, respectively. The selected parameters are put in Table 4. The results are shown in Figure 7. To explore path-finding law limited by various constraints, experiments have been done on the uniform distribution network topology where $n = 20$ and $n = 40$, respectively.

Figure 7 illustrates three simulation scenarios. The first one is only considering the impact of exposure on the path (as explicated in Figures 7(a) and 7(d)), which is transformed into find the minimum exposure path. The second solely thinks about the impact of the moving target energy consumption on the path (as shown in Figures 7(b) and 7(e)). Thus, it is equivalent to solving the minimal path problem. Thirdly, we consider both the exposure and energy consumption of the moving target (as revealed in Figures 7(c) and 7(f)).

We calculated the path exposure value and path length under three simulation conditions. The experimental results in Table 5 show that when only considering the effect of exposure on the path, the total exposure value of the path is the lowest. However, the length of path is the longest, which means that the invader has the highest energy consumption. When only considering the effect of energy consumption on the path, the length is the lowest, which means energy consumption is the lowest. However, the exposure degree increases accordingly. When considering both exposure and

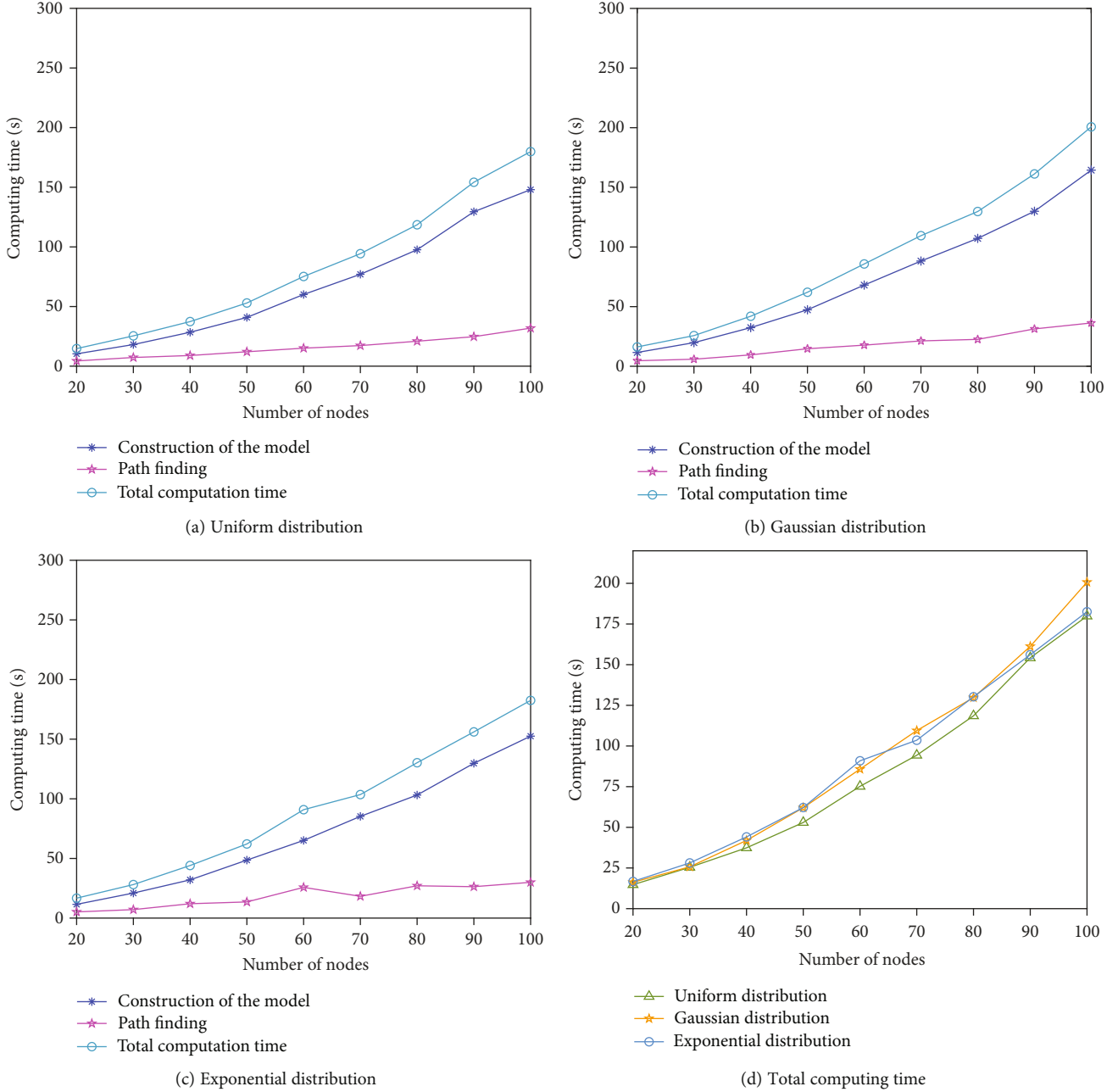


FIGURE 5: Computing time of MRP in 3 topologies.

energy consumption, the relevant parameters of the path in the data model generated by federated learning are between the above two results. It conforms to the hypothesis, proving that the SPF algorithm proposed can calculate the path according to different requirements.

The quality of MRP relates to the path's exposure, and it was affected by the amount of sum and various parts composed. Thus, we compared the maximum exposure value of parts E_{\max} of the path, and the results can be found in Table 6.

It can be seen in the column that the maximum exposure value of part of MRP obtained by the SPF algorithm is the same as that of MEP. But it takes less time and energy when

an invader moves along MRP. To test the universality of this circumstance, we also calculated MRP with different node numbers. Relevant experimental data is in Table 7.

According to Tables 6 and 7, we can get a conclusion. When calculating MRP by SPF algorithm, there is a 42.86% probability of getting a path with the same maximum exposure value of MEP but shorter travel time and less energy consumption. The simulation test was carried out under the parameter settings displayed in Table 4.

Figure 8 describes the relationship between MRP exposure (travel time) and the number of sensor nodes with different q values. With the augmentation of sensor nodes,

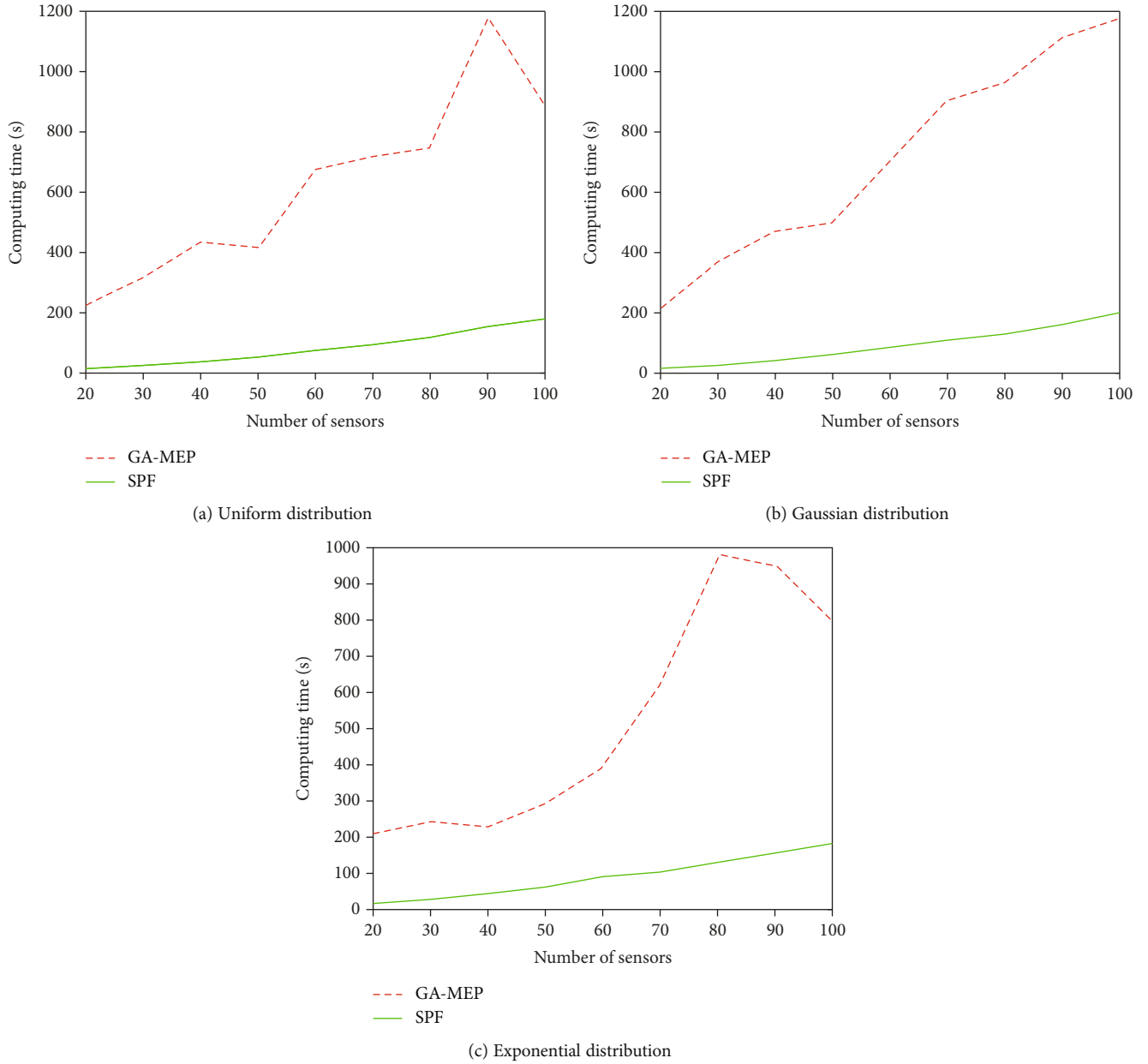


FIGURE 6: Comparison between SPF and GA-MEP.

TABLE 4: Experimental parameters (2).

Parameter	Value
Monitoring area	300 * 300
λ	1
K	2
q	0,50
k	2
Number of sensor nodes	20,40
Starting point	(0,300)
Ending point	(300,0)

the exposure degree keeps an upward trend and the intrusion time has a specific change.

In the identical topologies, we can adjust the model created by federated learning to get the path (MRP) with less exposure and shorter intrusion time. It is conducive to save the energy consumption and reduce the probability of being detected by the sensor nodes.

4.2. Multi Mobile Devices. In terms of multi-objective, a simulation was made for the verification of MFF performance. The value k represents the change of the edge when two moving targets are on the same edge. In the tangible situation, k can be adjusted according to different requirements for obtaining different path combinations.

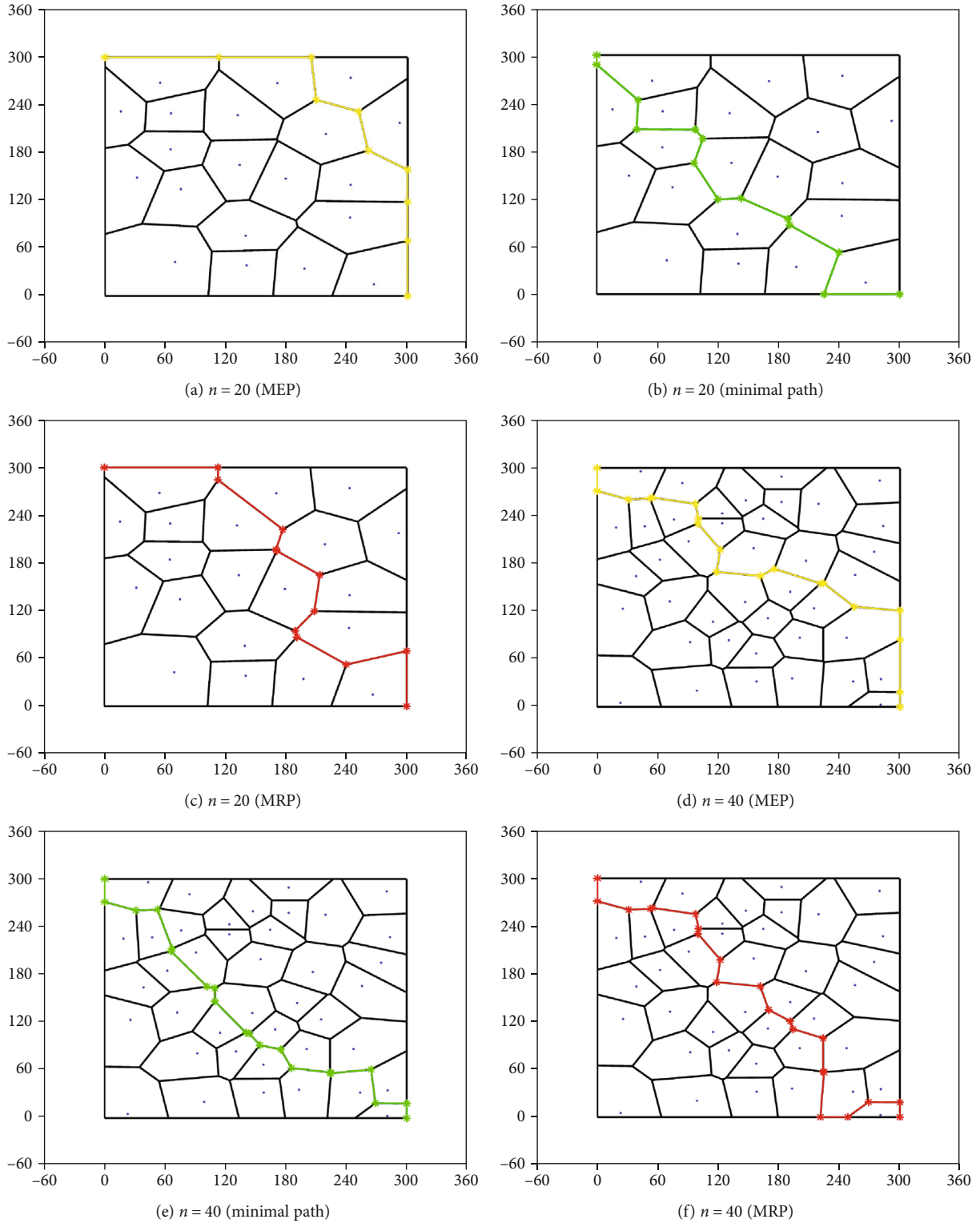


FIGURE 7: Different paths when $n = 20$ and $n = 40$.

Assume that there are four intruders with the same starting point $(0,300)$ and the same ending point $(300,0)$. Each moving target sets off every 0.6 seconds and $k=2$. The results are shown in Figure 9, which show the four paths found when 40 nodes distributed evenly in F . The

four intruders took a total of 12.32 seconds to travel from starting point to the ending point, with a total exposure degree of 678.58. And the exposure of each path is 162.13, 176.27, 162.13, and 178.05. It can be found that the trajectory of the third target moving coincides with

TABLE 5: Experimental results.

	Exposure	Length of path
$n = 20$ (MEP)	91.42	557.31
$n = 20$ (minimal path)	156.70	536.49
$n = 20$ (MRP)	94.72	551.91
$n = 40$ (MEP)	183.93	616.32
$n = 40$ (minimal path)	244.53	498.75
$n = 40$ (MRP)	200.96	535.20

TABLE 6: Experimental results.

	E_{\max} (exposure)	Length of path
$n = 20$	19.90	21.62
$n = 40$	36.93	36.93

TABLE 7: Exposure and length of path.

	E_{\max} (exposure)	E_{\max} (both)	l (exposure)	l (both)
$n = 60$	37.56	37.56	505.6	500.55
$n = 80$	31.07	43.10	524.55	510.60
$n = 100$	45.08	45.08	534.84	523.86
$n = 120$	43.27	47.76	563.91	539.76

the first as time going by. The result is identical when n equals 60.

What can be explained is that the first moving target starts first and moves farther during the same period without affecting the path planning of subsequent moving targets. Therefore, when $k = 2$, the first moving target trajectory is likely to be the same as the trajectory of the third moving target.

The experiment is carried out in this section when $n = 40$ so as to study the influence of departure time interval of moving targets on multiobjective path planning. Each intruder sets off at a time interval of 0.4, 0.6, 0.8, and 1.0, and the relevant experimental data are shown in Table 8. The maximum and minimum intrusion time of a single target is Time(max) and Time(min), the maximum exposure of a single target is Exp(max), and the minimum exposure of a target is Exp(min).

It can be seen from Table 8 that with the increase of the time interval of sending moving target, the total travel time increases continuously. But the total exposure decreases continuously until a minimum value and then increases accordingly. This is because the longer a target stays in the WSN region, the greater the risk probability detected by the sensor. When the time interval reaches a certain peak, cross-path interference factors are excluded, and the greater the total exposure. The minimum exposure and time consumption of a single target do not change with a time interval because the MRP of a single target is the path obtained by the SPF algorithm.

5. Performance Evaluation

Well-defined evaluation criteria and adversary models put the pathfinding schemes on common WSN topology, making it possible to assess the scenarios fairly and comprehensively [30–32]. The adversary model in this paper refers to different types of WSN topologies. Sensor nodes can detect moving targets but will not attack them. Invaders require finding one or more paths through the sensor area. Security, availability, efficiency, and deployability are important evaluation indexes for intrusion detection systems [33–36]. Similarly, we select some evaluation properties [34, 35] as the evaluation indexes of the intrusion path planning algorithm.

(A) Security

- (i) *S1 Exposure*. For an intruder, its security is reflected in the exposure of the invasion path mostly. Lower exposure means a safer moving target.
- (ii) *S2 Energy Consumption*. An ideal invasion path for an intruder requires low exposure and minimal energy consumption as the intruder moves along the trail. Otherwise, the moving target is likely to run out of energy on the way so that it cannot fulfill the task.

(B) Availability

- (i) *A1*. It can be used in WSN with a Boolean disk perception model.
- (ii) *A2*. It can be used in WSN, whose perception model is the probabilistic perception model.
- (iii) *A3*. It can be used in WSN with an attenuated disk perception model.

(C) Deployability

- (i) *D1*. Whether it is suitable for large-scale networks. In actual application scenarios, the scale of WSN is often large, so if we want to expand the application algorithm, it is imperative to apply it to large-scale networks.
- (ii) *D2*. Whether it considered multiple moving targets. The “moving target” is not only a single target. When the intrusion of a single target expands to multiple target intrusion, whether the algorithm is still effective also needs to be included in the evaluation.
- (iii) *D3*. Whether multiple sensor network topologies are considered.
- (iv) *D4*. Algorithmic efficiency, which is mainly compared from the time complexity and running time. It is divided into two levels, “excellent” and “good.”
- (v) According to the above criteria, we evaluate the algorithm proposed in this paper and the existing methods. The results are summarized in Table 9.

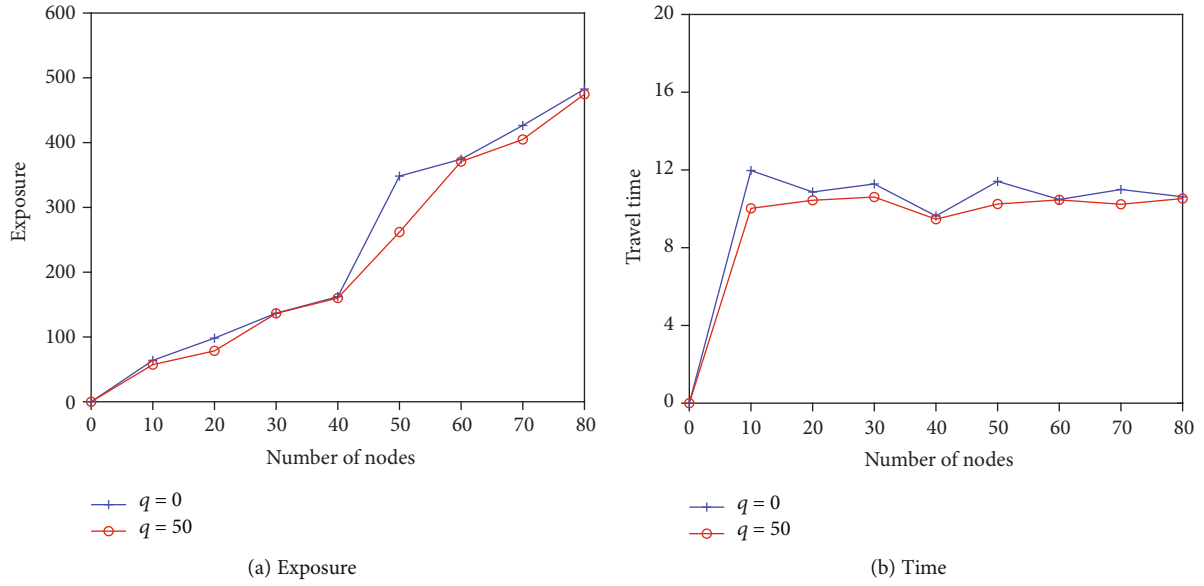


FIGURE 8: Exposure and travel time of different sensor nodes.

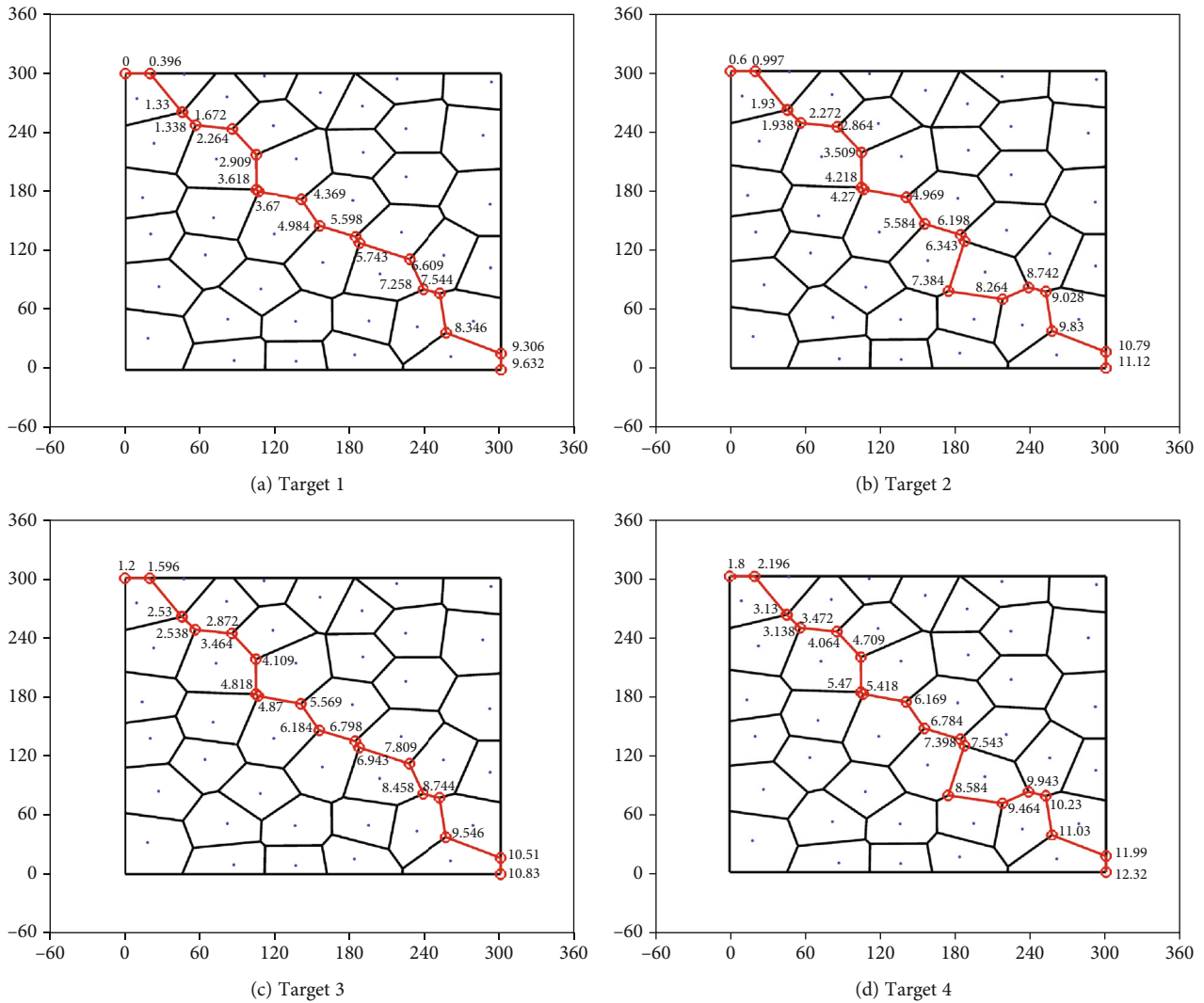


FIGURE 9: Paths for four intruders when $n = 40$ and $T = 0.6$.

TABLE 8: Exposure and length of path.

	$T = 0.4$	$T = 0.6$	$T = 0.8$	$T = 1.0$
Travel time	11.85	12.32	13.38	13.56
Total exposure	727.35	716.35	677.08	815.96
Time(max)	11.04	11.1	11.01	11.13
Time(min)	10.14	10.17	10.17	10.17
Exp(max)	206.26	232.68	214.01	217.18
Exp(min)	127.01	127.01	122.01	189.54

TABLE 9: Measuring security, availability, and deployability of algorithm.

Scheme	No.	No.	Security		Availability				Deployability		
			S1	S2	A1	A2	A3	D1	D2	D3	D4
Meguerdichian et al.	2001	[8]	✓	✗	○	○	✓	✗	✗	✗	☆
Song et al.	2014	[37]	✓	✗	○	○	✓	✗	✗	✓	☆
Ye et al.	2016	[6]	✓	✗	○	✓	○	✓	✗	✗	☆
Binh et al.	2019	[17]	✓	✗	○	✓	○	✓	✗	✓	★
Aravinth et al.	2021	[18]	✓	✓	✓	○	○	✓	✗	✗	★
Our scheme			✓	✓	○	○	✓	✓	✓	✓	★

Note: ✓ means achieving the corresponding goal, while ✗ not. ○ does not mean anything. ☆ means “good,” and ★ means “excellent.”

6. Conclusions

This paper built a data model of the dynamic-planning algorithm to keep the risk of multi-intrusion targets minimized, which utilizes computational geometry methods amalgamated with federated learning features. The experiment results show that the algorithm that introduced time variables can actualize the global optimization. By contrast with traditional planning ways, its computational performance prevails in complexity and time. $H(x)$ weights by $C(t_i, t_j)$ can be adjusted to meet various demands of path selection.

The MRP exposure of all the discrete paths distinctly declined in comparison with MEP. MRP can markedly lower the energy consumption without being detected by the sensor nodes as much as possible. Consequently, the algorithm accurately satisfies the real-life conditions, such as the battlefield crossing scenarios. The model has an inspired significance to the sensor network deployment.

The common application of multiple types of sensors in WSN becomes increasingly popular, which increases the path analysis complexity. Hence, it is necessary to analyze more actual models of WSN deployment to explore further. Besides, fulfilling federated learning in three-dimensional space to make path planning is a new direction.

Data Availability

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

Conflicts of Interest

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

Acknowledgments

This work was supported by the National Natural Science Foundation of Heilongjiang Province of China (JJ2019YX0922) and Basic Science Research Plan (JCKY2020208B045). We thank laboratory team members for assistance with the experiments.

References

- [1] J. Pan, F. Fan, S. Chu, Z. du, and H. Zhao, “A node location method in wireless sensor networks based on a hybrid optimization algorithm,” *Wireless Communications and Mobile Computing*, vol. 2020, 14 pages, 2020.
- [2] W. Fang, W. Zhang, W. Chen, T. Pan, Y. Ni, and Y. Yang, “Trust-based attack and defense in wireless sensor networks: a survey,” *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 2643546, 20 pages, 2020.
- [3] H. Mostafaei, M. U. Chowdhury, and M. S. Obaidat, “Border surveillance with WSN systems in a distributed manner,” *IEEE Systems Journal*, vol. 12, no. 4, pp. 3703–3712, 2018.
- [4] 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.
- [5] C. Ryan, F. Murphy, and M. Mullins, “Spatial risk modelling of behavioural hotspots: risk-aware path planning for autonomous vehicles,” *Transportation Research Part A: Policy and Practice*, vol. 134, pp. 152–163, 2020.
- [6] M. Ye, Y. Wang, C. Dai, and X. Wang, “A hybrid genetic algorithm for the minimum exposure path problem of wireless sensor networks based on a numerical functional extreme model,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 8644–8657, 2015.
- [7] L. Liu, X. Zhang, and H. Ma, “Minimal exposure path algorithms for directional sensor networks,” *Wireless Communications and Mobile Computing*, vol. 14, no. 10, p. 994, 2014.

- [8] S. Meguerdichian, F. Koushanfar, G. Qu, and M. Potkonjak, "Exposure in wireless ad-hoc sensor networks," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, pp. 139–150, Rome, Italy, 2001.
- [9] S. Chechik, M. Johnson, M. Parter, and D. Peleg, "Secluded connectivity problems," *Algorithmica*, vol. 79, no. 3, pp. 708–741, 2017.
- [10] T. Chang, D. Kong, N. Hao, K. Xu, and G. Yang, "Solving the dynamic weapon target assignment problem by an improved artificial bee colony algorithm with heuristic factor initialization," *Applied Soft Computing*, vol. 70, pp. 845–863, 2018.
- [11] P. Yu and Y. Liu, "Federated object detection: optimizing object detection model with federated learning," in *ACM International Conference Proceeding Series*, pp. 1–6, Vancouver BC, Canada, August 2019.
- [12] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: concept and applications," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, pp. 1–19, 2019.
- [13] H. Zhu and Y. Jin, "Multi-objective evolutionary federated learning," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 4, pp. 1310–1322, 2020.
- [14] A. H. Sodhro, S. Pirbhulal, and V. H. C. De Albuquerque, "Artificial intelligence-driven mechanism for edge computing-based industrial applications," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4235–4243, 2019.
- [15] J. Chen, J. Li, and T. H. Lai, "Trapping mobile targets in wireless sensor networks: an energy-efficient perspective," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 7, pp. 3287–3300, 2013.
- [16] N. Rai and R. Daruwala, "Node density optimisation using composite probabilistic sensing model in wireless sensor networks," *IET Wireless Sensor Systems*, vol. 9, no. 4, pp. 181–190, 2019.
- [17] H. T. T. Binh, N. T. M. Binh, N. H. Ngoc, D. T. H. Ly, and N. D. Nghia, "Efficient approximation approaches to minimal exposure path problem in probabilistic coverage model for wireless sensor networks," *Applied Soft Computing*, vol. 76, pp. 726–743, 2019.
- [18] S. S. Aravinth, J. Senthilkumar, V. Mohanraj, and Y. Suresh, "A hybrid swarm intelligence based optimization approach for solving minimum exposure problem in wireless sensor networks," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 3, article e5370, 2021.
- [19] Y. J. Liu, D. Fan, C. X. Xu, and Y. He, "Constructing intrinsic Delaunay triangulations from the dual of geodesic Voronoi diagrams," *ACM Transactions on Graphics*, vol. 36, no. 4, pp. 1–15, 2017.
- [20] F. Engmann, F. A. Katsriku, J. D. Abdulai, and K. S. Adu-Manu, "Reducing the energy budget in WSN using time series models," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 8893064, 15 pages, 2020.
- [21] G. Xu, H. Li, S. Liu, K. Yang, and X. Lin, "VerifyNet: secure and verifiable federated learning," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 911–926, 2019.
- [22] M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, "Efficient and privacy-enhanced federated learning for industrial artificial intelligence," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6532–6542, 2020.
- [23] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, 2019.
- [24] S. Rani, S. H. Ahmed, R. Talwar, and J. Malhotra, "Can sensors collect big data? An energy-efficient big data gathering algorithm for a WSN," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 4, pp. 1961–1968, 2017.
- [25] Q. Yang, Y. Liu, Y. Cheng, Y. Kang, T. Chen, and H. Yu, "Federated learning," *Synthesis Lectures on Artificial Intelligence and Machine Learning*, vol. 13, no. 3, pp. 1–207, 2019.
- [26] A. Driemel, S. Har-Peled, and B. Raichel, "On the expected complexity of Voronoi diagrams on terrains," *ACM Transactions on Algorithms*, vol. 12, no. 3, pp. 1–20, 2016.
- [27] A. Hilmani, A. Maizate, and L. Hassouni, "Automated real-time intelligent traffic control system for smart cities using wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 8841893, 28 pages, 2020.
- [28] J. Liu, Z. Wang, M. Zuba, Z. Peng, J.-H. Cui, and S. Zhou, "DAsync: a Doppler-assisted time-synchronization scheme for mobile underwater sensor networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 3, pp. 582–595, 2013.
- [29] T. Ojha, S. Misra, and S. Obaidat, "SEAL: self-adaptive AUV-based localization for sparsely deployed underwater sensor networks," *Computer Communications*, vol. 154, no. 1, pp. 204–215, 2020.
- [30] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K. K. R. Choo, "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9390–9401, 2020.
- [31] D. Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 708–722, 2016.
- [32] C. Wang, D. Wang, G. Xu, and D. He, "Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0," *Science China Information Sciences*, 2020.
- [33] S. Huang and K. Lei, "IGAN-IDS: an imbalanced generative adversarial network towards intrusion detection system in ad-hoc networks," *Ad Hoc Networks*, vol. 105, article 102177, 2020.
- [34] J. Bonneau, C. Herley, P. Oorschot, and F. Stajano, "The quest to replace passwords: a framework for comparative evaluation of web authentication schemes," in *2012 IEEE Symposium on Security and Privacy*, pp. 553–567, San Francisco, CA, USA, May 2012.
- [35] D. Wang, W. Li, and P. Wang, "Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4081–4092, 2018.
- [36] M. Eskandari, Z. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: an intelligent anomaly-based intrusion detection system for IoT edge devices," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6882–6897, 2020.
- [37] Y. Song, L. Liu, H. Ma, and A. Vasilakos, "A biology-based algorithm to minimal exposure problem of wireless sensor networks," *IEEE Transactions on Network and Service Management*, vol. 11, no. 3, pp. 417–430, 2014.

Research Article

Fast Policy Interpretation and Dynamic Conflict Resolution for Blockchain-Based IoT System

Yaozheng Fang , Zhaolong Jian , Zongming Jin , Xueshuo Xie , Ye Lu , and Tao Li 

College of Computer Science, Nankai University, China

Correspondence should be addressed to Xueshuo Xie; xueshuoxie@mail.nankai.edu.cn

Received 9 March 2021; Revised 29 April 2021; Accepted 28 June 2021; Published 9 July 2021

Academic Editor: Chi-Hua Chen

Copyright © 2021 Yaozheng Fang 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.

Although the blockchain-based Internet of Things (BC-IoT) has been applied in many fields, it still faces many security attacks due to lacking policy-based security management (PbSM). Previous PbSM is usually time-consuming, which is difficult to integrate into BC-IoT directly. The high-latency policy conflict resolving in traditional PbSM cannot meet the BC-IoT's low-latency requirement. Moreover, the conflict resolution rate is low as the PbSM usually neglects the runtime information. Therefore, it is challenging that achieving an efficient PbSM for BC-IoT and overcomes both time and resource consumption. To address the problem, we propose a novel PbSM for BC-IoT named FPICR to realize fast policy interpretation and dynamic conflict resolution efficiently. We first present policy templates based on system log to interpret policy in high speed in BC-IoT. Benefiting from matching the characteristics of the system processing, FPICR supports interpreting a policy into the smart contract directly without complex content parsing. We then propose a weighted directed policy graph (WDPG) to evaluate the importance of the deployed policies more accurately. To improve the policy conflict resolution rate, we implement the resolution algorithm through reconstructing the WDPG. Taking the traits of these properties, FPICR thus can also remove the redundant data to compress storage space by the WDPG. Experiment results highlight that FPICR outperforms the baseline in all measure metrics. Especially, compared with the state-of-the-art method, the speedup of interpretation in FPICR is about up to $2.1 \times$. The conflict resolution rate in FPICR can be improved by 6.2% on average and achieve up to 96.1%.

1. Introduction

Internet of Things (IoT) has been widely used in many fields such as smart cities [1], industrial control [2, 3], online gaming [4], and distributed computing system [5, 6]. However, massive IoT devices and networks face various real threats [7], in consequence, the security of IoT is becoming more and more important. Blockchain has many advantages such as decentralization, trustworthiness, anonymity, and immutability. Owing to these merits, blockchain has become a major solution to a lot of domains, such as supply chain, healthcare, and transportation [8]. The success stories in these domains inspire researchers in IoT to apply blockchain by using smart contract to address the problems of single-point failure and data security in IoT system. Therefore, blockchain-based IoT system (BC-IoT) has been a research hotspot [9, 10], and a proposal called smart contract-based

access control [11] falls into this category and already demonstrates the benefits of adopting blockchain for IoT system.

Although the new features of BC-IoT can help protect against the security risks to a certain extent, BC-IoT still faces some real attacks such as DDoS, on-off attack, and Parity Wallet attack [12–15], due to lacking policy-based security management (or short, PbSM). In fact, the attacks can be defended by deploying security policies in policy-based security management (PbSM). Unfortunately, traditional PbSM methods are so time-consuming and resource-intensive. These shortcomings make it difficult to integrate these PbSM methods into the BC-IoT system directly and freely. For example, traditional PbSM methods resolve policy conflict through comparing static priorities, the time-consuming process thus cannot meet the requirements of low latency in the BC-IoT system. And neglecting run-time information in the traditional PbSM methods leads to the rate of policy

conflict resolution degradation. Besides, the policies in PbSM also bring high storage cost, which is not a reasonable choice for the resource-constrained devices in BC-IoT. Therefore, traditional PbSM methods are inefficient for BC-IoT.

It is challenging to achieve an effective and efficient PbSM in the BC-IoT system. First, it is difficult to make full use of policy language expression to interpret policy quickly and accurately, according to the characteristic of smart contract. It should be noted that reducing interpretation latency by removing complex analysis should meanwhile ensure the accuracy of interpretation. Second, it is troublesome to find out the crucial information from larger-scale storage in BC-IoT system than other common systems. Because each node in BC-IoT executes the smart contract when it is invoked and generates additional data, it is hard for PbSM to take advantage of such system runtime information to resolve policy conflict dynamically. Third, it is also difficult to identify which is the redundant part in the policy storage space, since the dependencies on each other among various smart contracts are so complex, and removing the redundancy should not negatively impact on the conflict resolution algorithm. To meet the abovementioned challenges, in this paper, we propose a novel PbSM method named FPICR, which focuses on realizing fast policy interpretation and high conflict resolution rate with lower storage cost in the BC-IoT system. First, we present a new policy interpretation method through utilizing system logs to describe system states. This interpretation meshes with the running characteristics of smart contract, policies thus in FPICR can be interpreted in a short time. Second, we propose a dynamic policy conflict resolution algorithm to improve resolution rate, which can exploit runtime state information such as policy weight, to provide more accurate decisions rather than the presetting. Third, we design a weighted directed graph structure that can help determine the importance of the dependency between each policy and facilitate to remove the redundancy conveniently. Our innovations and major contributions in FPICR are highlighted as follows:

- (i) We present a novel policy interpretation method based on system log. This method can interpret a policy into a smart contract through simple notation parsing rather than complex semantic and lexical analysis. The speedup of the log-based interpretation achieving is about up to $2.1\times$ compared with XACML-based interpretation
- (ii) We propose a weighted decision algorithm to resolve policy conflict by utilizing the policy execution times and other important information of system runtime. Such an algorithm can evaluate the importance of the security policies in fine-grained. This algorithm facilitates FPICR to increase the rate of conflict resolution up to 96.1%, which is higher than the traditional method by 6.2%
- (iii) We design a weighted directed policy graph to store the dependencies among security policies. This policy graph can remove the redundant parts to reduce the ledger size in BC-IoT. Compared with the tradi-

tional method, the degradation of storage can be achieved by about 17%

2. Background and Motivation

In this section, we introduce the minimal background about policy-based security management (PbSM) in BC-IoT, followed by the discussion on the related work. Lastly, we conclude the challenges of achieving effective and efficient PbSM in BC-IoT.

2.1. Traditional PbSM. Traditional PbSM methods are inefficient for BC-IoT. In particular, the reasons in detail are as follows. They usually consist of four parts, policy administration point (PAP), policy decision point (PDP), policy information point (PIP), and policy enforcement point (PEP). PAP is responsible to describe policies by various high-level policy languages. Therefore, in order to make sense in the BC-IoT system, a policy should be first interpreted from high-level policy language to the codes by following the rules of smart contract. This process often suffers from high latency due to complex syntax and lexical analysis. Massive policies may cause policy conflict, and PDP provides the algorithms to solve policy conflicts. PIP can also help tune policy by retrieving system runtime-related information. However, the resolution results of existing algorithms in PbSM do not always work, since most of these algorithms utilize the limited static priority and policy comparison, they cannot make full use of the rich information of system runtime to address the conflicts dynamically. Once there are lots of conflicts to be resolved, they have to be handled manually. Consequently, traditional PbSM methods are so time-consuming and heavy labor works. Furthermore, because PIP stores the whole security policies which can generate lots of redundant smart contracts on blockchain, traditional PbSM will bring high storage cost if be integrated into the BC-IoT system directly. This heavy burden on storage will limit the ability of BC-IoT devices greatly. PEP is responsible for the execution and enforcement of policies. The first three time-consuming and resource-intensive parts in traditional PbSM also leads to the low efficiency of PEP, since PEP has to wait for the results of the preprocessing.

2.2. Related Work. FPICR is closely related to three aspects: policy interpretation, conflict resolution, and the smart contract as explained as follows.

The typical policy interpretation focuses on two main scenarios: network management and security management according to the application field's requirements [16]. Varadharajan et al. [17] propose a policy expression language based on the routing syntax, in order to realize the network packages routing. Lara and Ramamurthy propose an understandable language in OpenSec [18] which could realize the automatic reaction to the network events. Moreover, an expressive language is presented by Gember et al. in [19] to control data traffic flow, so as to protect the privacy information of devices. In the papers [20], a standard firewall rule is given to create a blacklist. Furthermore, in the paper [21], the

authors describe the security policy relying on the BNF notation. Besides, the access control rule languages are mostly based on the XACML [20], P3P [22], and so on. However, these methods for policy interpretation usually utilize a time-consuming two-step process to realize interpreting policies from the high-level expression to the executable program.

Resolving policy conflict in traditional methods often take advantage of the most commonly used priority mechanism [23, 24], and this method is applied to deal with conflicts in many current architectures [25–29]. However, rationally assign priority to each policy is almost impossible. It is even challenging for a well-trained administrator in this field. There are also other methods for conflict resolution, such as several rules combining algorithms to support conflict resolution strategies in [30], the conflict matrix in [31], the policy conflict analysis for QoS in [32], and the context-aware conflict resolution in [33]. Moreover, there are several conflict resolution strategies provided in XACML (i.e., permit-overrides and deny-unless-permit). Nevertheless, differing from FPICR, these works cannot make use of system running information to resolve the conflicts dynamically.

Defending attacks in blockchain system by smart contracts is an effective method [34]. Zhang et al. [11] propose a smart contract-based framework to implement distributed access control, but they neglect using the possible dependencies between policies. To manage the endpoint devices in IoT system, Novo [35] presents a decentralized security management technique, which can utilize devices by defining operations in smart contracts. Besides, Alphand et al. [36] design IoT chain as the security management architecture, which allows the access token to be stored in the smart contract to ensure data correctness. In order to protect private data, Kosba et al. [37] provide a framework for building public and private smart contracts. They focus on the smart contract-based access control implementation, but lead to undesirable results due to lacking policy enforcement, especially conflict resolution.

2.3. Challenges and Goals. The PbSM needs to be more effective and efficient to meet the requirements of real applications. Improving the performance of PbSM can be realized through fast interpretation and resolving policy conflicts efficiently. We identify three fundamental challenges and our goals as follows.

First, it is difficult to realize fast policy interpretation without missing the accuracy of interpretation results. Policy interpretation needs complex and time-consuming analysis, removing the analysis may miss important information. Besides, policy interpretation in BC-IoT should consider the characteristics of smart contract (e.g., GAS).

Second, resolving policy conflicts according to system runtime information is nearly impossible in BC-IoT as discovering the crucial information from large-scale data in BC-IoT is challenging. BC-IoT has larger-scale data than the traditional systems because BC-IoT generates additional data related to blockchain and smart contract (e.g., blocks and encryption information). As a result, resolving policy

conflicts dynamically is harder than the traditional PbSM systems.

Third, security policies have complex dependencies, which is important to the resolution of policy conflicts. It needs a larger storage space to store the dependency information, so the policy storage space in BC-IoT has many redundant parts. It is difficult to remove the redundant parts and the policy dependencies without negatively impacting on the resolution of policy conflicts.

3. System Overview

FPICR is designed to achieve fast interpretation and dynamic policy conflict resolution for general BC-IoT. FPICR consists of two key components (see Figure 1), log-based policy interpretation and policy graph reconstruction. The overall process in Figure 1 is as follows. When the BC-IoT system requires adding or updating policies to protect against attacks, FPICR first performs the policy conflict detection and resolution module to determine whether this new policy can be deployed on the system or not. A policy that can be deployed will be interpreted into a policy smart contract (or short, PSC) by a certain log-based template. The templates are obtained through analyzing the relationship between items among the system logs. Once the policy has been deployed, it will be inserted into the weighted directed graph to record the corresponding dependencies on each other policies. This policy graph then can be reconstructed and updated to generate a new policy graph contract (PGC). A PGC is responsible for saving the property data of PSC and provides parameters such as weight, the number of access, or other information that the conflict resolution algorithm desires to utilize.

4. Fast Interpretation

In this section, we introduce how to realize fast interpretation with system logs and templates in our FPICR. We first design the template structures by summarizing and simplifying the policy description which is based on the system logs. We then interpret the policy into the smart contract by the converting process relying on module matching. These processes are lower latency and less resource-consuming.

4.1. System Log. System log can reflect the system state and record various special events [38], so there are many important data that can be used in fine-grained for preventing security threats. Moreover, in general, there are also lots of regular formal logic in the system logs. Specifically, there are various kinds of modes, and we select the three typical modes in the system log to help us explain the details as follows:

Single implies that to define a threat can only use one entry of the log. For example, rebooting a device can generate a record in log, such as system status: locked, which represents the system is deadlocked currently.

4.1.1. Iteration. The iteration stream is a workflow of a certain process, thus, the iteration can also be used as the basis for judging whether the system has appeared exceptions or not.

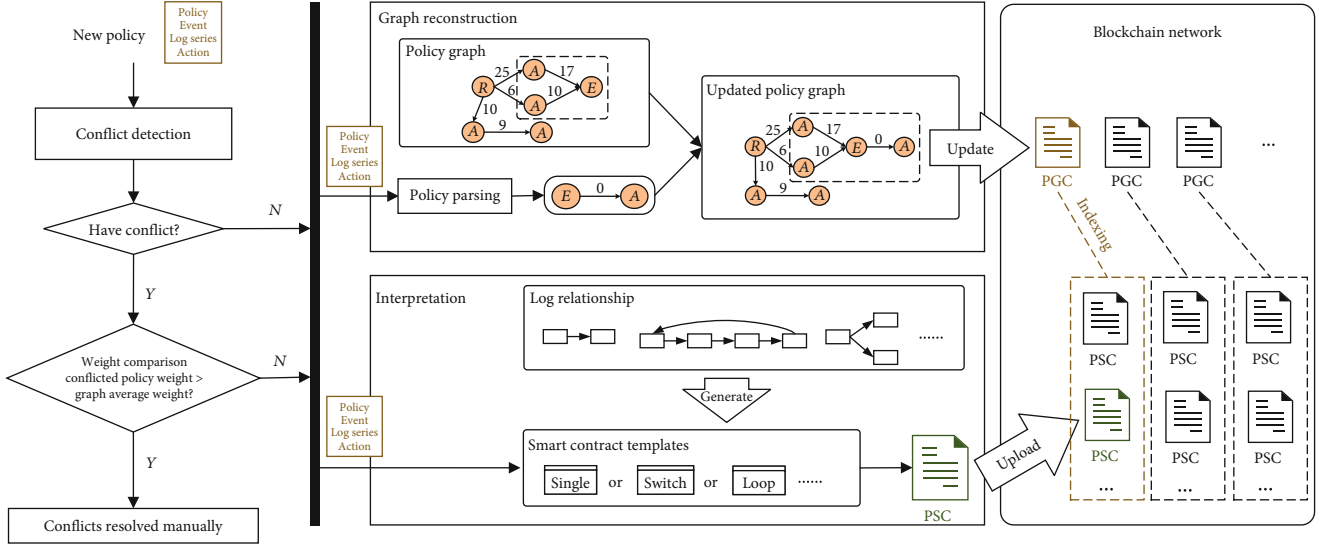


FIGURE 1: The FPICR architecture.

4.1.2. Loop. Loop refers to log entries repeating according to a certain regulation. When a loop appears in system log, the system may suffer from attacking or exceptions. For instance, a large repeat state of TCP retransmission means flooding attack happened. Based on the above explanations, in consequence, these observations facilitate us to skillfully combine the characteristic between system log and smart contract to speed up the interpretation.

4.2. Policy Template. In FPICR, an innovation is that we design templates based on system logs to describe various policies accurately. The policy template consists of four fields, MODE, CONDITION, ACTION, and CONF, respectively. Policy template has referenced the ECA (event-condition-action) paradigm [39]. A common template can be defined as follows:

$$LbP := [\text{MODE}][\mathcal{T}, N][\$SRC, \text{ACT}][\text{CONF}]. \quad (1)$$

MODE refers to the type of relationships among the log entries. There are several alternative options such as single, iteration, and loop. T represents specific entries of the system log. N is denoted as the times that T appears. SRC represents the resource in the specific entries. ACT is the action on the corresponding resource SRC. CONF specifies some actions which are conflicted with the expecting action described in the field ACT. Hence, CONF is the basis for conflict detection. We give an instance to explain how the policy template works. A policy, such as when the number of TCP retransmission from the same host greater than 10, blocking this host, can be denoted as follows:

$$LbP_{eg} := [\text{LOOP}][\$SRC \text{TCP_Trans}', 10], \\ [\$SRC, \text{'BLOCKING'}][\text{'OPEN'}]. \quad (2)$$

Moreover, FPICR supports complex policies owing to

enabling the fields in the template to be nested. Because of meshing with the characteristics of smart contract, the interpretation based on policy template can be program-friendly, machine-readable, and time-saving.

We have summarized some common security threats and attacks in Table 1, and we can observe that the designed log-based templates have strong policy descriptive capacity.

4.3. Converting into Smart Contract. Policy interpretation in FPICR refers to convert the log-based policy into an executable smart contract that is PSC. As shown in Figure 2, a PSC is usually composed of three parts as follows:

- (i) Metadata is implemented as an extensible structure that can record some important property information of the policy. For instance, metadata may include the policy mode, the unique identification number, the timestamp, the policy generator, and the other parameters
- (ii) Interceptor is used for gathering and checking the system log. Interceptor also has several templates, which are corresponding with the policy template, to facilitate fast converting for the policy interpretation. Once the gathered information in the interceptor matches with the parameter in CONDITION field of the policy, the corresponding actions described in ACT of the policy will be triggered
- (iii) Actuator can activate specific actions when corresponding conditions fulfill the requirement. It should be noted that a common defense program usually only gives the abstract expressions rather than implementation for an action set. The reason is that devices in IoT system are actually vendor-dependent, thus, we have to call the hardware device APIs to instantiate an actuator

TABLE 1: Common BC-IoT security attacks and the countermeasures based on log-based policy.

Security threats	Mode	Condition	Action
Node capture attack	Single	$['\$num \text{ in Consecutive exception}', t]$	$['SELF', 'ISOLATION']$
Sleep deprivation	Single	$['\$dev \text{ TIME_SLEEP DEL}', 1]$	$['\$dev', 'REBOOT_TIME_SLEEP']$
Flooding attack	Loop	$['\$SRC \text{ TCP_Transmission}', 10]$	$['\$SRC', 'BLOCKING']$
Blackhole attack	Iteration	$['\$addr \text{ Data_recv, Data_recv}', 100]$	$['\$addr', 'BLOCKING']$
Malicious injection	Single	$['\$str \text{ inserted abnormally}', 1]$	$['\$str', 'DELETE']$
Homing attack	Loop	$['\$SRC \text{ ConnectReq}', 20]$	$['\$addr', 'BLOCKING']$
Eavesdropping	Iteration	$['\$Addr \text{ EaringChel}', 2]$	$['\$addr', 'SHUTDOWN']$
Password attack	Loop	$['\$Usr \text{ PwLogin}', 5]$	$['\$USR', 'NOLOGIN']$
Hardware bugs	Single	$['\$bugid \text{ occured in } \$usr']$	$['\$usr', 'EXIT']$

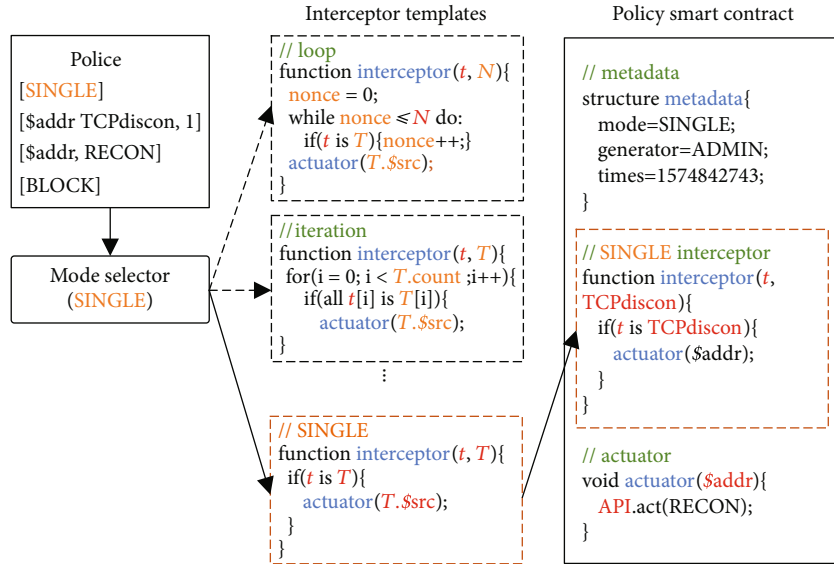


FIGURE 2: The policy interpretation based on template.

Mode selector in Figure 2 is used for choosing a desirable interceptor template in terms of the MODE parameters of the policy template. The other information in the policy will be filled into the selected template directly.

5. Conflict Resolution

To resolve policy conflict fast, we present weighted directed policy graph (WDPG) to organize deployed policies. WDPG is to store the dependencies between each policy and record the system runtime information. These dependencies and information can facilitate WDPG reconstruction to realize policy conflict resolution in FPICR.

5.1. Weight Directed Policy Graph. A WDPG consists of one or more policies. A policy in accordance with the ECA paradigm can be defined as follows:

$$\begin{cases} P = \langle V, E, \varphi \rangle, \\ V = \{v_{\text{event}}, v_{\text{action}}\}, \\ E = \{e_{\text{condition}}\}, \\ \varphi = \langle v_{\text{event}}, v_{\text{action}} \rangle. \end{cases} \quad (3)$$

P is a policy that consists of two vertexes and an edge. V represents the set of vertexes. E is the set of events. v_{event} and v_{action} represent an event and an action, respectively. $e_{\text{condition}}$ is the edge between the vertex v_{event} and the vertex v_{action} (see

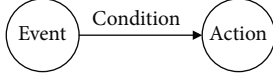


FIGURE 3: The security policy in policy graph.

Figure 3). φ represents to trigger an action execution when $e_{\text{condition}}$ meets requirement.

The weight of an edge in our WDPG can be defined in terms of the rich system runtime information. In other words, the meaning of the weight can be different in different applications, for example, the policy's priority, the execution time, the resource consumption, and so on. Because the execution frequency of action can reveal the importance of a policy, we denote weight by frequency in this paper. In system runtime, the frequency can be denoted as the called times of the corresponding smart contract which reflects the system state. Once a policy smart contract is involved, the relevant weight can be increased. The high frequency implies the policy contributes to a BC-IoT system relative greatly than other policies. Thus, WDPG can utilize the system runtime data to evaluate the importance of a policy as shown in Figure 4. The corresponding policies in the WDPG are listed in detail in the bottom of Figure 4. In the case, the policy $P1$ If NETFLOW is greater than 50, enable the firewall, with weight number 40, represents that this policy has been executed 40 times. As a result, the policy $P1$ is more important than the policy $P2$ which weight is 35. When the weight changes with the dynamic system runtime data, the importance of a policy to a BC-IoT system may be changed together. Therefore, WDPG is more dynamic and flexible than the other methods by presetting static priority for policies.

5.2. Graph Reconstruction and Updating. Policy conflict refers that there are inconsistent actions on the same resource. The conflicts are caused by multiple rules or rule instances. Policy conflict can make the state of system uncertain.

Because there are lots of dependencies between policies, it is challenging to process policy conflicts. In particular, adding or updating policy may generate redundant data, and deleting or deactivating a policy may cause the associated policies to be affected negatively. For such a difficult problem, we can address it through reconstructing WDPG, which is in charge of storing and updating the relationship between policies. In fact, the key process to solve policy conflicts is just reconstructing and updating the corresponding WDPG. We take an example to explain WDPG reconstruction flow (see Figure 5). We utilize an adjacent matrix as the storage structure of WDPG. We assume that when a new policy described by a pair of vertex and edge will be added into the existing WDPG, there is a conflict between policy A and F . A should be replaced by following certain requirement. Thus, we will delete A and add the new policy F into the WDPG. To do this, we first delete the row and column data related to A in the adjacent matrix which stores the previous WDPG.

Then, we delete C , the successor vertex of A . At last, we add F into the WDPG and update the weight value in the corresponding adjacent matrix.

An observation to evaluate the importance of a policy in WDPG is to calculate the in degree and the out degree of each vertex, respectively. A high out degree means a relative strong dependence. We can define the concept named impact factor (IF). It is a value reflecting the influence and importance of policy. IF can be obtained through calculating the sum of in and out degrees. Besides, we can utilize the average of all policy impact factor (or short, AvgIF) as a threshold to determine whether the new conflict policy can be updated directly or not.

Therefore, we propose a policy conflict resolution algorithm by comparing a policy IF with AvgIF (see Algorithm 1); this algorithm helps simplify the conflict processing. For example, while a conflicted policy's IF is smaller than AvgIF, the policy will be replaced by the new one due to being not important enough for the whole BC-IoT.

Algorithm 1: Policy conflict resolution. **Input:** Policy graph G , new policy P

Output: BOOL

function CheckG, P

$N \leftarrow \text{count}(G.\text{node});$

$TotalIF \leftarrow 0;$

fori in Ndo

forj in Ndo

$TotalIF \leftarrow G[i][j] + TotalIF;$

end for

end for

$AvgIF \leftarrow TotalIF/N;$

$W \leftarrow G[i][j];$; //Assume that i, j is conflicted policy.

if $W > AvgIF$ **then**

sendPolicy(P); //send P to application for resolving conflict.

return FALSE;

else

GraphReconstruction(P);

return TRUE;

end if

end function

function GraphReconstruction P

fork in Ndo

if $G[i][k] == 1$ **then**

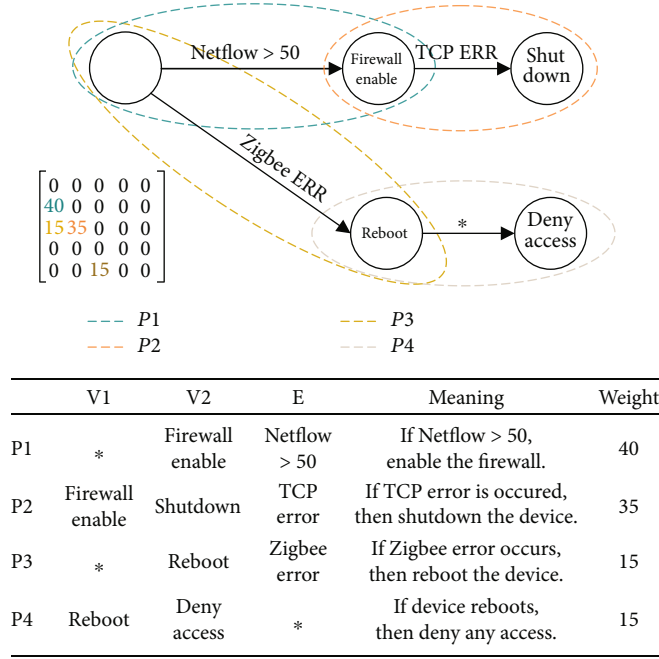


FIGURE 4: An example of policy graph.

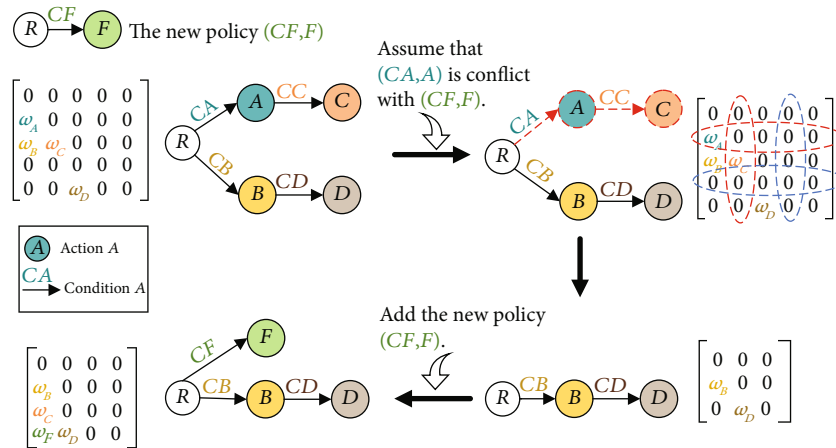


FIGURE 5: The policy graph reconstruction.

```

from G.
    deleteColumn(G, k); //delete the k column
    deleteRow(G, j);
end if
end for
if deleteColumn(G, i) == TRUE then
    G[i][j] ← 0; //initial weight is zero.
    node[i], node[j] ← P.event, P.action;
    edge[j] ← P.condition; //store the information of P.
return TRUE;
else
    return FALSE;
end if
end function
    
```

6. Evaluation

FPICR is evaluated on enforcing policies over mobile devices in a real Ethereum platform to demonstrate the performance FPICR achieved. We have made a fair comparison with one of the state-of-the-art solutions, XACML framework. The objectives of the evaluation are threefold: (1) testing the performance improvement of FPICR over traditional method; (2) studying the impact of FPICR on the blockchain; (3)


```

Input: Policy graph  $G$ , new policy  $P$ 
Output: BOOL
function CheckG,  $P$ 
   $N \leftarrow \text{count}(G.\text{node});$ 
   $TotalIF \leftarrow 0;$ 
  for  $i$  in  $N$  do
    for  $j$  in  $N$  do
       $TotalIF \leftarrow G[i][j] + TotalIF;$ 
    end for
  end for
   $AvgIF \leftarrow TotalIF/N;$ 
   $W \leftarrow G[i][j];$  //Assume that  $i, j$  is conflicted policy.
  if  $W > AvgIF$  then
     $\text{sendPolicy}(P);$  //send  $P$  to application for resolving conflict.
    return FALSE;
  else
     $\text{GraphReconstruction}(P);$ 
    return TRUE;
  end if
end function
function GraphReconstruction $P$ 
  for  $k$  in  $N$  do
    if  $G[i][k] == 1$  then
       $\text{deleteColumn}(G, k);$  //delete the  $k$  column from  $G.$ 
       $\text{deleteRow}(G, j);$ 
    end if
  end for
  if  $\text{deleteColumn}(G, i) == \text{TRUE}$  then
     $G[i][j] \leftarrow 0;$  //initial weight is zero.
     $\text{node}[i], \text{node}[j] \leftarrow P.\text{event}, P.\text{action};$ 
     $\text{edge}[j] \leftarrow P.\text{condition};$  //store the information of  $P.$ 
    return TRUE;
  else
    return FALSE;
  end if
end function

```

ALGORITHM 1. Policy conflict resolution.

providing insights of FPICR’s outperforming its peers in BC-IoT.

6.1. Experimental Setup

6.1.1. System Prototype. We build a real fully-equipped BC-IoT rather than a simulated testbed. We deploy five development boards Jetson-TK1s as endpoint devices, and three more servers as the security and mining server. All of these devices are under the same LAN, as shown in Figure 6. Besides, the miner server is set to be full mode, while others are set to be light mode. The security policies are enforced by sending transactions to Ethereum. The blockchain used is Go-ethereum (version 1.7), and the version of EVM we used is 1.7.0. The Ethereum official recommended evaluation framework Truffle is employed to evaluate the performance of blockchain. The hardware configurations in detail are shown in Table 2.

6.1.2. Data Set. We use a policy repository including 10,000 log-based policies and 10,000 XACML-based policies. The

logs utilized are HDFS data collected from the real running system for policy template construction. The priority of each log-based policy and each XACML-based policy is assigned one random of the five values ranged from 1 to 5. The weight of each policy is initialized by random values. The data and code used to support the findings of this study have been deposited in the FPICR repository (<https://github.com/nkicsl/FPICR>).

6.1.3. Measure Metrics. The PbSM in the BC-IoT mainly requires low latency to handle the security problems in real-time, high throughput to process more access requests in a short time, and a small ledger size to save the blockchain storage space. Therefore, to evaluate the performance improvement, we choose the following metrics: (1) the overall performance of FPICR measured by latency, we test the time consumption of policy conflict resolution in FPICR; (2) we then care about the resolution rate and the breakdown latency spent in conflict detection, resolution, and interpretation phases, the throughput for interpreting policies; (3) to further understand FPICR making full use of blockchain,

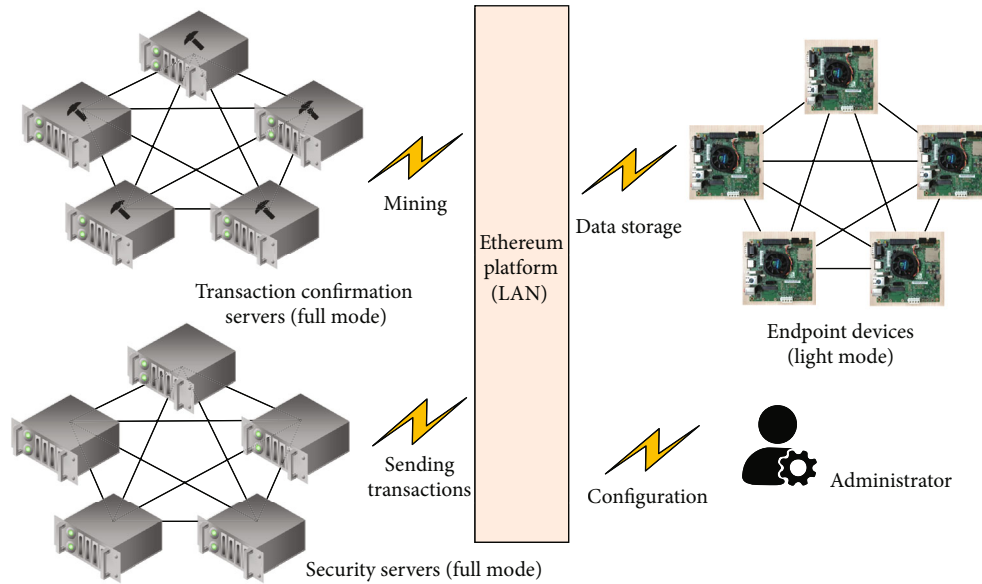


FIGURE 6: The prototype of FPICR.

TABLE 2: The hardware configuration in our experiment.

	Endpoint	Security
Hardware	Jetson-TK1	DELL tower
CPU	ARMv7	Xeon E5-2630
Memory	1.9 GB	96,566 MB
OS	Ubuntu 14.04	Ubuntu 16.04

we also evaluate the resource utilization and overhead of blockchain by ledger size and CPU's overhead; (4) at last, we give a breakdown analysis to explain why FPICR outperforms other PbsM methods in BC-IoT.

6.2. FPICR Overall Performance. To evaluate the overall performance, we select 5,000 policies with 1,500 conflicted ones in the policy repository. So there are 30% of the security conflicted policies in each group. In the experiment, policies number size varies from 500 to 5000 with an increment of five hundred. As a comparison, the control group or blank blockchain group is set to facilitate evaluating the communication overhead of blockchain. Experimental results have been summarized as shown in Figure 7. Compared with XACML, FPICR can achieve latency reduction by 14.1%, even maximum by 18.73%. Therefore, FPICR in the BC-IoT system is outstanding, and FPICR can decrease time consumption from policy interpretation and conflict resolution.

6.3. Resolution Rate

6.3.1. Conflict Resolution Performance. The resolution rate in this paper refers to the percentage of the resolved conflict policies to the total conflict policies. One of the FPICR goals is resolving more policy conflicts automatically according to the system runtime information. High conflict resolution rate means FPICR can resolve more policy conflicts without manual decision. We select 2,000 policies with 400 existing conflict policies to evaluate the resolution rate of FPICR. We

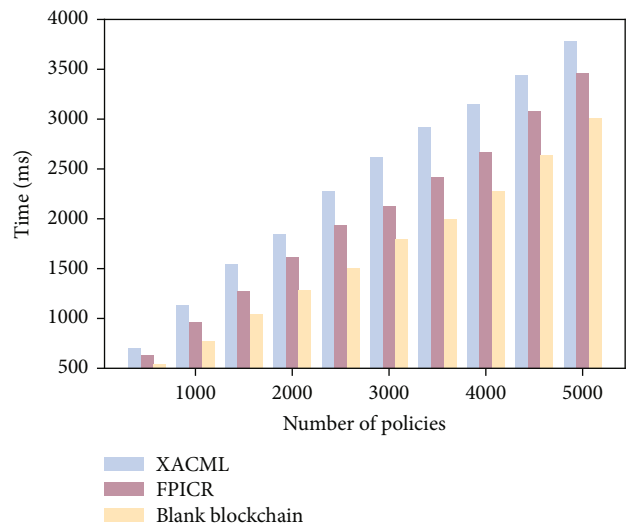


FIGURE 7: The overall performance of FPICR and XACML.

perform a comparison between FPICR and the baseline XACML by resolving policy conflicts for 500 times. The results of the resolution rate of two methods achieved are shown in Figure 8. We can observe that FPICR achieves a better policy conflict resolution rate by 91.6%-95.8%, reaching 93.7% on average, while the comparison one is only about 87.6%. It should be noted that though the resolution rate is higher than the comparison by 6%+ on average, FPICR processing speed can also be improved by up to 2.1 \times .

6.3.2. Latency. Next, we shift our attention to the time consumption FPICR takes to process the same number of policy conflicts. In this case, we measure the breakdown latency spent on the conflict resolution and interpretation phase. In our evaluation, conflict resolution consists of three steps roughly:

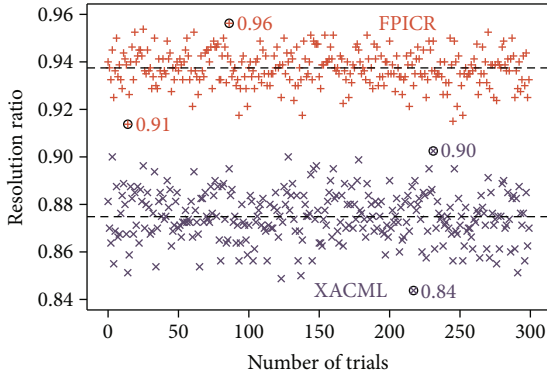


FIGURE 8: The resolution rate.

- (i) *Proposal*. We proposed transactions to the target systems, and each transaction contains one security log-based policy
- (ii) *Handling*. The uploaded policy can be detected whether there exist conflicts or not by a specific smart contract. Once the conflict has been detected, it will be resolved and the WDPG reconstruction will be performed. The new WDPG will be also updated into the PGC. If the conflict cannot be handled by FPICR or the comparison presetting static priority, this conflict will be handled manually
- (iii) *Submit Manually*. The result for the unresolved conflict will be submitted to the BC-IoT system again. This process can lead to lots of writing operations in the blockchain network, thus, this step is very time-consuming. The worse is that too many conflicts will lead to a large of labor works

Compared with the static priority-based resolution by 15%, 30%, and 45% conflicted policies among the total policies, FPICR can efficiently reduce the latency by 17.44%, 23.93%, and 34.47%, respectively. Because FPICR facilitates solving conflicts by smart contract executing automatically, policy enforcement can regain more time. In contrast, unsolved conflict policy which requires to be handled manually will introduce many labor works; as a result, the time consumption will be greatly increased.

6.4. Interpretation Performance. FPICR aims to achieve fast policy interpretation without missing the accuracy of interpretation results. In this part, we interpret the proposed policy and the typical policy and compare the latency between them. There are two steps for the interpretation phase, the first is policy conversion, and the second is contract deployment. The conversion refers to converting policy into a smart contract. The deployment is to deploy smart contract on the blockchain. We prepare several groups of policies from 300 to 5000 to perform a comparison between FPICR and the baseline XACML. The first metric we are concerned about is conversion latency. We do not care about the deployment time, because it costs the same time in both FPICR and baseline. The comparison results in Figure 9(a) show that com-

pared with XACML, FPICR can speed up by about $2.1 \times$ with the obvious advantages. FPICR can fast convert a single log-based policy by only using 0.051 ms on average.

6.4.1. Throughput. Throughput as another metric to evaluate the performance of interpretation. We have also made a comparison between FPICR and XACML to test the number of interpreting policies into smart contract per period. In Figure 9(b), the comparison results about throughput indicate that FPICR can convert and deploy more policies than XACML within 60 seconds. FPICR outperforms the baseline by 1% to 10% along with time. In addition, to further improve throughput, we make full use of a single machine to explore the limitation. We utilize several processes to work together and the results are shown in Figure 9(c). With the increment of the number of processes, the experimental BC-IoT system can enforce dozens of policies per second. When the number of processes increases from 15 to 30, the curve of enforced policy number tends to be gentle. However, when the number is over 30, the curve has begun to drop and flatten fast.

6.5. Blockchain Overhead. We care about the blockchain overhead of BC-IoT to measure the performance of WDPG. The experiments are performed from two aspects: storage reduction and CPU overhead. The reduction of blockchain storage space (or ledger size) is achieved by identifying and cutting the redundant parts brought by the policy dependencies.

6.5.1. Ledger Size. The main index of storage resources about blockchain is ledger size. In our evaluation, ledger size refers to the size of the Ethereum ledger file in runtime. In Figure 10, we can see that the ledger size of blockchain increases with the number of policies growing. Storage structure with WDPG can effectively reduce the size by 16.86% at most than the others.

6.5.2. CPU Overhead. At last, we also have evaluated the CPU overhead during the policy interpretation period. In light of the results in Figure 11, FPICR can interpret and upload 300 policies from 34 s to 110 s. During this period, the peak point of 8.89% represents the CPU occupied by the converting function and the process only lasts for a short time, thereafter, the CPU overhead decreases down to around 3.5%. By contrast, if the ordinary data is uploaded to the blockchain instead of deploying a contract, the overhead of the CPU fluctuates around 4.7%. Obviously, FPICR can effectively reduce CPU overhead during BC-IoT system running. The comparison also indicates that FPICR can be efficient enough to be installed in other real BC-IoT.

6.6. Performance Analysis. This subsection gives a breakdown analysis to explain why FPICR can achieve performance improvement than other PbSM methods in the BC-IoT system.

Because of system runtime information recording in our designed WDPG, FPICR can make full use of the real situation rather than speculation or presetting. The high-resolution rate of FPICR is also benefited from the design,

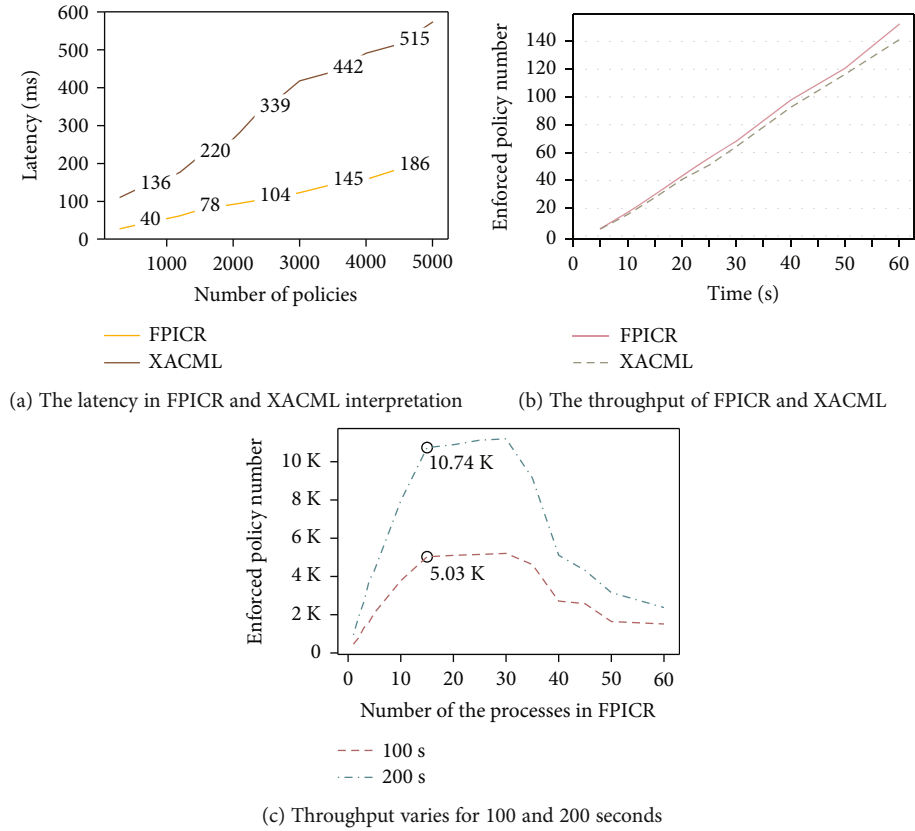


FIGURE 9: The performance of interpretation in prototype.

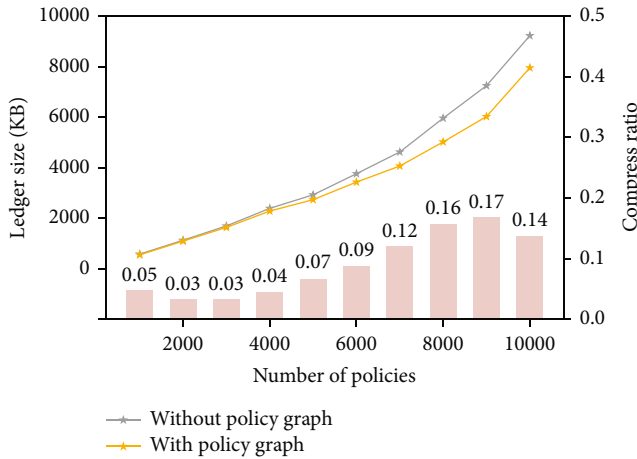


FIGURE 10: The ledger size with policy graph.

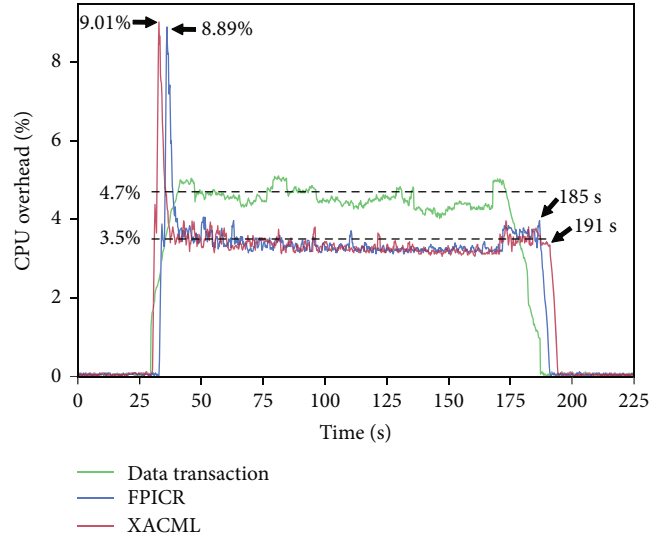


FIGURE 11: The CPU overhead during interpretation.

and more conflicts can be solved automatically, thus, FPICR can decrease heavy labor works. We can find results in the submit manually step in Figure 12, transactions by processing manually will be reduced relative greatly in FPICR.

As shown in Figure 9(a), the low latency metric results benefit from the log-based policy templates. The designed templates can match the smart contract template exactly. This facilitates that FPICR can fill the templates directly, instead of complex parsing. FPICR, in consequence, can only use one step to complete policy interpretation; otherwise, the

other methods usually need to take two steps to process. They often require to extract the variables and notations (i.e., “+”, “”) from the labels and then execute the parsing module. And the parsing is very time-consuming as shown in Figure 9(a). Therefore, our FPICR can meet the requirement of low latency and fast interpretation process very well. These advantages help FPICR achieve high throughput without

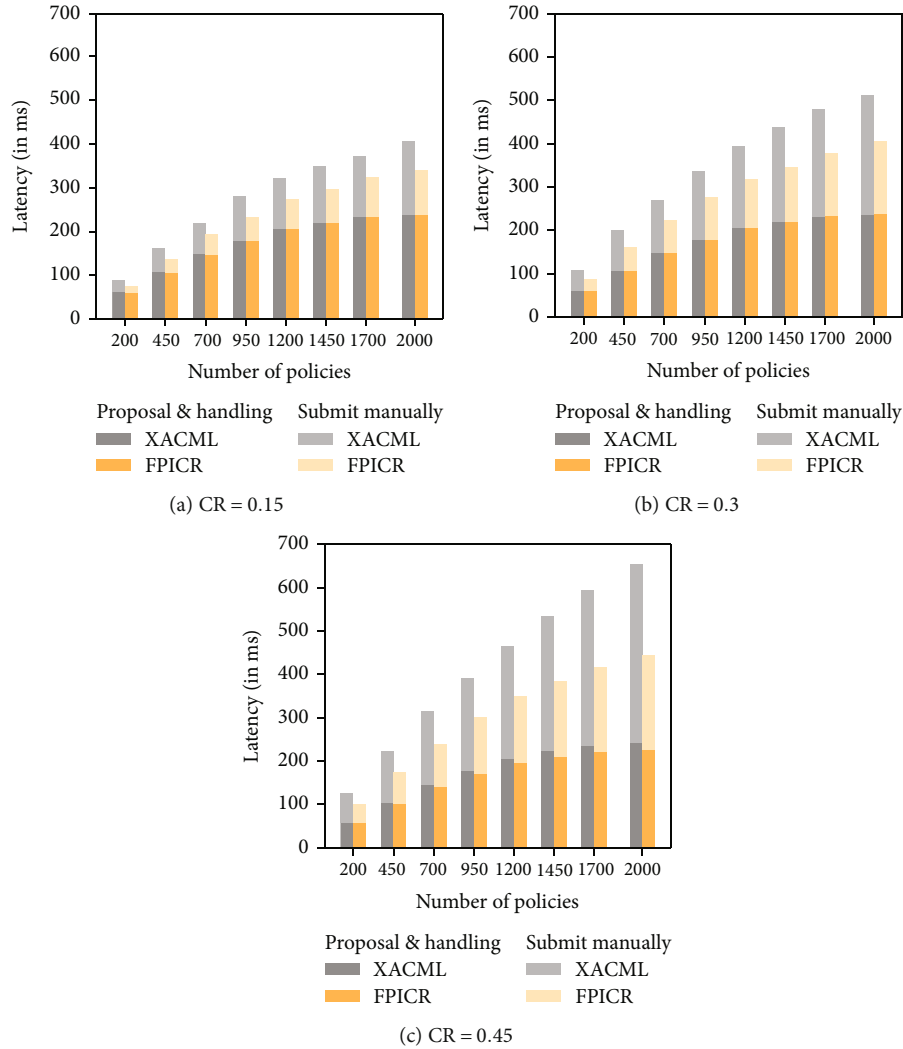


FIGURE 12: The performance of conflict resolution in FPICR.

blocking almost. The reason about storage reduction is that WDPG facilitates policies to only store a simple string rather than redundant uselessly information on blockchain. Therefore, the source data can be reduced and then the ledger size can be decreased. We also find that when the number of policies is increasing large, the compression rate of ledger size can be even further higher, as shown in Figure 10.

For CPU overhead, FPICR CPU resource is only occupied by 4% to 5%, compared with XACML. Because of removing the complex syntactic analysis, FPICR does not need additional computation and can reduce the consumption of CPU. This characteristic enables FPICR to be suitable for computational resource-limited IoT end devices.

7. Conclusion

In this paper, we present FPICR for fast interpretation and dynamic conflict resolution so as to implement effective and efficient PbSM in the BC-IoT system. We propose a new log-based policy interpretation method by extracting parameters directly only in one step. In addition, we present a weighted directed policy graph to organize the relationship

for thousands of deployed policies. To solve policy conflict dynamically, the resolution algorithm is proposed based on WDPG reconstruction. FPICR can overcome the limitations of the BC-IoT system and meet the requirements of low latency and compression storage space. Evaluation on FPICR and the comparison results have proved that FPICR can reduce policy interpretation latency and the ledger size of blockchain. Therefore, FPICR can actually realize efficient and economic PbSM for blockchain-based IoT system.

Data Availability

The data and code used to support the findings of this study have been deposited in the FPICR repository (<https://github.com/nkicsl/FPICR>).

Conflicts of Interest

On behalf of all authors, the corresponding author states that there is no conflict of interest.

Acknowledgments

This work is partially supported by the National Key Research and Development Program of China (2018YFB2100300), Zhejiang Lab (2021KF0AB04), the Natural Science Foundation of Tianjin (20JCZDJC00610 and 19JCQNJC00600), and the National Natural Science Foundation (62002175 and 61872200).

References

- [1] R. Petrolo, V. Loscri, and N. Mitton, "Towards a smart city based on cloud of things," in *Proceedings of the 2014 ACM international workshop on Wireless and mobile technologies for smart cities*, pp. 61–66, Philadelphia, Pennsylvania, USA, 2014.
- [2] Y. He, J. Guo, L. Liu et al., "Iot for the power industry: recent advances and future directions with pavatar," in *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems, SenSys'18*, pp. 353–354, New York, NY, USA, 2018.
- [3] L. Zhao and X. Dong, "An industrial internet of things feature selection method based on potential entropy evaluation criteria," *IEEE Access*, vol. 6, pp. 4608–4617, 2018.
- [4] X. Han, L. Wang, S. Xu, D. Zhao, and G. Liu, "Recognizing roles of online illegal gambling participants: an ensemble learning approach," *Computers & Security*, vol. 87, p. 101588, 2019.
- [5] A. A. Seif and N. El-Saber, "Scalable distributed-computing iot applied architecture with semantic interoperable gateway," in *Proceedings of the 3rd Africa and Middle East Conference on Software Engineering, AMECSSE '17*, pp. 43–44, New York, NY, USA, 2017.
- [6] Y. Zhao, Y. Li, X. Zhang, G. Geng, W. Zhang, and Y. Sun, "A survey of networking applications applying the software defined networking concept based on machine learning," *IEEE Access*, vol. 7, pp. 95397–95417, 2019.
- [7] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2019.
- [8] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2019.
- [9] V. Scoca, R. B. Uriarte, and R. De Nicola, "Smart contract negotiation in cloud computing," in *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*, pp. 592–599, Honolulu, HI, USA, 2017.
- [10] Z. Shae and J. Tsai, "Ai blockchain platform for trusting news," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 1610–1619, Dallas, TX, USA, 2019.
- [11] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, 2019.
- [12] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3162–3173, 2019.
- [13] F. Moradi, A. Sedaghatbaf, S. A. Asadollah, A. Causevic, and M. Sirjani, "On-off attack on a blockchain-based iot system," in *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pp. 1768–1773, Zaragoza, Spain, 2019.
- [14] Y. Wang, S. K. Lahiri, S. Chen et al., "Formal verification of workflow policies for smart contracts in azure blockchain," in *Working Conference on Verified Software: Theories, Tools, and Experiments*, pp. 87–106, Springer, 2019.
- [15] S. Zhu, W. Li, H. Li, L. Tian, G. Luo, and Z. Cai, "Coin hopping attack in blockchain-based iot," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4614–4626, 2019.
- [16] W. Han and C. Lei, "A survey on policy languages in network and security management," *Computer Networks*, vol. 56, no. 1, pp. 477–489, 2012.
- [17] V. Varadharajan, K. Karmakar, U. Tupakula, and M. Hitchens, "A policy-based security architecture for software-defined networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 897–912, 2019.
- [18] A. Lara and B. Ramamurthy, "Opensec: policy-based security using software-defined networking," *IEEE Transactions on Network and Service Management*, vol. 13, no. 1, pp. 30–42, 2016.
- [19] A. Gember, C. Dragga, and A. Akella, "Ecos: leveraging software-defined networks to support mobile application offloading," in *2012 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS)*, pp. 199–210, Austin, TX, USA, 2012.
- [20] A. A. Jabal, M. Davari, E. Bertino et al., "Methods and tools for policy analysis," *ACM Computing Surveys (CSUR)*, vol. 51, no. 6, pp. 1–35, 2019.
- [21] Z. B. Celik, G. Tan, and P. D. McDaniel, "Iotguard: dynamic enforcement of security and safety policy in commodity iot," in *Proceedings 2019 Network and Distributed System Security Symposium*, San Diego, California, USA, 2019.
- [22] L. F. Cranor, "P3p: making privacy policies more useful," *IEEE Security & Privacy*, vol. 1, no. 6, pp. 50–55, 2003.
- [23] J. D. Moffett and M. S. Sloman, "Policy conflict analysis in distributed system management," *Journal of Organizational Computing and Electronic Commerce*, vol. 4, no. 1, pp. 1–22, 1994.
- [24] H. X. Son and E. Chen, "Towards a fine-grained access control mechanism for privacy protection and policy conflict resolution," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 2, 2019.
- [25] X. Du, Z. Lv, J. Wu, C. Wu, and S. Chen, "Pdsdn: a policy-driven sdn controller improving scheme for multi-tenant cloud datacenter environments," in *2016 IEEE International Conference on Services Computing (SCC)*, pp. 387–394, San Francisco, CA, USA, 2016.
- [26] N. M. Hoang and H. X. Son, "A dynamic solution for fine-grained policy conflict resolution," in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, pp. 116–120, Kuala Lumpur, Malaysia, 2019.
- [27] Y. Kim, J. Nam, T. Park, S. Scott-Hayward, and S. Shin, "Soda: a software-defined security framework for iot environments," *Computer Networks*, vol. 163, p. 106889, 2019.
- [28] D. Wenxia, L. Chengyong, W. Ding, and F. Li, "Policy conflict resolution method and apparatus," US Patent 10,193,755, 2019.
- [29] A. Molina Zarca, J. B. Bernabe, R. Trapero et al., "Security management architecture for nfv/sdn-aware iot systems,"

- IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8005–8020, 2019.
- [30] S. Godik and T. Moses, *Oasis Extensible Access Control Markup Language*, OASIS Committee Specification cs-xacml-specification-1.0, 2002.
 - [31] B. Wu, X.-y. Chen, Y.-f. Zhang, and X.-d. Dai, “An extensible intra access control policy conflict detection algorithm,” in *2009 International Conference on Computational Intelligence and Security*, pp. 483–488, Beijing, China, 2009.
 - [32] M. Charalambides, P. Flegkas, G. Pavlou et al., “Policy conflict analysis for quality of service management,” in *Sixth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY’05)*, pp. 99–108, Stockholm, Sweden, 2005.
 - [33] C. Shin and W. Woo, *Conflict Resolution Method Utilizing Context History for Context-Aware Applications*, vol. 577, Cognitive Science Research Paper-University Of Sussex Csrp, 2005.
 - [34] B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, “A blockchain-based architecture for collaborative ddos mitigation with smart contracts,” in *Security of Networks and Services in an All-Connected World*, pp. 16–29, Springer, Cham, 2017.
 - [35] O. Novo, “Blockchain meets iot: an architecture for scalable access management in iot,” *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018.
 - [36] O. Alphand, M. Amoretti, T. Claeys et al., “Iotchain: a blockchain security architecture for the internet of things,” in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Barcelona, Spain, 2018.
 - [37] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: the blockchain model of cryptography and privacy-preserving smart contracts,” in *2016 IEEE symposium on security and privacy (SP)*, pp. 839–858, San Jose, CA, USA, 2016.
 - [38] M. Du, F. Li, G. Zheng, and V. Srikumar, “Deeplog: anomaly detection and diagnosis from system logs through deep learning,” in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1285–1298, Dallas, TX, USA, 2017.
 - [39] J. Bailey, G. Papamarkos, A. Poulouvassilis, and P. T. Wood, “An event-condition-action language for xml,” in *Web Dynamics*, pp. 223–248, Springer, 2004.

Research Article

Privacy Threats of Acoustic Covert Communication among Smart Mobile Devices

Li Duan ¹, Kejia Zhang ^{2,3,4}, Bo Cheng,³ and Bingfei Ren ³

¹Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing 100044, China

²School of Mathematical Science, Heilongjiang University, Harbin 150080, China

³State Key of Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, 100876, China

⁴Cryptology and Cyberspace Security Laboratory of Heilongjiang University, Harbin 150080, China

Correspondence should be addressed to Kejia Zhang; zhangkejia.bupt@gmail.com and Bingfei Ren; renbingfei0@gmail.com

Received 23 May 2021; Accepted 22 June 2021; Published 5 July 2021

Academic Editor: Weizhi Meng

Copyright © 2021 Li Duan 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 emerging, overlocking signal-based acoustic covert communication technique allows smart devices to communicate (without users' consent) utilizing their microphones and speakers in ultrasonic side channels, which offers users imperceptible and convenient personalized services, e.g., cross-device authentication and media tracking. However, microphones and speakers could be maliciously used and pose severe privacy threats to users. In this paper, we propose a novel high-frequency filtering- (HFF-) based protection model, named *UltraFilter*, which protects user privacy by enabling users to selectively filter out high-frequency signals from the metadata received by the device. We also analyze the feasibility of using audio frequencies (i.e., ≤ 18 kHz) to the acoustic covert communication and carry out the acoustic covert communication system by introducing the auditory masking effect. Experiments show that *UltraFilter* can prevent users' private information from leaking and reduce system load and that the audio frequencies can pose threats to user privacy.

1. Introduction

With the rapid development of the Internet of Things (IoT) and smart devices, a user may have more than a smart device [1] for communication and entertainment. There is an increasing need for cross-device authentication [2], and one of multiple devices can act as an identity to control the authorization of the other devices. Traditional cross-device authentication uses the network access or Bluetooth function of devices to complete the authorization task. Because of their long transmission distance, it cannot meet the demand of short-range cross-device authentication. Considering a situation that a user left the smart phone (i.e., the device to be authorized) in the office and a user is temporarily away, the user may use a smart watch (worn by the user and representing the user's identity) to complete an authorization process with the smart phone through wireless network or Bluetooth. At this time, attackers in the office can gain access to the user's smart phone.

Because the propagation distance of ultrasonic frequency (i.e., > 18 kHz) is short and imperceptible to users, it has gradually become a research hotspot to use ultrasonic frequency for cross-device authentication or media tracking. Taking media tracking for example, India's Silverpush Company [3] conducts advertising push business by providing a software development kit (SDK). Cooperative clients integrate the advertising push function in their own shopping software by using SDK. The SDK has a built-in ultrasonic frequency signal detection module and a data reporting module. When the detection module detects a specific overlocking signal, the data reporting module starts to collect and report users' personal information to Silverpush's servers. In this way, Silverpush can acquire a large amount of private data and track user's personal trajectories.

Using microphones and speakers in Android devices, acoustic covert communication can provide users with personalized and convenient services, such as cross-device authentication [2] and media tracking-based advertisement

push [3]. Covert communication refers to communication in which users do not perceive abnormality under normal circumstances [4]. However, a malicious use of microphones and speakers would bring potential privacy threats to users. Take the routing in an anonymous network [5] for an example. The source and destination addresses of a message are encrypted layer-by-layer, and the sender can access network resources anonymously.

By using acoustic covert communication, the anonymization operation in the anonymous network can be carried out the following four steps: (1) the attacker embeds overclocking signals in normal audio and anonymization video files as audio beacons and adds the synthesized audio files into the webpage of the anonymous network; (2) a target user sends the request to access the anonymous network by using a personal computer; (3) the target user plays the synthesized audio when browsing the webpage containing the synthesized audio and video files; (4) the target user does not perceive abnormality in the audio data, if the user carries an application with a decoding function or SDK integrated with a detection and decoding function (such as Silverpush); (5) the user receives the sound signal through the microphone and detects the hidden audio beacon; and (6) after detecting the special signal, the application begins to collect the user's personal information and send it to the attacker through the network. The detailed process is shown in Figure 1.

In order to protect microphones and speakers from malicious uses, the Android platform provides an authority system: Only when an application declares record authority (*RECORD_AUDIO*) in the configuration file and is authorized by the user, it can access the microphone of the device to collect sound, and only by declaring *MODIFY_AUDIO_SETTINGS*, the application can turn on the microphone or turn off the speaker of the device. However, the protection mechanism of microphone or speaker based on authority in Android systems can be easily bypassed by malicious software, such as collusion attack [6]. The devices can be turned to conduct covert sound wave communication, and malicious attacks can be executed without the user's awareness, causing serious privacy and security problems for users.

Existing studies typically focus on synthesizing confrontation samples, e.g., by using deep learning, to attack the Automatic Speech Recognition (ASR) systems of smart devices [7], such as Google Home, Apple's Siri, Amazon Echo, and Microsoft Cortana [8], and develop countermeasures. The existing studies have overlooked that attackers could use the microphone and speaker to achieve acoustic covert communication, compromising users' privacy (e.g., visiting anonymous networks). Despite microphone-based acoustic covert communication is analyzed in [9], yet no design or implementation of countermeasures is presented.

This paper designs and implements a new acoustic high-frequency signal filtering-based security protection mechanism, to address the privacy threats caused by acoustic covert communication attacks to Android devices. In particular, we carry out an in-depth study analysis of related works and reveal that acoustic covert communication between Android devices is primarily based on inaudible high-frequency signals (above 18 kHz). The inaudible high-frequency signals

are embedded into audio files (e.g., music and advertisements) to generate a synthetic audio file and delivered by playing the synthetic audio file. Specialized applications can detect and recognize the inaudible high-frequency signals at target devices.

By using high-frequency filtering, our security mechanism erases near-ultrasonic signals that are inaudible to the users. Further, we study the feasibility of using audible frequency for acoustic covert communication and analyze whether acoustic covert communication imperceptible to users in the audible frequency band poses a potential threat to the user's privacy. The contributions of this paper are summarized, as follows.

- (i) A new acoustic high-frequency filtering-based security framework, named *UltraFilter*, is proposed to address the privacy leakage issue of acoustic covert communication. Inaudible high-frequency signals (above 18 kHz) that do not affect the user's perception are filtered and suppressed, so as to protect user privacy
- (ii) We reveal that acoustic covert communication can be achieved even in the audible spectrum; the acoustic covert communication without user's perception is finished by employing the auditory masking effect model
- (iii) We design and implement two prototype systems. One is the security system based on the high-frequency filtering. The other is a prototype system of acoustic communication without user perception based on normal frequency. The functional verification and performance tests are conducted on the Android version 6.0 system (Xiaomi 4 devices)

The rest of this paper is organized, as follows. Section 2 reviews the related work. In Section 3, we elaborate on the proposed security mechanism, which erases near-ultrasonic signals and protects user privacy. In Section 4, we study the feasibility of using audible frequency for acoustic covert communication by introducing the auditory masking effect model. In Section 5, the prototype systems are designed, implemented, and tested. In Section 6, this paper is concluded.

2. Related Work

Existing studies on acoustic covert communication are focused primarily on three aspects: steganography on audio files, sound signals against sample generation for automatic speech recognition (ASR), and acoustic covert communication among smart devices based on inaudible high-frequency signals.

2.1. Steganography on Audio Files. Steganography [10] refers to the technical methods of hiding information in a harmless format. The communication parties attach the hidden information to normal carriers (such as text files) in a preagreed way and generate seemingly normal camouflage carriers

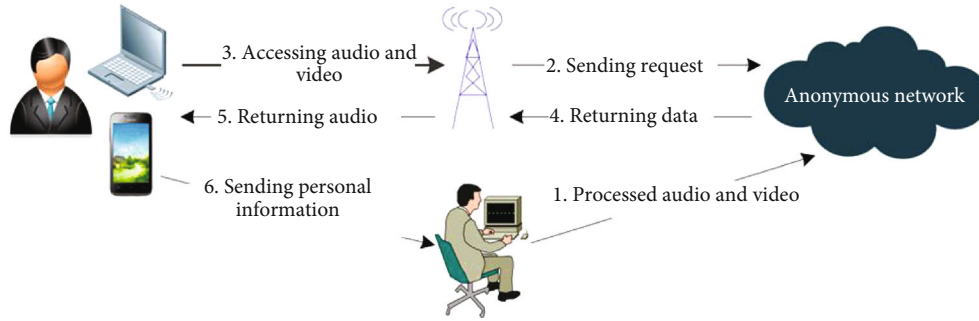


FIGURE 1: De-anonymization of anonymous network users using acoustic covert communication.

and spread it. Only the communication parties can accurately detect and analyze the hidden information. The larger the data file is, the harder it is to find the hidden information. After the concept of modern steganography [11, 12] was put forward in 1985. With the popularity of mobile Internet and the wide application of digital media, steganography based on digital media has developed rapidly. Digital media, such as video, pictures, and audio, contain a large amount of data and widely spread through the Internet. Therefore, steganography using digital media (e.g., audio files) for hiding information and dissemination has attracted wide attention [13–16].

The main challenge of steganography is to deceive the Human Auditory System (HAS) [17]. In the application of audio-based steganography, information can be hidden in three ways: temporal domain, frequency domain, and code domain. Each approach has a corresponding technology to encode hidden information into the carrier audio without damaging it (that is, users cannot perceive it). For example, least significant bits (LSB) can be used to hide the hidden information in the temporal domain of audio [18]. Because no obvious noise is introduced into the audio file, the whole information transmission process is imperceptible to the user.

It is reported in [19] that Discrete Wavelet Transform (DWT) can transform sound signals in the temporal domain to/from the frequency domain and obtain the corresponding wavelet correlation coefficient. By writing the hidden information into the LSB of the correlation coefficient, the covert transmission of hidden information can be accomplished. However, steganography has high requirements for the receiver and the transmission channels. It is difficult for the receiver to extract hidden information accurately. LSB-based audio steganography has high transmission performance (i.e., more hidden information) and is relatively easy to implement. However, it has low anti-interference ability, and the hidden information data in the LSBs can be destroyed. A method is to add a small amount of noises to audio files or losslessly compress the files [20].

2.2. Sound Signal Countermeasure Sample Generation for Automatic Speech Recognition (ASR). In recent years, ASR has made remarkable progress. Its main working mode is to make the machine recognize and understand the speech signal and convert the speech signal into texts or commands

[21]. ASR-based voice assistance is increasingly dominating the human-computer interaction, such as Google Assistant, Apple Siri, and Amazon voice assistant Alexa [8]. Voice assistants use voice classification models to detect voice commands, such as playing music, adding alarm clocks, making phone calls, inquiring weather, and controlling other smart devices in smart homes. The voice assistants also use the microphone of the devices to monitor the ambient sound continuously, so as to receive and recognize the voice commands quickly and provide timely services for users.

These automatic voice assistants are exposed to the risks of being maliciously controlled. Authors of [7] proposed that users' voice commands can be converted into ultrasonic frequencies by using ultrasonic devices. These overlocking voice commands, which are imperceptible to the user, can be used to control the speech recognition assistant. Compared with traditional speech recognition models based on hidden Markov chain, a deep learning-based ASR model generated by neural networks has greatly improved the recognition accuracy. However, neural networks are used by attackers to generate wrong targets or confrontation samples [22], so as to bypass the recognition of deep learning models or produce the results that attackers want from the models. Some researchers [23, 24] made use of this weakness of neural networks to generate confrontation samples of user voice commands to attack current ASR systems. The speech command countermeasure sample generation framework proposed in [25] can convert speech commands to any desired speech countermeasure samples. By processing a speech with the content of "without the dataset the article is useless", a corresponding confrontation sample can be generated and recognized by the ASR system as "okay google browse to evil dot com" [26]. The speech of this sample does not change to the user. At present, this kind of acoustic covert communication is mainly used to attack ASR systems. Because the attack target is clear, users can take precautions in advance.

2.3. High-Frequency Signal-Based Acoustic Covert Communication. With the rapid development of IoT technology and mobile intelligent devices, users are faced with the problem of continuous identity authentication for multiple mobile smart devices. Usually, it is necessary to use one of the devices as an identity to control the authorization of all other devices, such as cross-device authentication.

Traditional cross-device authentication technology often uses the network access or Bluetooth communication function in the devices to complete the authorization task. However, due to their long transmission distance, they cannot meet the requirements of short-distance cross-device authentication. In contrast, the high-frequency sound signal (above 18 kHz) has a short propagation distance and cannot be perceived by users. It has been increasingly considered for cross-device authentication [27, 28].

Yi et al. [29] proposed WakeLock, a smart phone security unlocking system based on acoustic communication. When the user unlocks its smart phone, the smart phone sends out a sound wave signal to verify the user's identity through the speaker of the device. The user receives the signal through the smart watch (which can be used as the user's identifier) and authorizes the request. Then, the mobile phone is unlocked for the user to use. When a stranger obtains the right to use the user's smart phone, the smart phone does not receive the authorization from the user's smart watch after sending the authorization request. The mobile phone remains locked to protect the user's device data from malicious access.

Mavroudis et al. [9] found that acoustic covert communication based on the microphones of smart phones can be used in media tracking. Shopkick [30] is location-based shopping software in the Android platform. When the user approaches a cooperative merchant, advertisement encoded into ultrasonic frequency signals is played at the door of the clients' shops. The ultrasonic signals that the user cannot perceive in the advertisement audio are detected by the Shopkick program in the user's mobile phone. Then, the merchant receives the notification of the user's arrival and sends a voucher to the user through the Shopkick application.

Covert communication based on inaudible high-frequency sound signals can provide users with convenient personalized services, such as identity authorization and shopping. However, it can also bring privacy threats to the users, such as the de-anonymization of anonymous network users. This paper focuses on how to mitigate the privacy threats imposed by the acoustic covert communication based on high-frequency signals and designs and implements the corresponding security model. In addition, the feasibility of using audible frequency for acoustic covert communication is studied, which can analyze whether the imperceptible acoustic covert communication in the audible frequency range can threaten the users' privacy.

3. Analysis of Acoustic Covert Communication Based on High-Frequency Signal

This section first briefly summarizes some basic concepts of acoustic communication and then studies the characteristics of the temporal and frequency domains of synthesized sounds (normal audio carriers and high-frequency special signals) in acoustic covert communication. According to the characteristics, a new security model is proposed, designed, and implemented to address the privacy issue arising from the acoustic covert communication, e.g., de-anonymization in anonymous networks.

Sound is a wave phenomenon which is generated by vibration, transmitted through medium (e.g., air, liquid, and solid), and then perceived by human or animal auditory organs. Sound sources with different vibration frequencies produce sounds with different pitches. The distance between the sound source and the receiver also directly affects the loudness felt by the receiver. In the Human Auditory System (HAS) [17], sound waves can be divided into the following three categories, according to the frequency:

- (1) *Infrasound*. Sound with a frequency lower than 20 Hz cannot be perceived by the human ears, and it is difficult to use infrasound to realize communication functions because the frequency is too low
- (2) *Audible Sound Waves*. Sound waves with frequencies between 20 Hz and 20 kHz can be perceived by the auditory system of human ears. The range of human hearing is between 20 Hz and 20 kHz
- (3) *Ultrasound*. sound wave, of which the frequency is higher than the upper limit of human hearing (i.e., 20 kHz), is called ultrasonic. Compared with infrasonic waves, ultrasonic waves have shorter wavelengths. Standard mobile devices can generate ultrasonic waves, and therefore, ultrasonic waves are suitable for short-distance acoustic communication

Due to the limitation of hardware configuration and human ear hearing system of smart mobile devices (such as smart phones and smart watches), only the frequency bandwidth from 18 kHz to 20 kHz can be used. Therefore, in order to realize acoustic covert communication without user's perception, FSK modulation technology is mainly used to modulate hidden information in acoustic covert communication. At the same time, in order to increase the transmission distance of high-frequency signals, the energy of high-frequency signals is set to a relatively high value (within this frequency bandwidth, users cannot perceive sound). As a result, the normal carrier audio (i.e., synthesized audio) synthesized with high-frequency signals is quite different from ordinary normal audio files in temporal domain, frequency domain, and spectrum characteristics. The normal carrier audio (synthesized audio) synthesized with high-frequency signals is quite different from ordinary normal audio files in temporal domain, frequency domain, and spectrum characteristics, as shown in Figures 2–4.

Because the high-frequency signal (18 kHz–20 kHz) is beyond the hearing range of normal people, the existing work makes use of this characteristic to realize acoustic covert communication based on high-frequency signal. By enhancing the energy of high-frequency signals, the long-distance transmission of high-frequency signals can be realized without causing users' doubts. Normal audio (such as music, advertisement, and conversation sounds) is in a frequency greater than 18 kHz, and its frequency energy is extremely low. However, the audio synthesized with high-frequency signal shows a strong energy distribution in the range of 18 kHz to 20 kHz (as shown in Figures 3 and 4). It is a great challenge to detect specific high-frequency signals in the sound

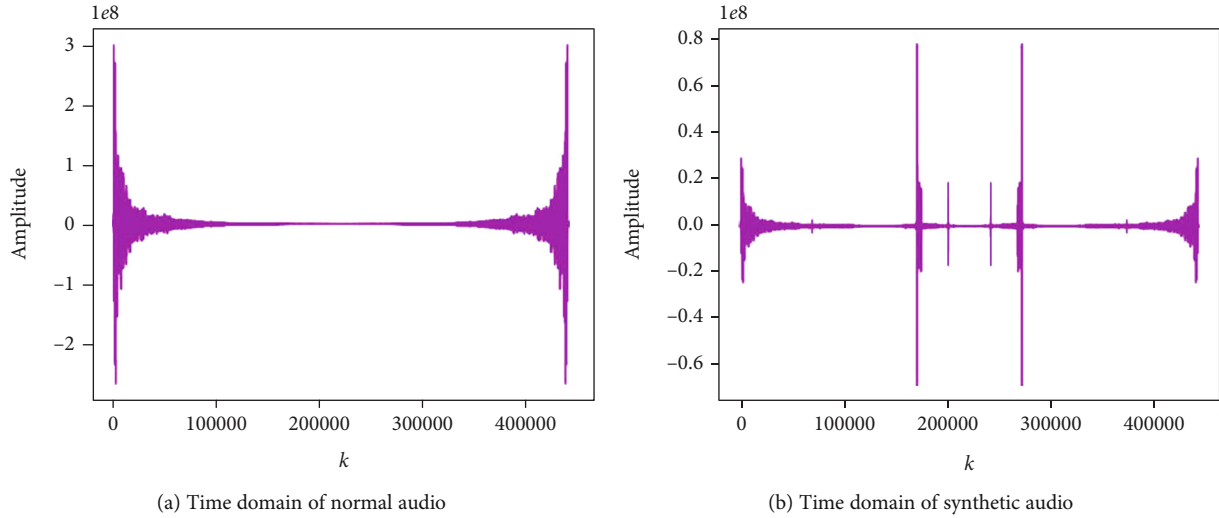


FIGURE 2: Comparison of time domain characteristics between synthetic audio and normal audio.

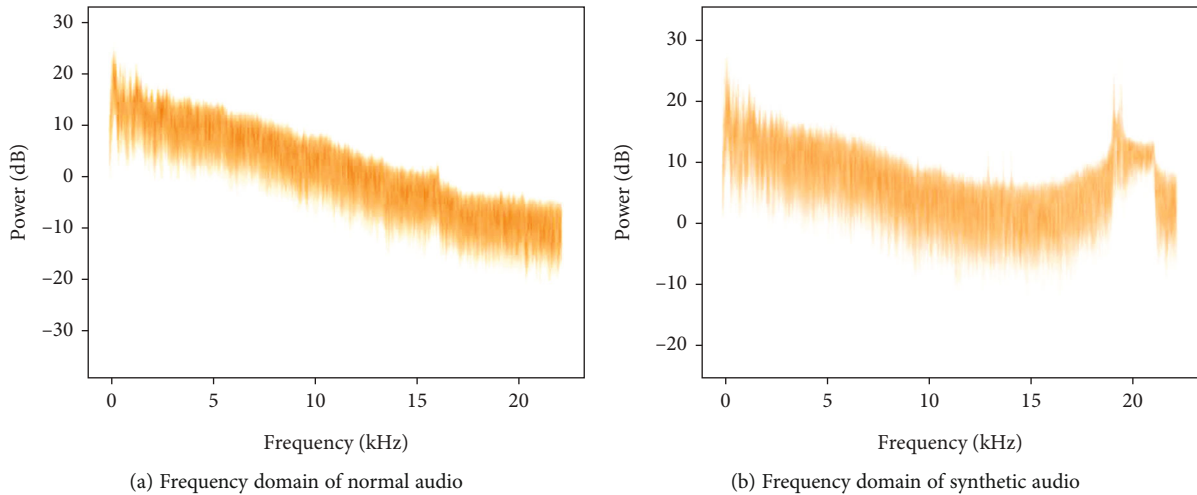


FIGURE 3: Comparison of frequency domain characteristics between synthesized audio and normal audio.

signals received by Android devices to identify potential acoustic covert communication. For example, it is difficult to master the modulation and demodulation scheme agreed by both parties and the specific high-frequency signal. Therefore, the corresponding security model can be designed and implemented in Android system by using the important characteristics of normal audio and synthesized audio, so as to enable users to protect personal privacy in a specific environment.

4. Security Model Based on High-Frequency Filtering of Sound Waves

4.1. Model Design. In a specific context, acoustic covert communication based on high-frequency signals, which is caused by the malicious use of equipment microphone and other resources, will bring potential privacy threats to users. Therefore, according to the analysis of the existing research work of acoustic covert communication based on high-frequency sig-

nals in the previous section, this section proposes a security model UltraFilter based on acoustic high-frequency filtering, which enable users to avoid privacy threats caused by high-frequency signal communication by controlling and protecting the Android system to obtain sound signals.

As shown in the work flow of security model in Figure 5, the upper part of the figure describes the work flow of Android device acquiring sound signal and Android system processing signal metadata under normal circumstances; the detailed description is as follows:

- (1) *Receiving the Signal.* The normal audio synthesized with special high-frequency signals is played out through the speaker of the device, and then, the user samples the external sound signals through the microphone in the intelligent device
- (2) *Sound Metadata.* Android system stores the sound signals sampled by microphone for subsequent processing

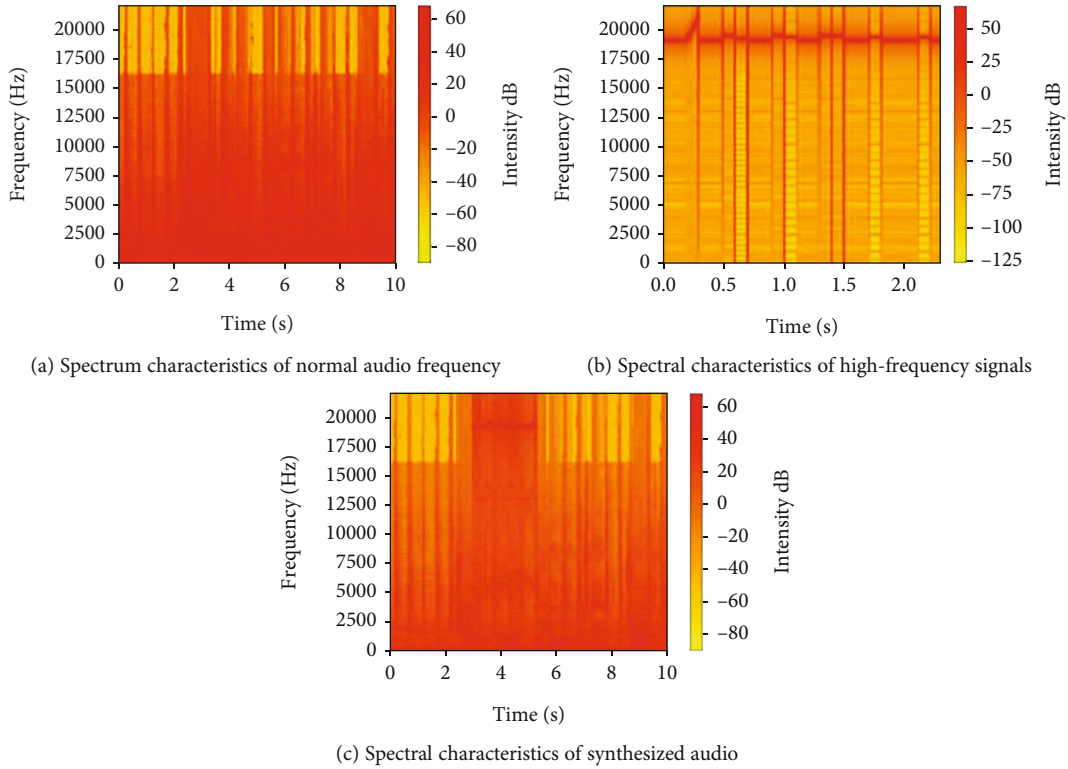


FIGURE 4: Comparison of spectrum characteristics between synthetic audio and normal audio.

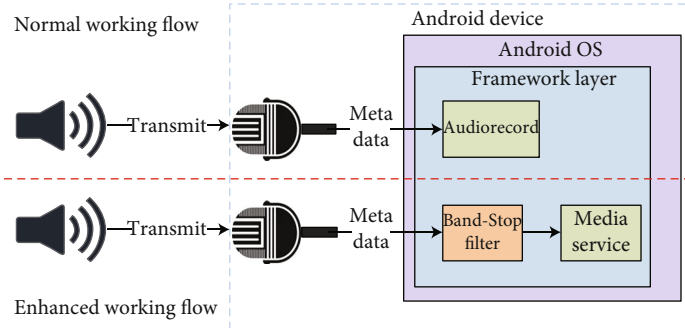


FIGURE 5: Security framework based on acoustic high-frequency filtering.

- (3) *High-Frequency Signal*. Particular applications in Android platform (such as Silverpush and Shopkick) call the *AudioRecord* interface provided by the media component in the system framework layer to obtain sound signal metadata; the applications directly call the *MediaRecorder* and *AudioRecorder* interface, but both of them need to use *AudioRecord* object to obtain sound data to detect and extract special high-frequency signals in them, and then perform corresponding functions, such as issuing bonus coupons to stimulate store consumption, pushing advertisements in a targeted manner, or anonymizing anonymous network users

By adding a band-stop filter (BSF) before the *AudioRecord* reads the original sound signal, the user can control

and filter out the high-frequency signals in the metadata, so as to ensure that personal privacy information is not leaked when accessing an anonymous network.

4.2. Model Implementation. This section introduces the technical details of the proposed UltraFilter, a security model based on high-frequency filtering of sound waves, which consists of the implementation of the BSF and the integration of the BSF into the Android system.

The purpose of the filter is to filter the signal in a specific frequency or frequency range. The commonly used filters [31] are Low-Pass Filter, High-Pass Filter, Band-Pass Filter, and band-stop filter (BSF). BSF is used in this paper. The key function of BSF is to attenuate the frequencies substantially in a specific range, so as to cut off the frequencies within a certain range in the signal data.

In this paper, a butterworth filter [32] is used to block the high-frequency part of the acoustic signal (from 18 kHz to 20 kHz). Band-stop filters based on various programming languages have similar structures. The following is our prototype.

$$\text{butter_filter}(\text{lowcut}, \text{highcut}, \text{fs}, \text{order} = \text{order}), \quad (1)$$

where *lowcut* and *highcut* are the upper and lower boundaries of the frequency range to be blocked, respectively, *fs* is the sampling frequency of the sound signal, *order* is the order of the filter, and the higher the order is, the faster the frequency attenuates in the specified range. For example, for a synthetic signal with frequencies of 600 Hz, 1200 Hz, and 1600 Hz is filtered with the band-stop filter. The noise data with frequency of 2 Hz is added to the synthetic signal for more obvious effect. The frequency to be suppressed ranges from 1000 Hz to 2000 Hz; i.e., the values of *lowcut* and *highcut* are 1000 and 2000, respectively. If the value of *fs* is consistent with the sampling frequency of the synthetic signal, the signal after passing through the band-stop filter should be a synthetic signal with a frequency of 600 Hz and the noise. The results shown in Figure 6 verify this reasoning and prove the effectiveness of the band-stop filter. Figure 7 shows the frequency attenuation characteristics in the range of 1000 Hz to 2000 Hz when order takes different values.

Because this paper needs to integrate the band-stop filter into the Android system, the third-party implementation library based on JAVA language [33] is the first choice in the implementation. The third-party library is integrated into the Android system, which is convenient for subsequent calling in the Android framework layer to realize the band-stop filter function. The integration steps are as follows:

- (1) Create a custom folder (usually named after the library) in the *external* folder in the Android source directory and a new folder named *src* in the newly created directory
- (2) Put the downloaded third-party library file or its source code file into the *src* directory created in the first step
- (3) Open the *Androdi.mk* file under the path *frameworks/base*, and add a new line “`../external/<your - dir >/src`” after the definition of the variable *ext_dirs*
- (4) Recompile Android source code or directly execute the “`mmmframeworks/base`” command to complete the integration of the third-party libraries

After integrating the third-party library into the Android system, the interface and function provided by the library file can be called directly in the Android framework code. In this paper, it is necessary to filter the metadata of sound signals at high frequency after the microphone obtains the metadata, to prevent the upper application from using the metadata through *MediaRecorder* or *AudioRecorder* interface. Through the detailed analysis of Android source code, it is found that

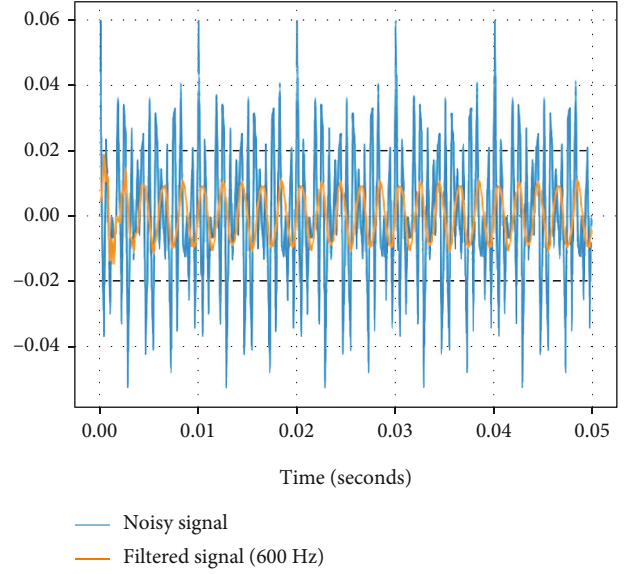


FIGURE 6: Working effect of band-stop filter.

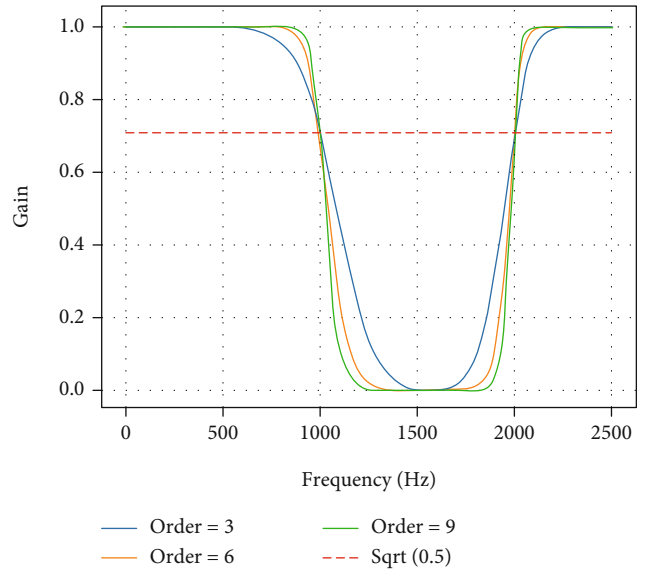


FIGURE 7: Influence of band-stop filters of different order on frequency attenuation speed.

both the *MediaRecorder* and *AudioRecorder* interfaces need to acquire sound signal data through the *AudioRecorder* interface [34] in the framework layer. Therefore, by customizing the interface, users can configure corresponding policies according to their needs, to dynamically control the high-frequency filtering of audio signal metadata.

5. Acoustic Covert Communication Based on Normal Frequency

In this section, we study the feasibility of the acoustic covert communication based on normal frequency and reveal that imperceptible acoustic covert communication in the normal

frequency band can pose threats to users' privacy. We further put forward countermeasures to mitigate the threats. The prototype system of acoustic covert communication using the normal frequency faces four challenges: how to determine the available normal frequency bandwidth for information modulation, which carrier modulation scheme to be selected for information modulation, how to select the appropriate insertion point in normal audio to synthesize with special signals, and how to eliminate the sound and other noises of normal frequency signals so as not to arouse users' doubts.

5.1. Available Normal Frequency Bandwidth. Normal frequency is used as the carrier frequency for information modulation. Other factors, such as human ear perception, equipment capability, and environmental noise, are considered. The core functional organ of the human auditory perception system [35] is the human ear. Because of the special structure of the human ear, human beings have different sensitivity to sound signals at different frequencies. The typical audible frequency range of human beings is between 20 Hz and 20 kHz. Most people's auditory systems are insensitive to frequencies above 18 kHz. They are the most sensitive to sounds in the frequency range from 300 Hz to 4 kHz, which is also the frequency range of human speech sounds.

Extremely low signal energy can be perceived by human beings. The response frequency of microphones and speakers in smart mobile devices to sound signals is below 20 kHz. In addition, the frequencies of various noises are generally below 9 kHz. In this sense, it is reasonable to select carrier signals above 9 kHz to reduce the interference of environmental noises to carrier signals based on normal frequencies. According to the above factors, within the normal frequency range that humans can hear, the frequency suitable for acoustic covert communication ranges from 9 kHz to 18 kHz.

5.2. Selection of Modulation Technology. When sound wave is used as carrier to transmit information, the first problem to be considered is how to encode information (i.e., baseband signal); that is, information is modulated into the sound signal. Given the commonality between acoustic wave and electromagnetic wave, the modulation and demodulation techniques in electromagnetic wave communications can be applied to acoustic wave communications. In this paper, the FSK modulation is selected to implement the prototype system of the normal frequency-based acoustic covert communication.

5.3. Selecting the Insertion Point of the Carrier Signal. To realize acoustic covert communication using normal audio, it is necessary to modulate the covert information to generate signals at the carrier frequency. The covert information is synthesized with normal audio to reduce the possibility of the covert signals arousing the users' suspicions. We assume that the length of the signals is much shorter than the duration of normal audio. In order to find a suitable insertion point in the normal audio to synthesize the signals, the amplitude of the normal audio is analyzed to find the part with the strongest energy to place the signal. As shown in Figure 8, energy

analysis is performed on the normal audio to simplify the implementation. The Python library `pydub` [36] is used to obtain the energy value of sound signals, and the part of the audio with the largest average energy is found. The covert signals are inserted from the start of the part of the audio.

5.4. Elimination of Sound and Other Noise of Special Signal. Because the carrier frequency of the covert signals is within the audible normal frequency range, it can produce audible noises. According to the masking effect of sound [37], we further process the signals to reduce the audible noises. The masking effect of sound [37] refers to the phenomenon that when masking sound and masked sound are played at the same time, the hearing threshold of masked sound increases due to the existence of the masking sound, and users can only perceive the existence of the masking sound. There are two typical types of masking techniques: frequency-domain masking and temporal-domain masking.

Frequency-domain masking enables sounds with different frequencies to mask each other. The basic rules are that low frequency signals mask high-frequency signals and strong sound masks weak sound. It is difficult to accurately calculate how much the energy of the masked sound is lower than that of the masking sound. When there is a big difference between two frequencies, it is impossible to mask completely. Some researchers put forward a calculation model [38], which roughly estimates the critical value of the masked sound (i.e., the covert signals), provided the knowledge of the energy intensity of the masked sound (i.e., the normal audio). In this paper, the critical value is evaluated and used as the decibel number of the masked sound.

Temporal-domain masking is constituted of premasking and postmasking, according to the time sequence of masking sound and masked sound. In premasking, masking sound is emitted first, followed by the masked sound (within 200 ms). In postmasking, the masking sound is emitted after the masked sound (within 50 ms). The masking effect is achieved within the corresponding time interval. Because the insertion point of the covert signals is within the normal audio frequency, temporal-domain masking can reduce the noises perceptible to the users.

When the carrier frequency is synthesized with normal audio frequency, the sharp change of frequency causes the raised tip in the sound wave or the discontinuity of the sound wave in a short time. This can make the noise easily perceivable to the users. In order to eliminate this influence, the signal at the insertion point can be faded in and out by using Sigmoid function [39]; that is, the signal strength of the normal audio is zero for a short time, and the strength of the covert signal increases from 0 to the normal value, as shown in Figure 9. In this way, the noise caused by the convex tip in the sound wave or the discontinuity of the sound wave in a short time can be eliminated.

6. Implementation of Prototype System

Based on the above analysis, we design a prototype system of acoustic covert communication based on normal audio

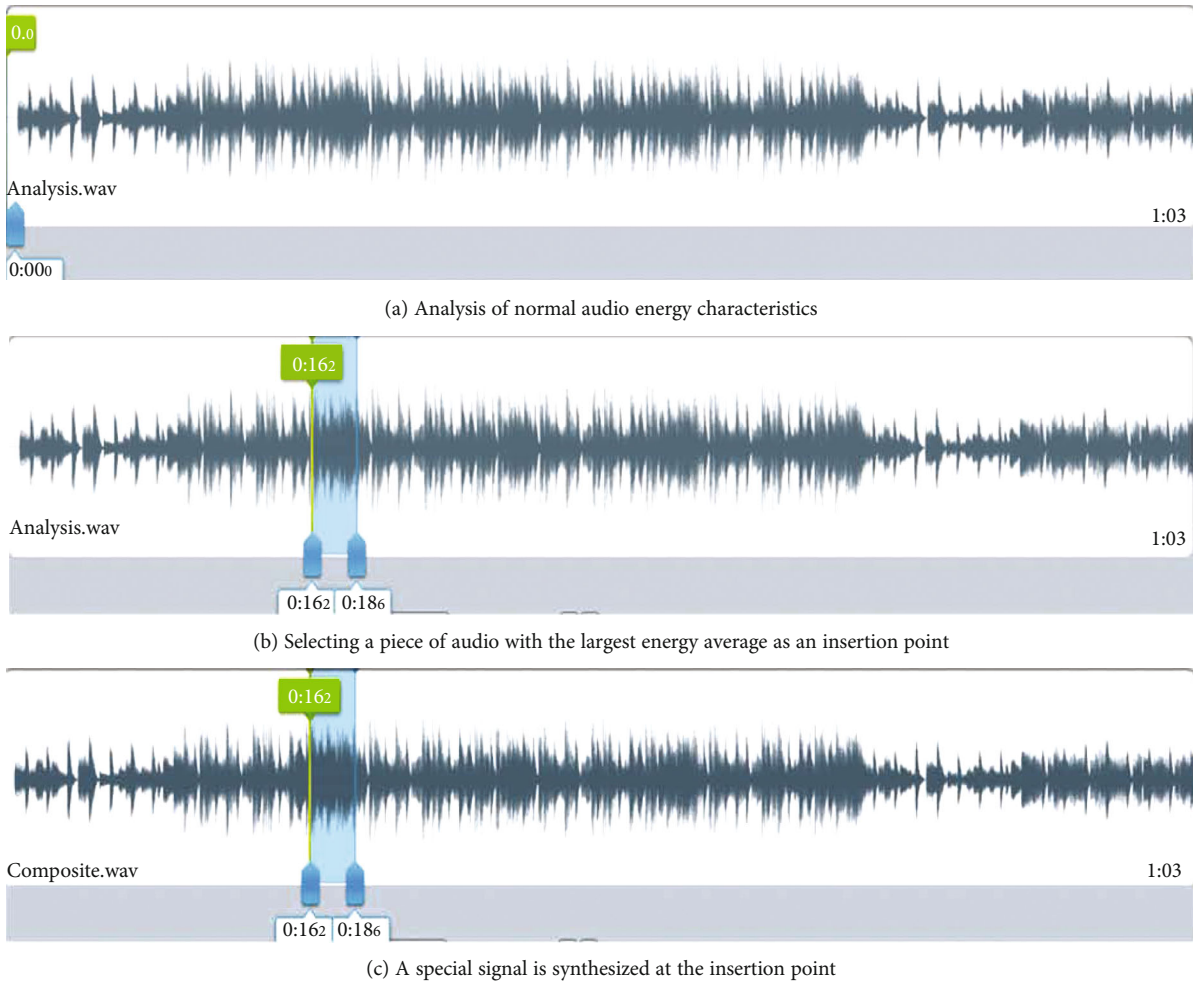


FIGURE 8: Analysis of normal audio energy characteristics and selection of insertion points for special signal synthesis.

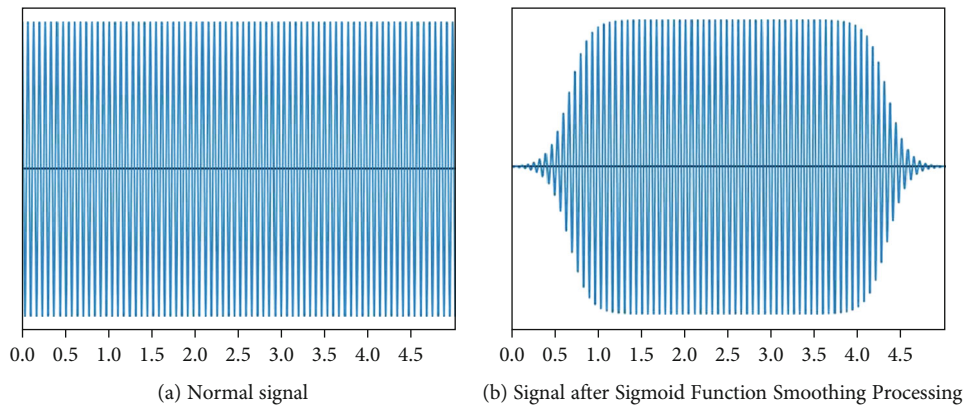


FIGURE 9: Smooth processing of sound signal to eliminate noise.

frequency, in which frequencies are selected from 9 kHz to 18 kHz. The system architecture is shown in Figure 10.

The prototype system is developed for Android version 6.0 system, and the selected frequency range is from 12 kHz to 14 kHz. Because the main purpose of this paper is to verify the feasibility of normal audio-based acoustic covert communication, the system bit rate and other per-

formance are not specially treated. 16-FSK modulation is used to modulate information. Each symbol has a duration of 0.1 s to transmit 80 bits. The synchronization signal is a chirp signal from the start frequency to the end frequency and has a length of 2 symbols. The signal synchronization between the sender and receiver is accomplished by using matched filters [40, 41].

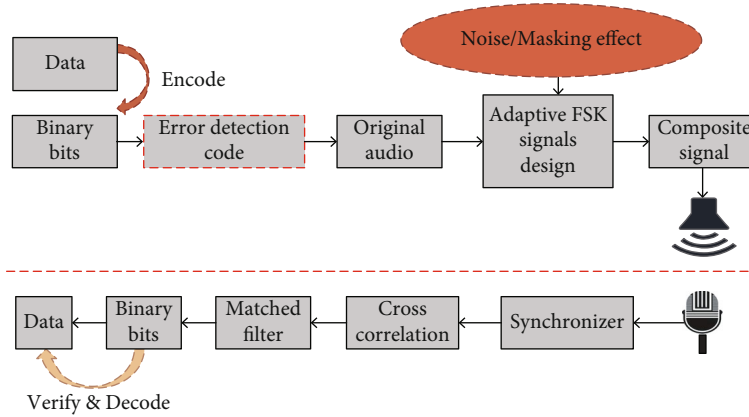


FIGURE 10: Prototype system architecture.

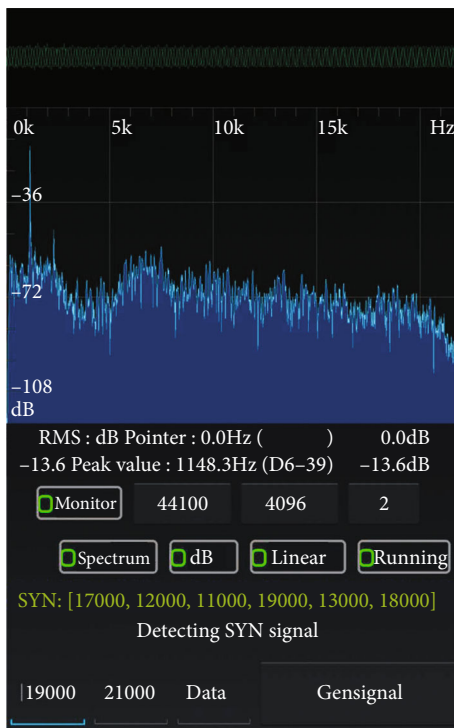


FIGURE 11: A prototype system of acoustic covert communication based on normal audio frequency.

Our prototype of normal frequency-based acoustic covert communication is shown in Figure 11. The overall framework of the prototype program is based on open source projects (<https://github.com/bewantbe/audio-analyzer-for-android>).

7. Function Test and Performance Analysis

In this section, we first design experiments to test the function and performance of the security model based on high-frequency filtering and the prototype system of normal audio-based acoustic covert communication. Then, the experimental results are discussed. Finally, we analyze the impact of this work on the execution performance of mobile smart phones.

7.1. Security Model Test with Acoustic High-Frequency Filtering. In order to increase the reliability of the experimental results, we first integrate the prototype system of security model based on high-frequency filtering into Android 6.0 version system. Then, we transplant the customized Android system (ROM) to Xiaomi 4 mobile phone for testing. The operation steps and related documents of Android source code compilation, ROM customization, and ROM transplantation to new devices involved in this paper were obtained from the relevant URLs [42].

7.1.1. Function Testing. The proposed security model based on acoustic high-frequency filtering is aimed at a specific context (i.e., visiting anonymous networks). Attackers use high-frequency signals above 18 kHz, which cannot be perceived by users and hidden in normal audio, to conduct covert acoustic communication and obtain users' private information (de-anonymization). To test the prototype system, we randomly select a music file and insert high-frequency covert signals and test the prototype system by observing the temporal domain, frequency domain, and spectrum characteristics of sound signals in three objects received by an Android device and filtered by the Android system 14. The three objects are the original file, the synthesized file, and the audio file. As shown in Figure 12, the prototype system successfully blocks the propagation of high-frequency signals (greater than 18 kHz) and effectively eliminates the temporal-domain, frequency-domain, and spectrum characteristics of the covert signals.

7.1.2. Performance Test. Because the security model based on high-frequency filtering is implemented in the framework layer of Android systems, the new band-stop filter filtering the metadata of received audio signals is consistent with the design purpose. As compared with the workflow of sound signal processing in the traditional Android system, the additional step of filtering metadata at high frequency can bring time delay for applications to use microphones. In order to test whether the delay has any impact on the operation of the applications, a recording application is issued separately, and the time consumed by the application to obtain sound signals through microphone in normal Android system and

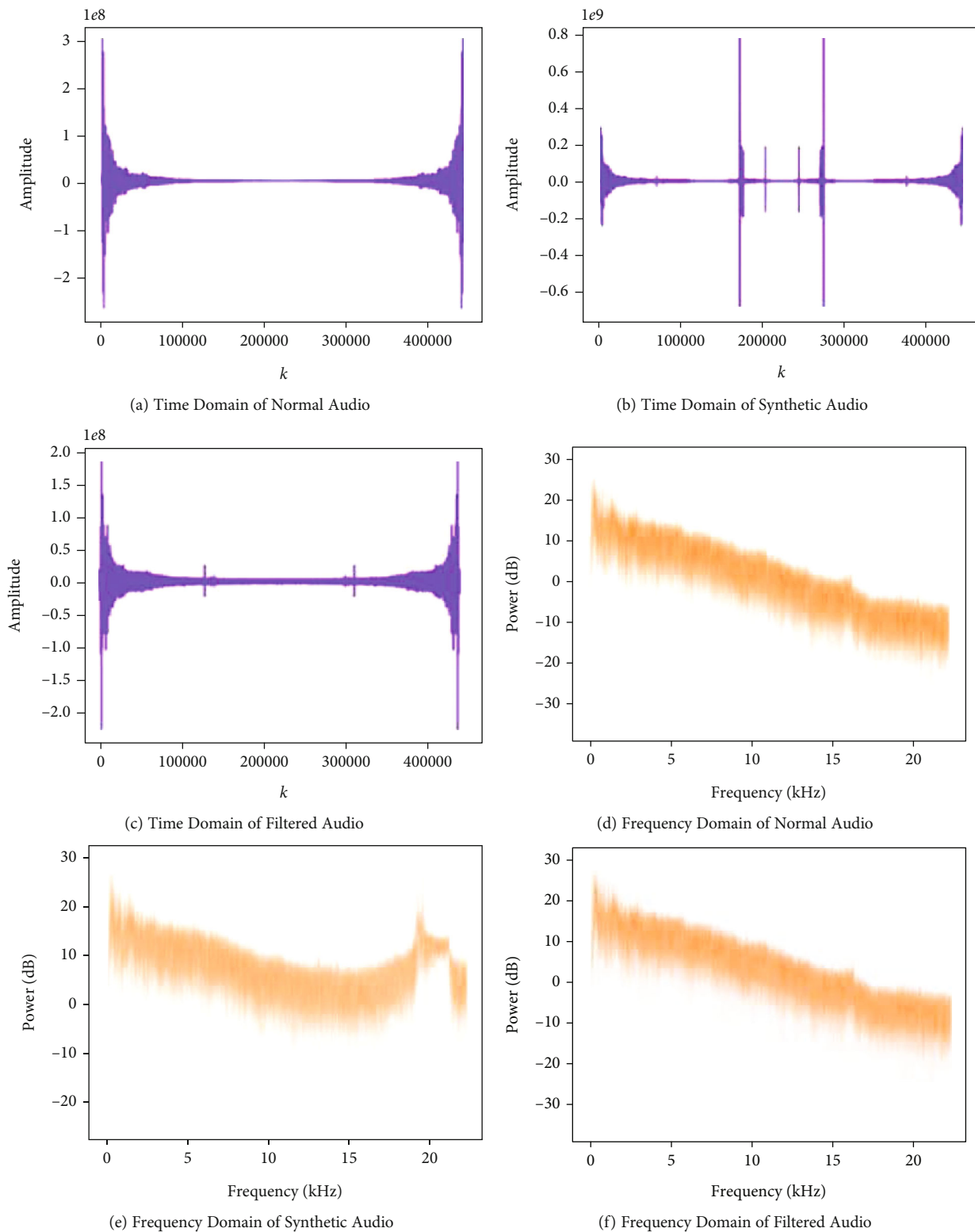


FIGURE 12: Continued.

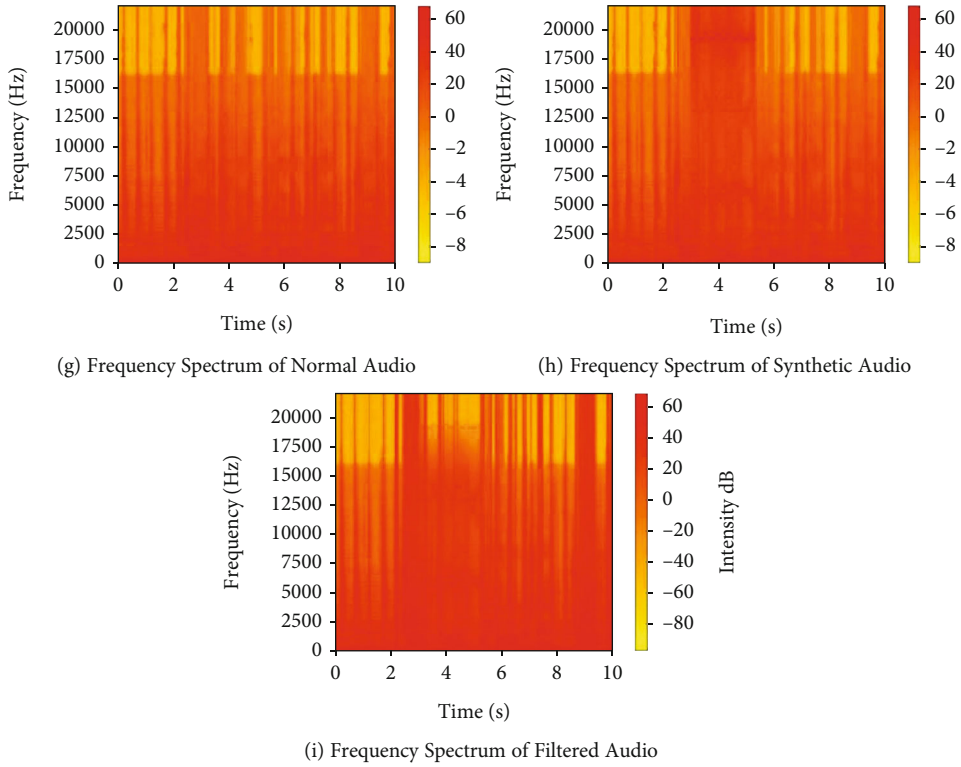


FIGURE 12: Functional test of security model based on high-frequency filtering.

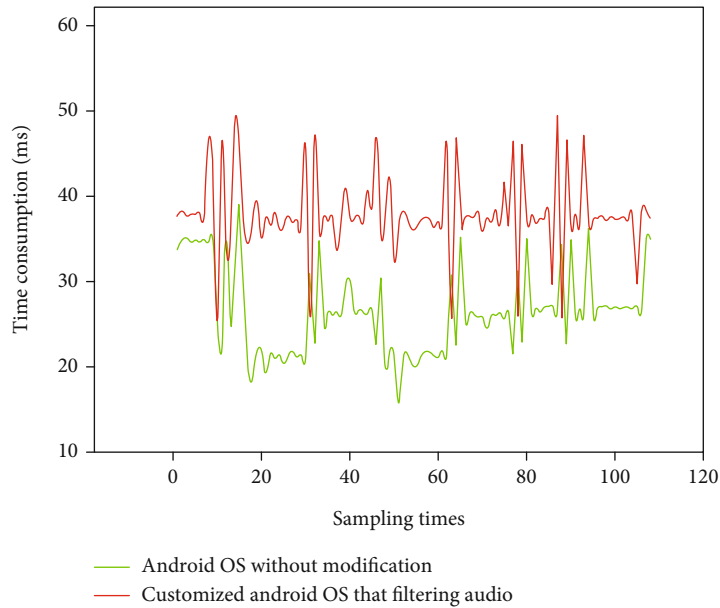


FIGURE 13: Performance test of the security model based on high-frequency filtering.

customized Android system (with high-frequency filtering function) is recorded by way of log. A comparison study is provided in Figure 13, which shows that the prototype system of the proposed security model only adds less than 20 ms delay, and meets the typical use requirements of protecting users’ personal information from malicious theft.

7.2. *Prototype System of Normal Frequency-Based Acoustic Covert Communication.* This section tests the function and performance of normal frequency-based acoustic covert communication proposed in this paper. The receiver is tested comprehensively, and the sender is responsible for playing out the synthesized audio. The key functions and

performances tested include the detection accuracy, the detection time/delay, and the evaluation of whether the user can perceive the covert signals in the audio.

7.2.1. Testing of Detection Accuracy. Two groups of comparative experiments are designed to test the detection accuracy of the prototype system in different environments. We fix the sound source (i.e., the equipment playing synthetic audio, such as PC) at one place and adjust the distance of the smart phone with the prototype application installed to the sound source: 0 m, 1 m, 2 m, 3 m, 4 m, and 5 m, so as to test the actual detection performance of the prototype system in various scenes at different distances. The prototype application is installed in Xiaomi 4 mobile phones, and the sound playing decibel value of the sound source is 70 dB.

The experimental results are shown in Figure 14. When the prototype system is in a noisy environment, due to the interference of environmental noise, the actual performance of receiving and detecting the covert signals decreases, and the detection accuracy also degrades with the increasing distance between the receiver and sound source. However, when the distance of the sound source and receiver is within 3 meters, the accuracy can still reach about 90%. The feasibility of using normal frequency as the carrier frequency to modulate covert information is verified.

7.2.2. Time Load Test. In the process of detecting covert signals in environmental sounds, a Xiaomi 4 mobile phone is used. There are three functional modules that need to perform calculations and introduce delays in the prototype application installed in the smart phone, namely, synchronous signal detection, original special signal recovery, and demodulation of covert information from covert signals. When the prototype application executes the detection task, the time consumed by each functional module is recorded in the form of log. The average time consumption of each functional module is shown in Table 1.

In Table 1, we can see that the prototype system consumes less than 1 millisecond when detecting the synchronization signal (chirp signal from the start frequency to the end frequency and with a length of 2 symbols) of the received sound signals. The reason is because the sender and receiver negotiated the format of the synchronization signal in advance, and the receiver only needs to apply a matched filter to the metadata of the received sound signal to complete the synchronization operation. The time consumption is short. In contrast, the recovery and demodulation functions take much longer, but they are still within the acceptable range (i.e., less than 2 seconds).

7.2.3. Concealment Satisfaction of Covert Communication. The core function of acoustic covert communication is to realize covert communication without arousing users' suspicion. In this paper, normal frequency is used as the carrier frequency to modulate the covert information. Because the frequency of the modulated signals is within the auditory range of the human ears, users can notice the signals. In order to reduce the perceivability of the covert signals and other noises at the users, the masking effect of sound is used to fade

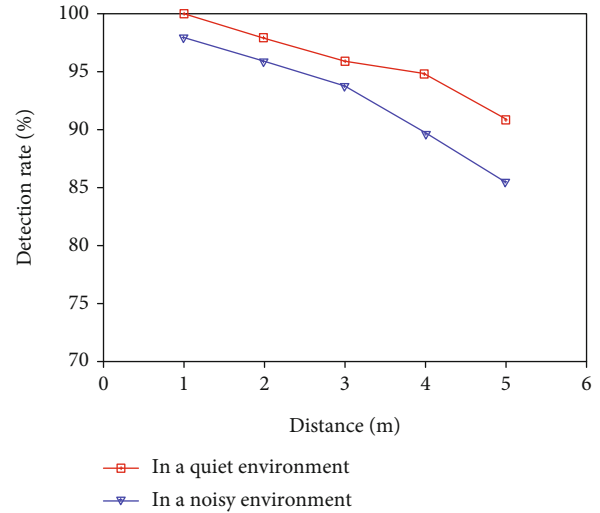


FIGURE 14: Testing accuracy of the acoustic covert communication based on normal frequency.

in and out the covert signals and normal audio insertion point signals.

Fifty volunteers, aged between 20 and 50, participated in our satisfaction survey experiment. The participants (or users) were randomly divided into two groups A and B, with 25 people in each group. Those in group A were unaware of the existence of covert signals in the played audio files. Those in group B were informed that the audio files could be synthesized with covert signals before the audio files were played to them. In order to help the volunteers evaluate the quality of synthesized audio, four scores were set in this experiment: (1) 4 points, if no abnormality can be perceived; (2) 3 points, if it is difficult to perceive abnormal sounds unless extra attention is paid; (3) 2 points, if abnormality is perceived in the synthesized audio file without paying extra attention, but does not arouse suspicion; and (4) 1 point, if there are obvious abnormal noises arousing the user's suspicion. In addition, the experiment selects three types of audio as normal audio, i.e., light music (blues, country and folk, etc.), heavy metal music (electronic, rock, and metal), and human voice (advertisement and conversation), to assess whether different types of normal audio have impact on the perception of covert signals in the synthesized audio. These music files are free resources published on the Internet [43].

To obtain accurate feedback from the participants, we develop a satisfaction survey platform, as shown in Figure 15. By randomly generating and arranging normal audio and synthesized audio in each group of music, the interaction between participants is reduced. For example, when a participant P1 enters the blues music interface for the first time, the music labeled "Audio1" may be normal audio, but when P1 enters this page again or other participants enter the blues page, "Audio1" may be a synthesized audio. According to the experimental results in Figure 16, heavy metal music has higher high-frequency signal energy, and the covert sound signals can be well masked.

The experimental results of group B show that the users with a priori knowledge were particularly sensitive to

TABLE 1: Time load test results of prototype system.

Functional module	Synchronous signal detection	Special signal recovery	Demodulate special signals
Time consumption (milliseconds)	0.81	1063	431

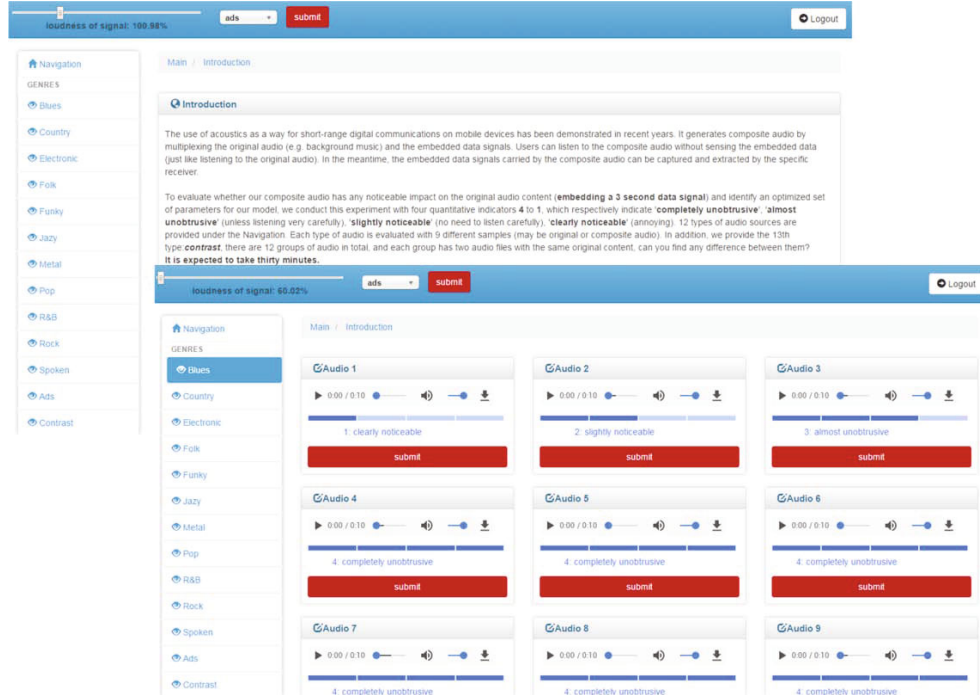


FIGURE 15: Covert satisfaction research platform.

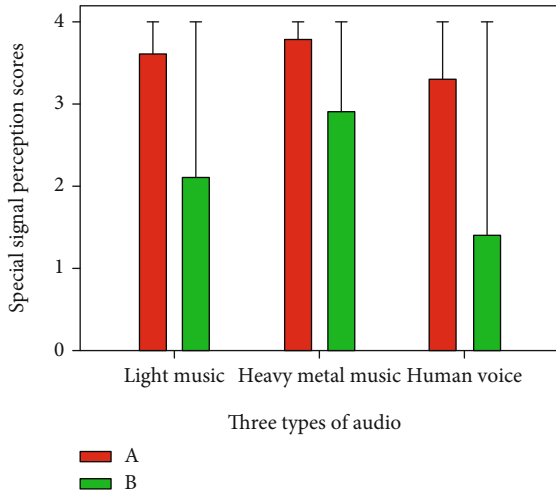


FIGURE 16: Investigation results of concealment satisfaction.

abnormal noises in the sound. However, if a user was not given the knowledge in advance, the noise caused by the covert signals was not easily perceivable. In most cases, it was considered as a short-term failure of the audio file or the playback device.

Based on the above analysis, acoustic covert communication based on normal frequency is feasible, and for ordinary

users, it has the same or similar privacy threat as that based on high-frequency signals. Therefore, when users perform anonymous operations in a specific context, the mechanism based on high-frequency filtering can not cope with this attack. It is necessary to set up additional resource usage policies to control the application programs using microphones and speakers.

8. Conclusions

Applications conducting covert communication based on high-frequency sound waves threat users' privacy. We proposed a new security mechanism which uses high-frequency filtering to erase inaudible near-ultrasonic covert signals. We revealed that acoustic covert communication imperceptible to users in the normal frequency band is also threat. Two prototype systems were developed for the new security model and the normal-frequency acoustic covert communication. Their functions and performance were experimentally evaluated.

Despite the new security model can address the current privacy threats, our new study indicates that the normal frequency-based acoustic covert communication cannot be addressed by the model or other existing techniques. Our future work will focus on how to effectively detect the covert signals in audible normal frequency bands.

Data Availability

Previously reported data were used to support this study and are available at [\url{https://github.com/bewantbe/audio-analyzer-for-android.}}](https://github.com/bewantbe/audio-analyzer-for-android).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grant No. 61902021, the Beijing Natural Science Foundation under Grant 4212008, the Open Foundation of State key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications) under Grant SKLNST-2019-2-08, the National Natural Science Foundation of China under Grant No. 61802118, and the Natural Science Foundation of Heilongjiang Province under Grant No.YQ2020F013.

References

- [1] Sophos, “Users weighed down by multiple gadgets and mobile devices [EB/OL],” 2013, <https://www.sophos.com/en-us/press-office/pressreleases/2013/03/mobile-security-survey.aspx>.
- [2] P. Samangouei, V. M. Patel, and R. Chellappa, “Attribute-based continuous user authentication on mobile devices,” in *Proceedings of the 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–8, Arlington, VA, USA, 2015.
- [3] Silverpush, “Artificial intelligence powered context detection marketing [EB/OL],” 2018, <https://www.silverpush.co/>.
- [4] Z. Liu, J. Liu, Y. Zeng, and J. Ma, “Covert wireless communication in IoT network: from AWGN channel to THz Band,” *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3378–3388, 2020.
- [5] D. McCoy, K. Bauer, D. Grunwald, T. Kohno, and D. Sicker, “Shining light in dark places: understanding the Tor network,” in *Privacy Enhancing Technologies*, pp. 63–76, Springer, Berlin, Heidelberg, 2008.
- [6] C. Marforio, A. Francillon, and S. Capkun, *Application Collusion Attack on the Permission-Based Security Model and its Implications for Modern Smartphone Systems*, ETH Zurich, 2011.
- [7] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, “DolphinAttack: inaudible voice commands,” in *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security (CCS '17)*, pp. 103–117, New York, NY, USA, 2017.
- [8] Forbes, “Voice assistants: this is what the future of technology looks like [EB/OL],” 2017, <https://www.forbes.com/sites/herbertsim/2017/11/01/voice-assistants-this-is-what-the-future-of-technology-looks-like/#7a2e4546523a>.
- [9] V. Mavroudis, S. Hao, Y. Fratantonio, F. Maggi, C. Kruegel, and G. Vigna, “On the privacy and security of the ultrasound ecosystem,” *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 2, pp. 95–112, 2017.
- [10] N. F. Johnson and S. Jajodia, “Exploring steganography: seeing the unseen,” *Computer*, vol. 31, no. 2, pp. 26–34, 1998.
- [11] D. Kahn, “The history of steganography,” *Proceedings of the International Workshop on Information Hiding*, pp. 1–5, Springer, Berlin, Heidelberg, 1996.
- [12] J. C. Judge, *Steganography: Past, Present, Future*, Lawrence Livermore National Lab., CA (US), 2001.
- [13] K. Gopalan, “Audio steganography using bit modification,” in *Proceedings of the International Conference on Multimedia and Expo. ICME'03. Proceedings (Cat. No. 03TH8698)*, vol. 1, pp. 1–629, Hong Kong, China, 2003.
- [14] N. Cvejic and T. Seppanen, “Increasing the capacity of LSB-based audio steganography,” in *Proceedings fo the IEEE Workshop on Multimedia Signal Processing*, pp. 336–338, St. Thomas, VI, USA, 2002.
- [15] P. Jayaram, H. R. Ranganatha, and H. S. Anupama, “Information hiding using audio steganography - a survey,” *The International Journal of Multimedia & Its Applications*, vol. 3, no. 3, pp. 86–96, 2011.
- [16] M. Zamani, A. Manaf, R. B. Ahmad, F. Jaryani, H. Taherdoost, and A. M. Zeki, “A secure audio steganography approach,” in *Proceedings of the 2009 International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 1–6, London, UK, 2009.
- [17] C. Alain, S. R. Arnott, S. Hevenor, S. Graham, and C. L. Grady, ““What” and “where” in the human auditory system,” *Proceedings of the National Academy of Sciences*, vol. 98, no. 21, pp. 12301–12306, 2001.
- [18] A. Chadha and N. Satam, “An efficient method for image and audio steganography using Least Significant Bit (LSB) substitution,” 2013, <https://arxiv.org/abs/1311.1083>.
- [19] N. Cvejic and T. Seppanen, “A wavelet domain LSB insertion algorithm for high capacity audio steganography,” in *Proceedings of 10th Digital Signal Processing Workshop, 2002 and the 2nd Signal Processing Education Workshop*, pp. 53–55, Pine Mountain, GA, USA, 2002.
- [20] F. Djebbar, B. Ayad, K. A. Meraim, and H. Hamam, “Comparative study of digital audio steganography techniques,” *EURASIP Journal on Audio, Speech, and Music Processing*, vol. 2012, no. 1, 2012.
- [21] D. Yu and L. Deng, *Automatic Speech Recognition*, Springer London limited, 2016.
- [22] S. M. Moosavi-Dezfooli, A. Fawzi, and P. Frossard, “Deepfool: a simple and accurate method to fool deep neural networks,” in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 2574–2582, Las Vegas, NV, USA, 2016.
- [23] N. Carlini, P. Mishra, T. Vaidya et al., “Hidden voice commands,” in *Proceedings of the 25th USENIX Security Symposium (USENIX Security 16)*, pp. 513–530, Austin, TX, USA, 2016.
- [24] X. Lei, G.-H. Tu, A. X. Liu, K. Ali, C.-Y. Li, and T. Xie, “The insecurity of home digital voice assistants—Amazon Alexa as a case study,” 2017, <https://arxiv.org/abs/1712.03327>.
- [25] L. Schönherr, K. Kohls, S. Zeiler, T. Holz, and D. Kolossa, “Adversarial attacks against automatic speech recognition systems via psychoacoustic hiding,” 2018, <https://arxiv.org/abs/1808.05665>.
- [26] N. Carlini, “Audio adversarial examples [EB/OL],” 2018, https://nicholas.carlini.com/code/audio_adversarial_examples.

- [27] N. Z. Gong, A. Ozen, Y. Wu et al., "Piano: proximity-based user authentication on voice-powered internet-of-things devices," in *Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pp. 2212–2219, Atlanta, GA, USA, 2017.
- [28] B. Zhang, Q. Zhan, S. Chen et al., "PriWhisper: enabling key-less secure acoustic communication for smartphones," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 33–45, 2014.
- [29] S. Yi, Z. Qin, N. Carter, and Q. Li, "WearLock: unlocking your phone via acoustics using smartwatch," in *Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pp. 469–479, Atlanta, GA, USA, 2017.
- [30] G. Play, "Shopkick: shopping, rewards and deals [EB/OL]," 2019, https://play.google.com/store/apps/details?id=com.shopkick.app&hl=en_US.
- [31] M. K. Mandal and P. Mondal, "Design of sharp-rejection, compact, wideband bandstop filters," *IET Microwaves, Antennas and Propagation*, vol. 2, no. 4, pp. 389–393, 2008.
- [32] I. W. Selesnick and C. S. Burrus, "Generalized digital Butterworth filter design," *IEEE Transactions on Signal Processing*, vol. 46, no. 6, pp. 1688–1694, 1998.
- [33] Source-Code, "A collection of java classes for digital signal processing [EB/OL]," 2018, <http://www.source-code.biz/dsp/java/>.
- [34] AndroidXRef, "Android source code cross reference: AndroidRecord [EB/OL]," 2018, http://androidxref.com/9.0.0_r3/xref/frameworks/base/media/java/android/media/AudioRecord.java#native_read_in_short_array.
- [35] E. Zwicker and U. T. Zwicker, "Audio engineering and psychoacoustics: matching signals to the final receiver, the human auditory system," *Journal of the Audio Engineering Society*, vol. 39, no. 3, pp. 115–126, 1991.
- [36] "pydub [OL]," <https://pypi.org/project/pydub/>.
- [37] Y. C. Tung and K. G. Shin, "Exploiting sound masking for audio privacy in smartphones," in *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, pp. 257–268, New York, NY, USA, 2019.
- [38] "Decibels calculation [OL]," <http://hyperphysics.phy-astr.gsu.edu/hbase/Sound/db.html>.
- [39] "Sigmoid function [OL]," <https://mathworld.wolfram.com/SigmoidFunction.html>.
- [40] K. Suzuki, "Digital matched filter," 1999, US Patent 5–903595.
- [41] C. E. Wheatley III and J. E. Maloney, "Method and apparatus for pilot search using a matched filter," 2004, US Patent 6–760366.
- [42] "Build lineageos ROM [OL]," 2017, <https://www.lineageosrom.com/2017/01/how-to-build-lineageos-rom-for-any.html>.
- [43] "Free music archive [OL]," <http://freemusicarchive.org/>.

Research Article

A Blind Signature-Aided Privacy-Preserving Power Request Scheme for Smart Grid

Weijian Zhang,¹ Zhimin Guo,² Nuannuan Li,² Mingyan Li ,² Qing Fan,³ and Min Luo ³

¹State Grid Henan Electric Power Company, Zhengzhou, China

²State Grid Henan Electric Power Research Institute, Zhengzhou, China

³Wuhan Lianweitu Software Co., Ltd., Wuhan, China

Correspondence should be addressed to Mingyan Li; limingyan@stu.xjtu.edu.cn

Received 22 March 2021; Revised 4 May 2021; Accepted 6 June 2021; Published 1 July 2021

Academic Editor: Ding Wang

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

Smart grid is an emerging power system capable of providing appropriate electricity generation and distribution adjustments in the two-way communication mode. However, privacy preservation is a critical issue in the power request system since malicious adversaries could obtain users' daily schedule through power transmission channel. Blind signature is an effective method of hiding users' private information. In this paper, we propose an untraceable blind signature scheme under the reputable modification digital signature algorithm (MDSA). Moreover, we put forward an improved credential-based power request system architecture integrated with the proposed blind signature. In addition, we prove our blind signature's blindness and unforgeability under the assumption of Elliptic Curve Discrete Logarithm Problem (ECDLP). Meanwhile, we analyze privacy preservation, unforgeability, untraceability, and verifiability of the proposed scheme. Computational cost analysis demonstrates that our scheme has better efficiency compared with other two blind signatures.

1. Introduction

The concept of "Intelligrid" is first proposed by the American Electric Power Research Institute in 2001 [1], and exploration of smart grid is becoming more and more popular. Since the notion of industry 4.0 is put forward, operation and management of smart grid are optimized through connection of various facilities, equipment, and devices [2]. Smart grid is regarded as the next-generation power grid infrastructure capable of promoting secure and effective electricity transmission from power operators to electric appliance. Power operation and management in smart grid are upgraded by integrating advanced bidirectional communications and widespread computing capabilities for efficient control, distribution, reliability, and safety [3]. Smart grid not only eliminates barriers between users and power producers but also ensures continuous electricity supply for users due to intelligently monitoring electricity consumption behaviour of users to realize suitable adjustments in the amount of power deployment [4].

In general, a smart grid network is roughly comprised of three layers: control center, substations, and smart appliances (i.e., smart meters) [5]. Figure 1 depicts a simplified architecture of the smart grid network. As a kind of physical carrier, smart meters are installed in each electricity appliance system and users could send power request to substation with the help of smart meters. Moreover, smart meters will push appliance information to substations periodically. Substations could collect users' real-time demand and forward it to the control center via the Supervisory Control and Data Acquisition (SCADA) system [6, 7]. Then, the power control center will make further power deployment analysis and distribute proper electricity amount to substations as various requirements. Finally, users could obtain the required electricity through substations.

It should be noted that the major differences between traditional power network and smart grid are that smart meters bearing users' application information communicate with substations via wired or wireless networks. Specifically, one of the main information is the users' real-time electricity

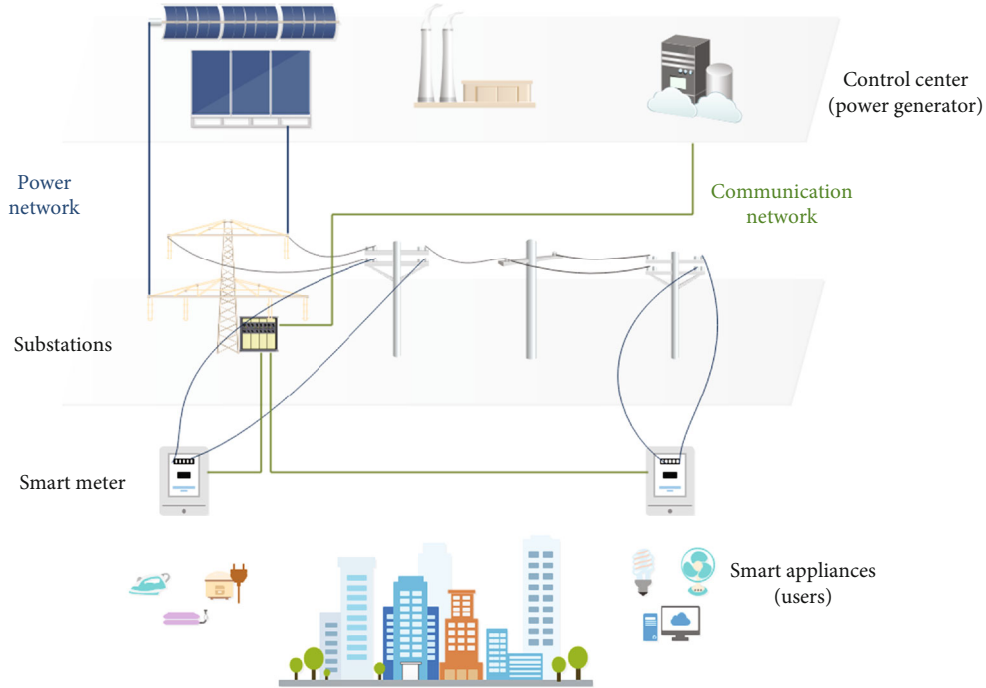


FIGURE 1: Model of the smart grid.

consumption and demands. Due to the power request which has the potential of leaking users' daily schedule, which is private, we devote to the privacy and security issues of electricity request communication. Furthermore, power demands are not only related to users' privacy directly but also related to the charging policy and fairness. How to take effective measures to guarantee genuineness of power demand sources and the user's privacy is a significant issue. The former problem could be solved by identity authentication, and the latter needs privacy preservation techniques to be settled [8].

The digital signature is an important cryptographic protocol for ensuring the authenticity and the integrity of messages [9–11]. The blind signature is a special digital signature, which is an effective method for user's privacy preservation. The pioneer of blind signature conception is from Chaum et al.'s research [12], in which they established a user's privacy-preserved electric payment system based on blind signature. The blind digital signature generation process contains two parties: a signer \mathcal{S} and a user \mathcal{U} . On receiving a blind signature request from a user \mathcal{U} , the signer \mathcal{S} generates a random element and sends it to \mathcal{U} . Then, the user utilizes received element and produced blind factors to blind the original message m . The blinded message denoted by \tilde{m} is sent to \mathcal{S} . Actually, \mathcal{S} signs \tilde{m} as a secure signature scheme. Finally, \mathcal{U} unblinded signature values from \mathcal{S} to obtain the ultimate blind signature. In the above process, \mathcal{S} cannot recognize the real signing message even if he saves all the signature scripts that he has signed. The unmatchability between output of blind signature and signer's signature scripts is viewed as untraceability.

Amounts of blind signature schemes have been proposed [13–19], but they cannot hold untraceability, where the signer \mathcal{S} can find a match between his signature scripts and

blind signature outputs. Thus, \mathcal{S} can distinguish the original message he has signed and privacy of user could not be ensured. In this paper, we improved Bütün and Demirer's scheme and proposed a secure blind signature. Based on the advanced blind signature, we put forward a power request system model. Contributions of this paper are as follows:

- (i) We put forward an improved blind signature-aided power request privacy preservation system model, in which smart meters (i.e., users) could send power request, a blindly signed credential with a certain amount, to substations, and the control center cannot identify the real user identity through blind signature verification
- (ii) We analyze Bütün and Demirer's scheme and point out its weakness, that is a malicious signer could find a match message between his signing scripts and user's blind signature outputs
- (iii) We propose a secure blind signature scheme under the reputable MDSA digital signature. What is more, blindness and unforgeability of our proposed blind signature are proved under difficulty assumption of ECDLP

1.1. Organizations of This Paper. Some works related to blind signature and smart grid privacy preservation are described in Section 2. Section 3 are preliminaries of this paper, which introduces our proposed system model, fundamental knowledge, definition of blind signature, and security model of blind signature. In Section 4, we review Bütün and Demirer's scheme. Then, we point out the linkability attack on the reviewed scheme in Section 5, that is, a signer can find an

original message he has signed. In Section 6, we proposed our improved blind signature with untraceability. In Section 7, we prove our scheme's blindness and unforgeability and analyze properties of privacy preservation, unforgeability, untraceability, and verifiability. Section 8 gives comparisons of security properties and computational costs with Bütün and Demirel's scheme [13] and Verma and Singh's scheme [16].

2. Related Works

Since the advent of "smart grid" concept, a flow of smart grid surveys has sprung up [3, 20–26]. Fang et al. explore three major systems and gave the future expectations for smart grid [20]. This paper has an important reference value for the following smart grid survey. Alshehri gives further research for smart grid and studied multiperiod demand response management [21]. Wen et al. [25] and Makhadmeh et al. [26], respectively, conducted researches on smart meters and smart homes. However, some sensitive information of users may leak through the two-way communication channel. Therefore, privacy preservation is especially significant.

Si et al. analyze the existing privacy problems and enumerate some solutions from a global perspective for smart grid [27]. Mahmood et al. propose an elliptic curve-based authentication to provide communication security between customers and substations [28]. Blind signature is an effective way of hiding users' sensitive information and first proposed by Camenisch et al. [29]. Blind signature could guarantee anonymity of participants. Tseng put forward a specific privacy-preserving communication protocol utilizing the restrictive partially blind signature [30]. Sarde and Banerjee propose an incentive-based demand response privacy-preserving scheme for the smart grid [14]. Yang et al. make an attempt to identify the privacy-preserving issues and put forward a reward architecture for V2G networks [31]. Yu et al. propose a power request scheme to satisfy the security requirements [32]. Han and Xiao give a thorough and deep survey on the privacy preservation for smart grid and point out that the blind signature is a universal method for users' security issues [33], but they do not give a detailed blind signature based privacy preservation scheme.

In conclusion, the above papers have great effects on the smart grid privacy preservation research. But they either give a general description or lack of a comprehensive blind signature scheme. In this paper, we proposed an integrated blind signature-aided privacy-preserving power request scheme for smart grid.

3. Preliminaries

In this section, we introduce the system model, fundamental knowledge, definition of blind signature, and security model of blind signature.

3.1. The System Model. In this subsection, we propose an improved system model of Cheung et al.'s architecture [34]. A smart grid network can be simplified into a hierarchical structure consisting of three basic layer-control centers, sub-

stations, and smart meters. It can be shown that they have different characteristics.

- (i) A control center (CC) is at the top level and maintained by the power operator. It can be a single server inside the power plant or be distributed servers at different locations responsible for parameter generation, entity registration, and issuing credentials for smart meters. In this paper, we assume that the control center is trusted
- (ii) Substations (SS) are at the middle of the structure and fixed in a particular geographic location as it contains expensive electric devices. They could communicate with users directly
- (iii) Smart meters (SM) are at the lowest level and installed in the power application positions such as users' homes. They could send power requests to the control center

In our system construction, the main idea is that the control center makes good use of the proposed blind signature scheme to sign credentials for users. In this case, identities of users cannot be recognized when he or she sends a request to the control center, while the user's identity can be validly verified due to only legal user could have requested control center for blind signatures.

The workflow of the system model is shown in Figure 2 [5]. In the system setup phase, the control center (CC) generates a pair of public and private keys and assigns a unique identifier ID_{SM} for each smart meter (SM) to be registered. In the smart meter registration phase, the CC first authenticates the SM's identity and decides to accept or reject this SM. Then, each user submits the blinded credential information to the CC. Each credential consists of a unique identity CID, issuance date T , a substation identifier ID_{SS} , and a value of power amount ν that a credential holder could request. Then, the CC generates a blind signature for the credential and sends it to SM. Eventually, the SM unblinds the signature and obtains a signed credential. In the power requesting phase, smart meters of a user request for more power when it finds the electric appliances cannot be satisfied. The SM chooses a signed credential of required value and transmits it to the SS with identity ID_{SS} noted in the credential. Then, SS sends the signature credential to CC. If the signature is valid and the credential's identity CID is not in the credential revocation list, CC distributes proper power as the credential to the SS. Meanwhile, CC adds CID in the credential revocation list. Finally, the SM receives required power amount.

In the above process, the control center cannot recognize the real user identity through blind signature. Therefore, the power consumption information is not disclosed to CC. In the next subsection, we will introduce blind signatures related to knowledge.

3.2. Fundamental Knowledge

3.2.1. Elliptic Curve. Given a large prime p and the finite field F_p , the elliptic curve equation is defined by $E(F_p): y^2 = x^3$

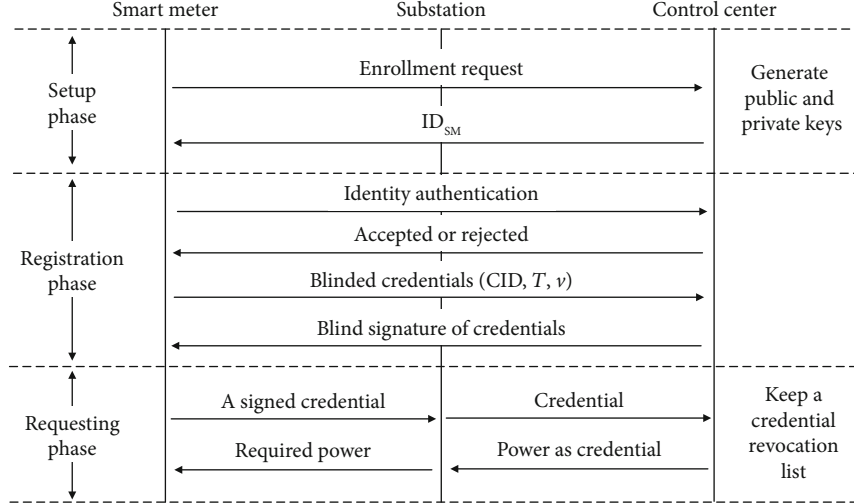


FIGURE 2: System architecture.

$+ ax + b \pmod p$, where $a, b \in F_p$. All points satisfying the elliptic curve equation together with a point at infinity \mathcal{O} are composed of an Abelian group. Order of the group is denoted by n .

Elliptic Curve Discrete Logarithm Problem (ECDLP). Suppose that G is a generator on $E(F_p)$ and Q is a possible point on the elliptic curve, it is difficult to find an $x \in Z_n^*$ such that the equation $Q = x \cdot G$ holds.

3.2.2. The Modification Digital Signature Algorithm (MDSA). As cited, the MDSA is mainly composed of three phases as follows: key generation, signing, and verifying.

- (i) **Key Generation.** The signer randomly chooses an $x \in Z_n$ as the private key and computes $Q = x \cdot G$ as the public key
- (ii) **Signing.** The user selects a random number $k \in Z_n$ and computes $R = k \cdot G = (x_1, y_1)$. $x_1 \pmod n$ is denoted by r . Then, he calculates $e = H(m)$ and $s = ke + xr \pmod n$. The signature output is (s, R)
- (iii) **Verifying.** Upon receiving m, s, R , the verifier first computes $e = H(m)$ and extracts $r = x_1 \pmod n$. Then, he verifies the equation $s \cdot G = H(m)R + r \cdot Q$. If it is the case, (s, R) is a valid signature

3.3. Definition of Blind Signature. A complete blind signature is composed of setup phase, key generation phase, blind signature phase, and verification phase [29]. Specifically, the blind signature phase consists of two probabilistic polynomial-time (PPT) interactive algorithms in the respective party of signer \mathcal{S} and user \mathcal{U} .

- (i) **Setup Phase** (params \leftarrow Setup(λ)). On inputting a security parameter λ for expected security level, a series of public parameters are output in this phase
- (ii) **Key Generation Phase** ($(pk, sk) \leftarrow$ Gen(λ)). This is a probabilistic polynomial-time (PPT) algorithm.

Taking the security parameter λ as input, outputting a public and private key (pk, sk)

- (iii) **Blind Signature Phase.** This phase includes two interactive PPT algorithms Signer(pk, sk) and User(pk, m)
 - (a) complete or uncomplete \leftarrow Signer(pk, sk). Upon inputting a public key pk and the corresponding secret key sk generated by Gen(\cdot), the signer \mathcal{S} outputs complete or uncomplete through blind signature interactive process
 - (b) $\sigma(m)$ or fail \leftarrow User($pk, nonce, m$). Upon inputting a common public key pk of \mathcal{S} , selected blind factors $nonce$, and the message m to be signed, the user \mathcal{U} selects the demanded blind outputs fail or $\sigma(m)$ through blind signature interactive process
- (iv) **Verification Phase** (accept or reject \leftarrow Verify($pk, m, \sigma(m)$)). This is a deterministic polynomial-time algorithm. On inputting public key pk , message m , and the signature $\sigma(m)$, it always outputs accept with the condition that both signer \mathcal{S} and user \mathcal{U} follows the blind signature and \mathcal{S} outputs complete, \mathcal{U} outputs complete

3.4. Security Model of Blind Signature. We refer to Okamoto who proposed a security model for blind signatures and consider the following two properties: blindness and unforgeability [35].

3.4.1. Blindness. The blindness of blind signature is depicted by the following game between an adversarial signer \mathcal{S}^* and a simulator \mathcal{B} which controls two honest users $\mathcal{U}_0, \mathcal{U}_1$.

- (i) An adversary \mathcal{S}^* inputs the security parameter λ to obtain the public key pk and two ordered messages

denoted by (m_0, m_1) . Then, (m_0, m_1) are transmitted to the simulator \mathcal{B}

- (ii) \mathcal{B} randomly chooses a bit $b \in \{0, 1\}$ to reorder the two messages (m_b, m_{1-b}) and, respectively, distributes m_b and m_{1-b} to \mathcal{U}_0 and \mathcal{U}_1 as secret information. Then, $\mathcal{U}_0(\mathcal{U}_1)$ selects proper blind factors nonce and inputs corresponding message $m_b(m_{1-b})$ and pk to run $\text{User}(\text{pk}, \text{nonce}, m)$ algorithm
- (iii) \mathcal{S}^* engages in these two parallel interactive blind signatures separately with $\mathcal{U}_0, \mathcal{U}_1$
- (iv) If $\mathcal{U}_0, \mathcal{U}_1$, respectively, outputs valid blind signatures $(m_b, \sigma(m_b))$ and $(m_{1-b}, \sigma(m_{1-b}))$, send the two signatures to \mathcal{S}^* in random order. Otherwise, output \perp
- (v) Finally, \mathcal{S}^* outputs a guess bit $b' \in \{0, 1\}$

We define

$$\text{Adv}_{\text{BS}}^{\text{blind}} = 2 \cdot \Pr [b' = b] - 1, \quad (1)$$

where $\text{Adv}_{\text{BS}}^{\text{blind}}$ is the advantage of adversary \mathcal{S}^* breaking the blindness property.

Definition 1 (blindness property). A blind signature protocol is recognized to be (t, ϵ) -blind if no PPT adversary \mathcal{S}^* breaks the blindness property in time at most t , and $\text{Adv}_{\text{BS}}^{\text{blind}}$ is at least ϵ .

3.4.2. Unforgeability. The unforgeability of blind signature is described by the following game between an honest signer \mathcal{S} and a malicious user \mathcal{U}^* .

- (i) $\text{Gen}(\lambda)$ is run to obtain public and private keys (pk, sk) . Then, pk is sent to \mathcal{U}^* and sk is secretly held by \mathcal{S}
- (ii) \mathcal{U}^* adaptively engages in polynomially parallel interactive blind signatures by $\text{User}(\text{pk}, m)$ algorithm with \mathcal{S} executing $\text{Signer}(\text{pk}, \text{sk})$ algorithm
- (iii) Let l denote the number of executions among \mathcal{U}^* and \mathcal{S} , where \mathcal{S} outputs complete
- (iv) \mathcal{U}^* wins the game if he outputs l^* valid signature $(m_1, \sigma(m_1), \dots, (m_{l^*}, \sigma(m_{l^*})))$ such that they are different signatures for l^* different messages and $l^* l$

We define $\text{Adv}_{\text{BS}}^{\text{unforge}}$ is the probability that \mathcal{U}^* wins the above game. Then, we give the definition of blind signature unforgeability.

Definition 2 (unforgeability). A blind signature is (t, q_S, ϵ) -unforgeable if there does not exist PPT adversary \mathcal{U}^* win the above game, where t is the most time, q_S is the most times \mathcal{U}^* motivates the blind signature, and ϵ is the least $\text{Adv}_{\text{BS}}^{\text{unforge}}$.

Notations used in this paper are explained in Table 1.

TABLE 1: Notations.

Notations	Description
p	A large prime number
F_p	A finite field with the order p
a, b	Coefficients defining the elliptic curve
G	A generator point
n	The prime order of generator G
Z_n^*	Nonzero integers not larger than n
$H(\cdot)$	One-way hash function
\mathcal{S}	The signer
\mathcal{U}	The user asking for blind signature
d	Private key of \mathcal{S}
Q	Public key of \mathcal{S} , where $Q = d \cdot G$
m	The original message to be signed
\tilde{m}	The blinded message
s	Digital signature for m
\tilde{s}	Blind signature
R, \tilde{R}	Points on the elliptic curve
r	x -coordinate of point R
\tilde{r}	x -coordinate of point \tilde{R}
α, β	The blind factors
k	The random integer number

4. Review of Bütün and Demirer's Scheme

In this section, Bütün and Demirer's scheme [13] will be briefly reviewed. Their scheme comprises the following five phases, including initialization, blinding, signing, unblinding, and verifying. Each phase of Bütün and Demirer's scheme is presented in the following subsection.

- (i) *Initialization Phase.* The elliptic curve parameters are $\text{params} = \{p, F_p, a, b, G, n\}$, where F_p is a finite field defined by the big prime number p ; a, b defines the elliptic curve $E(F_p): y^2 = x^3 + ax + b \pmod{p}$; G is a base point on $E(F_p)$ with the order n

The signer randomly selects an integer $d \in Z_n^*$ as the secret key and calculates $Q = d \cdot G$ as the public key. For each blind signature request from a user, the signer chooses a random number $k \in Z_n^*$ and computes the point $\tilde{R} = kG = (x_1', y_1')$ and $\tilde{r} = x_1' \pmod{n}$. If $\tilde{r} = 0$, the signer reselects the nonce k ; otherwise, he transmits \tilde{R} to the user.

- (ii) *Blinding Phase.* Upon receiving \tilde{R} , the user first extracts \tilde{r} from \tilde{R} and chooses two blind factors $\alpha, \beta \in Z_n^*$. Then, he calculates $R = \alpha\tilde{R} + \beta G = (x_1, y_1)$, $r = x_1 \pmod{n}$ and blinds message m through $\tilde{m} = \alpha H(m)\tilde{r}r^{-1} \pmod{n}$. Finally, the user transmits the blinded message \tilde{m} to the signer

- (iii) *Signing Phase.* On receiving the blinded message, the signer uses his private key d to sign tildem. He computes $\tilde{s} = d\tilde{r} + k\tilde{m} \bmod n$ and sends \tilde{s} to the user
- (iv) *Unblinding Phase.* On receiving \tilde{s} , \mathcal{U} verifies whether \tilde{s} is in the range of Z_n^* . If it holds, the signature is unblinded as follows:

$$s = \tilde{s}r\tilde{r}^{-1} + \beta H(m) \bmod n. \quad (2)$$

Eventually, \mathcal{U} outputs the digital signature $\{s, R\}$ on message m

- (v) *Verifying Phase.* On receiving $\{s, R\}$, the verifier, respectively, calculates $f_1 = s \cdot G \bmod n$ and $f_2 = r \cdot Q + H(m) \cdot R$. Then, he verifies the equation $f_1 = f_2$. If the equation holds, $\{s, R\}$ is a valid signature of the message m ; otherwise, the signature is invalid

Correctness. The correctness can be verified by the following equations:

$$\begin{aligned} s &= \tilde{s}r\tilde{r}^{-1} + \beta H(m) \bmod n = (d\tilde{r} + k\tilde{m})r\tilde{r}^{-1} + \beta H(m) \bmod n \\ &= dr + k\tilde{m}r\tilde{r}^{-1} + \beta H(m) \bmod n \\ &= dr + k(\alpha H(m)\tilde{r}r^{-1})\tilde{r}r^{-1} + \beta H(m) \bmod n \\ &= dr + \alpha kH(m) + \beta H(m) \bmod n, \end{aligned}$$

$$\begin{aligned} f_1 &= s \cdot G = (dr + \alpha kH(m) + \beta H(m)) \cdot G \\ &= rd \cdot G + H(m)(\alpha \cdot \tilde{R} + \beta \cdot G) = r \cdot Q + H(m) \cdot R = f_2. \end{aligned} \quad (3)$$

5. Attack on Bütün and Demirer's Scheme

In this section, we show a malicious signer \mathcal{M} can find a link between the blind signature s' and the original message m .

Suppose that the signer saves all the transcripts $\{k, \tilde{R}', m', \tilde{s}'\}$ of his signatures. Using the unblinded signature $\{m, R, s\}$, \mathcal{M} can match a blinded signature he has signed to an original message m . Detailed procedures are as follows:

- (i) Extracting $r = x_1 \bmod n, \tilde{r}' = x_1' \bmod n$ from $R = (x_1, y_1), \tilde{R}' = (x_1', y_1')$
- (ii) Calculating $\tilde{m}'r\tilde{r}'^{-1}$ denoted as $\alpha'H(m')$
- (iii) Calculating $s - \tilde{s}'r\tilde{r}'^{-1}$ denoted as $\beta'H(m')$
- (iv) Using the private key d to verify whether the following equation $dr + \alpha'H(m') + \beta'H(m') = s$ holds

$$dr + \alpha'H(m') + \beta'H(m') = s \quad (4)$$

If equation (4) holds, \mathcal{M} is able to find the linkage between the blind signature and his signed blind message m ; otherwise, going through all transcripts $\{k, R', m', s'\}$ and

repeating the above process. This shows Bütün and Demirer's scheme is insecure, because there is absence of untraceability. The next section is our improvement of Bütün and Demirer's scheme.

6. Our Proposed Scheme

In this section, an untraceable blind signature scheme is completely described. Our blind signature scheme comprises four phases: setup phase, key generation phase, blind signing phase, and verification phase.

6.1. Setup Phase. On inputting the security parameter λ to reach the expected security magnitude, the elliptic curve parameters are output as $\text{params} = \{p, F_p, a, b, G, n\}$, where p is a large prime that specifies the finite field F_p ; $a, b \in F_p$ defines the elliptic curve $E(F_p): y^2 = x^3 + ax + b \bmod p$; G is a base point on $E(F_p)$, and n is the prime order of G .

6.2. Key Generation Phase. The private and public key of the signer \mathcal{S} is generated by the following steps: First, generating a random nonce d from Z_n^* . Second, calculating the elliptic curve point $Q = d \cdot G = (x_Q, y_Q)$. Finally, \mathcal{S} keeps the private key d secret and the public key Q published.

6.3. Blind Signing Phase. As shown in Figure 3, the user and the signer execute the following steps to generate a signature.

- (i) For each blind signature request, a random integer k is generated by \mathcal{S} and the elliptic curve point \tilde{R} is computed as follows:

$$\begin{aligned} \tilde{R} &= k \cdot G = (x_1', y_1'), \\ \tilde{r} &= x_1' \bmod n. \end{aligned} \quad (5)$$

Moreover, the signer checks $\tilde{r} \neq 0$. If the inequation holds, \mathcal{S} transmits the elliptic curve point \tilde{R} to the user \mathcal{U} ; otherwise, \mathcal{S} reselecs k and repeats (5) to fulfill $\tilde{r} \neq 0$

- (ii) Upon receiving \tilde{R} , \mathcal{U} performs the following operations to obtain the blinded message \tilde{m} . Firstly, extracting $\tilde{r} = x_1' \bmod n$ from \tilde{R} . Secondly, randomly selecting two factors $\alpha, \beta \in Z_n^*$ and computes $R = (\alpha + \beta H(m)^{-1})\tilde{R} + (\alpha^{-1}\tilde{r}^{-1} + \alpha\beta)G = (x_1, y_1)$. Thirdly, extracting $r = x_1 \bmod n$ from R . Finally, calculating $\tilde{m} = (\alpha H(m) + \beta)r^{-1}\tilde{r} \bmod n$ to blind the original message. Having executed the above steps, \mathcal{U} sends the blinded message \tilde{m} to \mathcal{S}
- (iii) Upon receiving \tilde{m} , \mathcal{S} first extracts $\tilde{r} = x_1' \bmod n$ from \tilde{R} . Then, he uses private key d and selects a random nonce k to compute the blind signature $\tilde{s} = d\tilde{r} + k\tilde{m} \bmod n$. Finally, \mathcal{S} transmits the blinded signature \tilde{s} to \mathcal{U}
- (iv) On receiving \tilde{s} , \mathcal{U} verifies whether $\tilde{s} \in Z_n^*$ satisfies. If it holds, the signature is unblinded as follows:

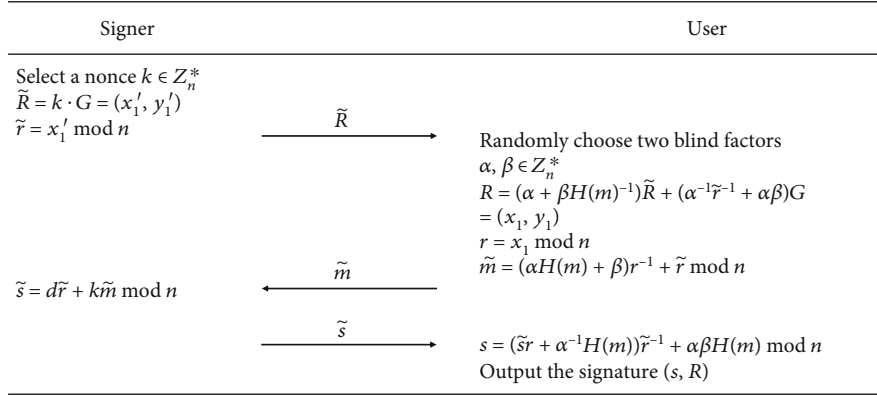


FIGURE 3: The proposed scheme.

TABLE 2: Comparison of security properties.

Properties	Schemes				
	Ours	[13]	[16]	[36]	[37]
Correctness	✓	✓	✓	✓	✓
Verifiability	✓	✓	✓	✓	✓
Impersonality resistance	✓	✓	✓	✓	✓
Privileged insider resistance	✓	✓	✓	✓	×
Privacy preservation	✓	×	✓	✓	✓
Unforgeability	✓	✓	✓	✓	✓
Untraceability	✓	×	✓	✓	✓
Unlinkability proof	✓	×	✓	×	×

TABLE 3: Performance comparisons.

Protocol	Computation cost	Communication cost (bit)
Ours	$3T_{\text{pm}} + 4T_{\text{mi}} = 6.663$ ms	1024
Ref. [13]	$3T_{\text{pm}} + 2T_{\text{mi}} = 6.579$ ms	1024
Ref. [16]	$2T_{\text{H}} + 3T_{\text{pm}} + 1T_{\text{mi}} = 17.523$ ms	1280
Ref. [36]	$5T_{\text{pm}} = 10.825$ ms	2368
Ref. [37]	$9T_{\text{pm}} = 19.485$ ms	3136

TABLE 4: Running time of basic operations (ms).

Notations	Description	Running time
T_{H}	Hash-to-point	5.493
T_{pm}	Point multiplication	2.165
T_{mi}	Modular inversion	0.042

$$s = (\tilde{s}r + \alpha^{-1}H(m))\tilde{r}^{-1} + \alpha\beta H(m) \bmod n. \quad (6)$$

Eventually, \mathcal{U} outputs the digital signature $\{s, R\}$ on message m

6.4. Verification Phase. Any verifier can verify the validity of the signature $\{s, R\}$. First, using the public parameter G and signature s to compute $g_1 = s \cdot G \bmod n$; second, extracting $r = x_1 \bmod n$ from $R = (x_1, y_1)$; third, using the signer's public key Q and signature value R to calculate $g_2 = r \cdot Q + H(m) \cdot R$; finally, verifying whether the equation $g_1 = g_2$ holds. If the equation holds, $\{s, R\}$ is a valid signature of message m ; otherwise, the signature is invalid.

Correctness. The correctness can be verified by the following equations:

$$\begin{aligned} s &= (\tilde{s}r + \alpha^{-1}H(m))\tilde{r}^{-1} + \alpha\beta H(m) \bmod n \\ &= ((d\tilde{r} + k\tilde{m})r + \alpha^{-1}H(m))\tilde{r}^{-1} + \alpha\beta H(m) \bmod n \\ &= dr + k\tilde{m}r\tilde{r}^{-1} + \alpha^{-1}H(m)\tilde{r}^{-1} + \alpha\beta H(m) \bmod n \\ &= dr + H(m)(\alpha + \beta H(m)^{-1})k + H(m)(\alpha^{-1}\tilde{r}^{-1} + \alpha\beta) \bmod n, \end{aligned}$$

$$\begin{aligned} g_1 &= s \cdot G = rd \cdot G + H(m)((\alpha + \beta H(m)^{-1})\tilde{R} + (\alpha^{-1}\tilde{r}^{-1} + \alpha\beta) \cdot G) \\ &= r \cdot Q + H(m) \cdot R = g_2. \end{aligned} \quad (7)$$

7. Security

In this section, we give the formal security proof of our blind signature scheme's blindness property and unforgeability.

7.1. Security Proof. According to the security model of blindness in Section 3.4, the blindness is to guarantee that an adversarial signer \mathcal{S}^* cannot distinguish signatures from two different messages. We will show that our scheme's signature values are independent from the view of \mathcal{S}^* .

Theorem 3 (blindness property). *Our proposed blind signature keeps blindness property.*

Proof. For any public key output Q from the malicious signer \mathcal{S}^* , (k, \tilde{m}) is perfectly independent from (m, α, β) in the blind signature process in the view of \mathcal{S}^* . On the one hand, the k is a completely random number chosen from Z_n^* . On the other hand, $\tilde{m} = (\alpha H(m) + \beta)r^{-1}\tilde{r} \bmod n$, where \tilde{r} is the

x -coordinate of $\tilde{R} = k \cdot G$. Due to the randomness of k , \tilde{m} is independent of (m, α, β) . \square

Next, we will prove that the signature (m, s, R) is independent from the view of \mathcal{S}^* . Since $s = (\tilde{s}r + \alpha^{-1}H(m))\tilde{r}^{-1} + \alpha\beta H(m) \pmod n$ and (m, α, β) cannot be obtained from (k, \tilde{m}) , s is perfectly independent. Moreover, $R = (\alpha + \beta H(m)^{-1})\tilde{R} + (\alpha^{-1}\tilde{r}^{-1})G + \alpha\beta G$ and (α, β) is not related to (k, \tilde{m}) . Therefore, the signature values (m, s, R) are independent in the view of \mathcal{S}^* .

Above all, our blind signature scheme keeps perfectly blindness property.

Theorem 4 (unforgeability). *If the ECDLP assumption holds, our proposed blind signature is existential unforgeability against chosen-message attacks (EU-CMA).*

Proof. Suppose that \mathcal{A} is an adversary delegated for a malicious user that forges the proposed blind signature scheme, there exists a challenger \mathcal{C} that can break unforgeability of the MDSA. Then, it is contradictory to the ECDLP assumption. \square

In this proof, Signer(pk, sk) algorithm is modelled as a signing oracle and forging process of the proposed blind signature is depicted as follows.

- (i) \mathcal{C} runs the Gen(λ) to generate a pair of public and private keys ($Q = x \cdot G, sk = x$). Then, \mathcal{B} sends Q to \mathcal{A} as the public key
- (ii) \mathcal{C} executes signing oracle following the proposed blind signature, that is, the signing oracle outputs \tilde{R} and \tilde{s} with the corresponding \tilde{m} from \mathcal{A}
- (iii) \mathcal{A} could adaptively request l times \mathcal{C} to sign different \tilde{m} as the proposed interactive blind signature
- (iv) If \mathcal{A} outputs l^* different signatures $\Sigma = ((m_1, s_1, R_1), \dots, (m_{l^*}, s_{l^*}, R_{l^*}), l^*)$, there exists one signature $(m_f, s_f, R_f) \in \Sigma$ forged by \mathcal{A} . In addition, \mathcal{A} cannot obtain the secret key x through \tilde{R}, \tilde{s} due to \tilde{R} is unrelated to x and the private key cannot be recovered by the equation $\tilde{s} = x\tilde{r} + k\tilde{m} \pmod n$ with k unknown to \mathcal{A}

Moreover, the signature (s, R) is a variant of MDSA since $s = (\tilde{s}r + \alpha^{-1}H(m))\tilde{r}^{-1} + \alpha\beta H(m) \pmod n = xr + H(m)(\alpha + \beta H(m)^{-1} + \alpha^{-1}\tilde{r}^{-1} + \alpha\beta) = xr + H(m)z$ where $z = \alpha + \beta H(m)^{-1} + \alpha^{-1}\tilde{r}^{-1} + \alpha\beta$ and the signature is verified by the equation $s \cdot G = r \cdot Q + H(m) \cdot R$. Therefore, unforgeability of the proposed blind signature is reduced to the security of MDSA. Under the difficulty assumption of ECDLP, MDSA is existential unforgeability.

7.2. Security Analysis. According to references, we analyze identity privacy preservation, unforgeability, untraceability, and verifiability of the proposed scheme.

- (i) *Privacy Preservation.* We have proven blindness of our proposed blind signature in 7.1. Therefore, nobody including the control center and substations could recognize the real identity of users when they request for more power. Thus, identity and electricity consumption privacy of users could be protected
- (ii) *Unforgeability.* As shown in 7.1, the proposed blind signature scheme is existential unforgeability. Thereby, any users (i.e., smart meters) cannot unforge blind signatures for credentials with desired values
- (iii) *Untraceability.* Suppose that a control center attempts to find linkage among the credential he signed and signature. For this, he could preserve all the transcripts $(k, \tilde{m}, \tilde{s})$. Even after the blind signature (m, s, R) is made public by the user, the control center is still unable to find the blind factors α, β . Moreover, $(k, \tilde{m}, \tilde{s})$ and (m, s, R) are independent of each other. Above all, it is impossible for the control center to link the signature (m, s, R) with corresponding transcript $(k, \tilde{m}, \tilde{s})$
- (iv) *Verifiability.* The correctness of proposed blind signature insures that the control center can verify validity of credentials by checking equation $s \cdot G = r \cdot Q + H(m) \cdot R$

8. Performance Analysis

In this section, we compare the proposed scheme with Bütün and Demirel's [13], Verma and Singh's [16], Chaudhry et al.'s [36], and Mahmood et al.'s [37] in terms of security properties, computational cost, and communication cost. The results are listed in Tables 2 and 3 separately.

8.1. Security Properties. As we have analyzed in this paper, Bütün and Demirel's scheme [13] cannot resist that a malicious signer traces the original message he has signed, which means there is no untraceability in Bütün and Demirel's scheme. Furthermore, traceability provides opportunities for adversaries to recognize users' daily schedule and privacy preservation does not hold. In addition, [36] does not provide unlinkability proof and [37] does not have privileged insider resistance and unlinkability proof.

8.2. Performance Analysis

8.2.1. Computational Cost. In this subsection, we mainly consider the more time-consuming operations hash-to-point (T_H), point multiplication (T_{pm}), and modular inversion (T_{mi}) and adopt the executing time in [38] as shown in Table 4. It can be seen that the proposed scheme requires 3 point multiplication operations and 4 modular inversions, i.e., 6.663 ms, which is only slightly larger than that of [13] and smaller than the other three schemes' computational cost.

8.2.2. Communication Cost. We set the size of point on $E(F_p)$ is 512 bits, size of n is 256 bits, output size of general hash

function is 256 bits, and size of timestamp is 32 bits. Then, we have the communication cost comparison in Table 3. We can see that our scheme and Ref. [13] have the least communication cost, i.e., 1024 bits than the other three literatures. Therefore, our scheme needs the least communicational bandwidth.

Above all, the proposed scheme has better security properties than Bütün and Demirer's [13] although performing two more modular inversions and has better computational costs with the same security properties of Verma et al.'s scheme.

9. Conclusion

Our scheme provided values of theory and application to some extent. On the one hand, the proposed untraceable blind signature is constructed under the noted MDSA algorithm and proof of which gave theoretical insurance of blindness and unforgeability. On the other hand, we put forward a new credential-based privacy-preserving power request model for smart grid. In this system model, the user's daily schedule could not leak outside with the help of blind signature since blinded factors hide the real signed message for the signer and verifiers cannot identify the real sources of messages. Moreover, it was shown that this scheme has better security or computational costs compared with other blind signatures under the same background or cryptographic infrastructure.

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.

References

- [1] J. W. Hughes, "IntelliGrid architecture concepts and IEC61850," in *Transmission and Distribution Conference and Exhibition, 2005/2006 IEEE PES*, pp. 401–404, 2006.
- [2] W. Kong, J. Shen, P. Vijayakumar, Y. Cho, and V. Chang, "A practical group blind signature scheme for privacy protection in smart grid," *Journal of Parallel and Distributed Computing*, vol. 136, pp. 29–39, 2020.
- [3] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: motivations, requirements and challenges," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 5–20, 2013.
- [4] Q. Gao, Y. Wang, X. Cheng, J. Yu, X. Chen, and T. Jing, "Identification of vulnerable lines in smart grid systems based on affinity propagation clustering," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5163–5171, 2019.
- [5] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "Pass: privacy-preserving authentication scheme for smart grid network," in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Brussels, Belgium, 2011.
- [6] A A Group, "Scada systems for smart grid," <http://www.arcweb.com/Research/Studies/Pages/SCADA-Power.aspx>.
- [7] 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, 2019.
- [8] R. Liu, Y. Wang, S. Wu, C.-X. Wang, and W. Zhang, "Energy efficiency and area spectral efficiency tradeoff for coexisting wireless body sensor networks," *Science China Information Sciences*, vol. 59, no. 12, pp. 1–15, 2016.
- [9] D. He, Y. Zhang, D. Wang, and K.-K. R. Choo, "Secure and efficient two-party signing protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 1124–1132, 2020.
- [10] Q. Feng, D. He, Z. Liu, D. Wang, and K.-K. R. Choo, "Distributed signing protocol for IEEE P1363-compliant identity-based signature scheme," *IET Information Security*, vol. 14, no. 4, pp. 443–451, 2020.
- [11] Y. Zhang, D. He, X. Huang, D. Wang, K.-K. R. Choo, and J. Wang, "White-box implementation of the identity-based signature scheme in the IEEE P1363 standard for public key cryptography," *IEICE Transactions on Information and Systems*, vol. E103.D, no. 2, pp. 188–195, 2020.
- [12] D. Chaum, R. L. Rivest, and A. T. Sherman, *Blind signatures for untraceable payments*, Springer, 1983.
- [13] İ. Bütün and M. Demirer, "A blind digital signature scheme using elliptic curve digital signature algorithm," *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 21, 2013.
- [14] P. Sarde and A. Banerjee, "A secure ID-based blind and proxy blind signature scheme from bilinear pairings," *Journal of Applied Security Research*, vol. 12, no. 2, pp. 276–286, 2017.
- [15] C. Popescu, "Blind signature schemes based on the elliptic curve discrete logarithm problem," *Studies in Informatics and Control*, vol. 19, no. 4, pp. 397–402, 2010.
- [16] G. K. Verma and B. B. Singh, "Efficient identity-based blind message recovery signature scheme from pairings," *IET Information Security*, vol. 12, no. 2, pp. 150–156, 2018.
- [17] G. K. Verma and B. B. Singh, "Efficient message recovery proxy blind signature scheme from pairings," *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 11, 2017.
- [18] H. Chen, L. Zhang, J. Xie, and C. Wang, "New efficient certificateless blind signature scheme," in *2016 IEEE Trustcom/Big-DataSE/ISPA*, Tianjin, 2016.
- [19] G. K. Verma, B. B. Singh, and H. Singh, "Provably secure certificate-based proxy blind signature scheme from pairings," *Information Sciences*, vol. 468, pp. 1–13, 2018.
- [20] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid — the new and improved power grid: a survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 944–980, 2012.
- [21] K. M. A. Alshehri, "Multi-period demand response management in the smart grid: a stackelberg game approach," <http://hdl.handle.net/2142/88959>.
- [22] R. Zafar, A. Mahmood, S. Razaq, W. Ali, U. Naeem, and K. Shehzad, "Prosumer based energy management and sharing in smart grid," *Renewable & Sustainable Energy Reviews*, vol. 82, pp. 1675–1684, 2018.
- [23] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, "Software defined networks based smart grid communication: a

- comprehensive survey,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 99, 2019.
- [24] N. I. Nimalsiri, C. P. Mediwaththe, E. L. Ratnam, M. Shaw, and S. K. Halgamuge, “A survey of algorithms for distributed charging control of electric vehicles in smart grid,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 99, pp. 1–19, 2019.
- [25] L. Wen, K. Zhou, S. Yang, and L. Li, “Compression of smart meter big data: a survey,” *Renewable & Sustainable Energy Reviews*, vol. 91, pp. 59–69, 2018.
- [26] S. N. Makhadmeh, A. T. Khader, M. A. al-Betar, S. Naim, A. K. Abasi, and Z. A. A. Alyasseri, “Optimization methods for power scheduling problems in smart home: survey,” *Renewable & Sustainable Energy Reviews*, vol. 115, article 109362, 2019.
- [27] G. Si, Z. Guan, J. Li, P. Liu, and H. Yao, “A comprehensive survey of privacy-preserving in smart grid,” in *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, Zhangjiajie, China, 2016.
- [28] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, “An elliptic curve cryptography based lightweight authentication scheme for smart grid communication,” *Future Generations Computer Systems*, vol. 81, pp. 557–565, 2018.
- [29] J. L. Camenisch, J. M. Piveteau, and M. A. Stadler, “Blind signatures based on the discrete logarithm problem,” in *Workshop on the Theory and Application of Cryptographic Techniques*, Perugia, Italy, 1994.
- [30] H. R. Tseng, “A secure and privacy-preserving communication protocol for V2G networks,” in *2012 IEEE Wireless Communications and Networking Conference (WCNC)*, Paris, France, 2012.
- [31] Z. Yang, S. Yu, W. Lou, and C. Liu, “ P^2 : privacy-preserving communication and precise reward architecture for V2G networks in smart grid,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 697–706, 2011.
- [32] C. Yu, C. Chen, S. Kuo, and H. Chao, “Privacy-preserving power request in smart grid networks,” *IEEE Systems Journal*, vol. 8, no. 2, pp. 441–449, 2014.
- [33] W. Han and Y. Xiao, “Privacy preservation for V2G networks in smart grid: a survey,” *Computer Communications*, vol. 91–92, pp. 17–28, 2016.
- [34] J. C. L. Cheung, T. W. Chim, S. M. Yiu, V. O. K. Li, and L. C. K. Hui, “Credential-based privacy-preserving power request scheme for smart grid network,” in *2011 IEEE Global Telecommunications Conference - GLOBECOM 2011*, pp. 1–5, Houston, TX, USA, 2011.
- [35] T. Okamoto, “Efficient blind and partially blind signatures without random oracles,” in *Theory of Cryptography*, S. Halevi and T. Rabin, Eds., pp. 80–99, Springer, Berlin, Heidelberg, 2006.
- [36] S. A. Chaudhry, H. Alhakami, A. Baz, and F. Al-Turjman, “Securing demand response management: a certificate-based access control in smart grid edge computing infrastructure,” *IEEE Access*, vol. 8, pp. 101235–101243, 2020.
- [37] K. Mahmood, J. Arshad, S. A. Chaudhry, and S. Kumari, “An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure,” *International Journal of Communication Systems*, vol. 32, no. 16, 2019.
- [38] Q. Fan, J. Chen, L. J. Deborah, and M. Luo, “A secure and efficient authentication and data sharing scheme for internet of things based on blockchain,” *Journal of Systems Architecture*, vol. 117, article 102112, 2021.

Review Article

A Survey on Adversarial Attack in the Age of Artificial Intelligence

Zixiao Kong,¹ Jingfeng Xue,¹ Yong Wang¹ ,¹ Lu Huang,¹ Zequn Niu,¹ and Feng Li²

¹School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China

²Shandong Cloudsky Security Technology Co., Ltd, Jinan, China

Correspondence should be addressed to Yong Wang; wangyong@bit.edu.cn

Received 9 April 2021; Revised 24 May 2021; Accepted 11 June 2021; Published 22 June 2021

Academic Editor: Weizhi Meng

Copyright © 2021 Zixiao Kong 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 evolution of the Internet, the application of artificial intelligence fields is more and more extensive, and the era of AI has come. At the same time, adversarial attacks in the AI field are also frequent. Therefore, the research into adversarial attack security is extremely urgent. An increasing number of researchers are working in this field. We provide a comprehensive review of the theories and methods that enable researchers to enter the field of adversarial attack. This article is according to the “Why? → What? → How?” research line for elaboration. Firstly, we explain the significance of adversarial attack. Then, we introduce the concepts, types, and hazards of adversarial attack. Finally, we review the typical attack algorithms and defense techniques in each application area. Facing the increasingly complex neural network model, this paper focuses on the fields of image, text, and malicious code and focuses on the adversarial attack classifications and methods of these three data types, so that researchers can quickly find their own type of study. At the end of this review, we also raised some discussions and open issues and compared them with other similar reviews.

1. Introduction

In the age of the Internet, with the accumulation of large amounts of data, the evolution of computing power, and the constant innovation and evolution of machine learning methods and frameworks, artificial intelligence (AI) technologies such as image recognition, machine translation, and autonomous driving have been widely deployed and widely applied all over the world [1]. Artificial intelligence is marching towards historic moments for mankind. At the same time, machine learning algorithms also have a significant impact on the research of the traditional computer security field [2]. In addition to using machine learning (ML) to build various malicious detections and attack identification systems, hackers may also use ML to achieve more accurate attacks. Recent studies have shown that many application fields, from computer vision to network security, are vulnerable to adversarial attack threats [3, 4].

Szegedy et al. [5] first proposed the concept of adversarial sample—an interesting weakness in neural networks. This

paper has sparked widespread interest in adversarial attacks among researchers, and the number of adversarial attacks will continue to increase in the future as the economic benefits trend. Based on gradient descent and L-norm optimization methods, Liu et al. [6] first presented the method to exploit a malware-based visual detector to adversarial example attacks. Zhou et al. [7] were the first to propose an alternative model for training adversarial attacks without real data.

In order to provide a comprehensive reference tool for researchers to study adversarial attack, this paper classifies and compares adversarial attack algorithms of image, text, and malware fields. Moreover, the concepts, types, harms, evolution trends of adversarial attack, and the commonly used defense technologies in recent years are reviewed systematically, and the future research direction is discussed [8, 9]. This paper is aimed at providing theoretical and methodological support for the research on adversarial attack security by extensively investigating the research literature on adversarial attacks and robustness [10, 11].

To sum up, the main contributions are as follows:

- (1) Present adversarial attacks according to the idea of “Why? → What? → How?” In this way, researchers can quickly and efficiently establish the awareness of adversarial attack
- (2) Portray a roadmap for carrying out adversarial attack research, which can help researchers quickly and efficiently access the domain of adversarial attacks security research
- (3) In order to ensure the timeliness of the review, the most up-to-date and comprehensive references are provided based on the articles published in authoritative journals and top academic conferences after 2010
- (4) In order to enable researchers to find referable methods as needed, the technical core and deficiency of methods in each typical method are introduced
- (5) In order to quickly find the entry point of adversarial attack research, the pieces of literature on adversarial attack are classified from different perspectives.

The structure of the article is as follows. In “Why Study Adversarial Attack,” we first recommend why we should study adversarial attacks. In “Adversarial Attack,” we describe the concepts, classifications, hazards, and methods associated with adversarial attacks. A separate section is devoted to categorizing and comparing the adversarial attack methods of images, text, and malware. In “Defense Methods,” we discuss defense methods. Then, in “Additional Complements,” the additional supplements needed for adversarial attack research are presented. After that, we put forward a broader prospect of research direction in “Discussion.” In “Comparison with Other Similar Reviews,” the differences between this paper and other similar reviews are discussed. Finally, we concluded in “Conclusions.”

2. Why Study Adversarial Attack

Choosing directions is the first step in conducting research. The research direction of adversarial attack security is reflected in the following aspects:

- (1) Adversarial attack has become a serious threat to the current AI system. In the era of the Internet of Everything, the network has become the ideal goal for cyber attackers. Vulnerability in artificial intelligence is often exploited by attackers to launch cyber-attacks. In 2018, a fake video of Obama railing against Trump went viral across the United States. Some criminals fabricate information to manipulate the election. With the frequent occurrence of these fraud incidents, governments and organizations of various countries have formulated and improved the relevant laws and regulations. In the United States, for example, the Deepfake Report Act was introduced in June 2019 and passed unanimously in the Senate as a separate bill only 120 days later. Despite the relentless

efforts of the machine learning and AI communities to erect protective fences, the number of adversarial attacks is climbing significantly, and the threat posed by them continues to increase. Szegedy et al. [5] first proposed the concept of adversarial samples—intriguing weaknesses of neural networks. Their essay has sparked broad interest among researchers in adversarial attacks. Moreover, the number of adversarial attacks will continue to increase in the future, as economic interests evolve. Only by continuously strengthening the protective barrier of the deep learning model can a secure network security environment be built [12]

- (2) The race of AI can promote adversarial attack security research. Attacking and defending adversarial machine learning is a process of iterative evolution. Adversarial attack creators have been probing new vulnerabilities, depicting new algorithms, and seeking new threats, while the defenders have been analyzing the features of new adversarial attacks and employing new methods to ensure efficient and effective defense against adversarial attacks. Consequently, choosing adversarial attack security as the research direction can not only merely keep the study at the forefront of AI security but also enable researchers to stimulate continuous motivation in the process of research.

3. Adversarial Attack

3.1. Concepts. In this subsection, some common terms used in the literature related to adversarial attacks are presented.

3.1.1. Adversarial Example. Adversarial example is an artificially constructed example that makes machine learning models misjudge by adding subtle perturbations to the original example but at the same time does not make human eyes misjudge [13].

3.1.2. White-Box Attack. White-box attacks assume that the target model can fully obtain the structure of the model, including the composition of the model and the parameters of the partition layer, and can fully control the input of the model [14].

3.1.3. Black-Box Attack. Black-box attacks have no idea of the internal structure of the model and can only control the input and carry out the next attack by comparing the feedback of the input and output [15].

3.1.4. Real-World Attack/Physical Attack. Real-world attacks/physical attacks do not understand the structure of the model and even have weak control over the input [16].

3.1.5. Targeted Attack. Targeted attacks will set the target before the attack, causing it to incorrectly predict the specific label of the adversarial images, which means that the effects after the attacks are determined [17].

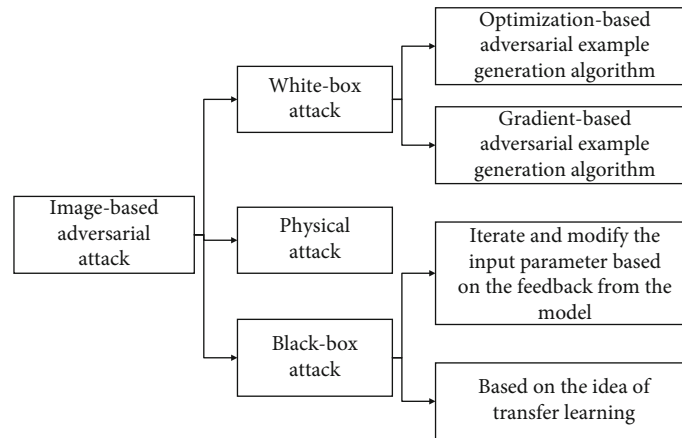


FIGURE 1: Classification of image-based adversarial attack.

3.1.6. Untargeted Attack. Untargeted attacks do not need to set the target before the attack, as long as the result of identification is wrong after the attack [18].

3.1.7. Evade Attack. Evade attacks refer to adding disturbance to test samples and modifying the input during the test phase, to avoid or deceive the detection of the model and make the AI model unable to be correctly identified [19].

3.1.8. Poisoning Attack. By adding carefully constructed malicious examples in the model training phase, poisoning attacks make the trained model have backdoor or vulnerability, which can be used by attackers to carry out attacks [20].

3.1.9. Backdoor Attack. Backdoor attack means that the attacker can enter the system without identity authentication, which means that the attacker can bypass the security control to gain access to the system and even further damage the computer or network. The neural network backdoor attack referred to in this paper refers to that the attacker generates a model with a backdoor by implanting specific neurons in the neural network model, so that the judgment of the model on normal inputs is consistent with the original model, but the judgment on special inputs will be controlled by the attacker [21]. A backdoor attack is a type of poisoning attack [22].

3.1.10. Detection Model. The detection model means to detect whether the examples to be judged are adversarial examples by detecting components. Various detection models may judge whether the input is an adversarial example according to different criteria [23].

3.2. Classifications. In this section, we describe the main methods for generating adversarial examples in the image, text, and malware domains. And the work of some researchers is reviewed. Adversarial machine learning is a widely used technology in the field of image, and the research has been quite comprehensive. The malicious code domain and the text domain are similar and can be borrowed from each other. Figure 1 is the classification of image-based adversarial attack. According to the attacker's knowledge, the attack can be divided into black-box attack, white-box

attack, and physical attack. Figure 2 is the classification of text-based adversarial attack. According to the access permissions of the model, the attack can be divided into black-box attack and white-box attack. And according to the effect after the attack, it can be divided into the targeted attack and non-targeted attack. Moreover, according to the text granularity, it can be divided into character level, word level, and sentence level. Besides, according to the attack strategy, it can be divided into image-to-text, importance-based, optimization-based, and neural network-based. Figure 3 is the classification of malware-based adversarial attack. According to the object, it can be divided into attacks on training data and attacks on neural network model.

3.3. Hazards. The main harm of adversarial attack includes the following:

- (1) Model losing or stealing: network information data has become the most precious intangible asset in the current Internet of Everything era. In the current era of the Internet of Everything, network information data has become the most precious intangible asset. Plenty of adversarial attacks are designed to steal secret data, such as stealing privacy data from computers or servers and after that deceiving or blackmailing victims. More malicious attacks are aimed at enterprises to steal valuable trade secrets from enterprises and obtain economic benefits, even worse, targeting a country and stealing national security-related intelligence information from government departments for strategic purposes
- (2) Model failure: the adversarial attack causes the failure of the deep learning model and makes it unable to work properly utilizing physical attack against the vulnerability of the model. For instance, in the field of autonomous driving, the superposition of image data with subtle perturbations makes it difficult for humans to recognize by senses, which leads to the wrong classification decision made by the machine learning model and causes traffic accidents

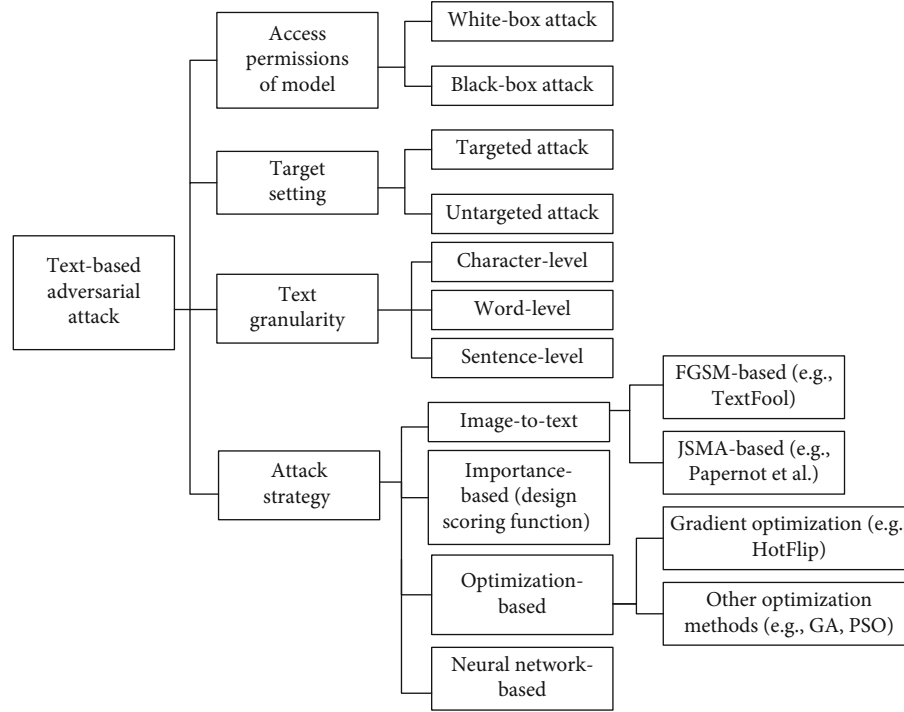


FIGURE 2: Classification of text-based adversarial attack.

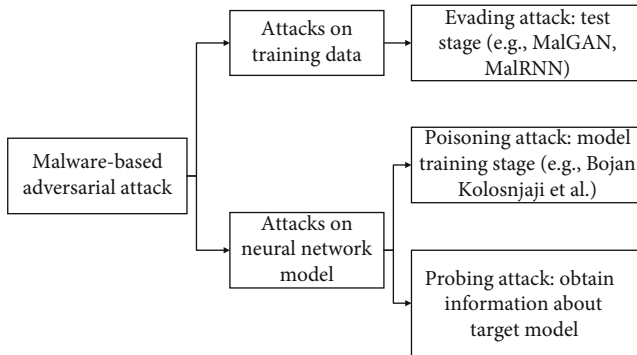


FIGURE 3: Classification of malware-based adversarial attack.

- (3) Data poisoning: a typical scenario is the recommendation system. When hackers add abnormal data to the training samples of deep learning, the most direct impact is that the classification error of the deep learning model, i.e., the recommendation system, generates an error
- (4) Other hidden hazards: apart from the obvious harms mentioned above, adversarial attacks can also cause some hidden hazards. For instance, many malwares generate adversarial examples through some algorithms, and the malicious behavior does not change, but the detection of antivirus system fails, which eventually leads to malicious attacks on computers and networks as well as losses of profits.

3.4. *Methods.* The typical attack algorithms of each application domain are shown in Table 1.

3.4.1. *Image-Based Adversarial Attack.* Adversarial attacks are a major threat to computer vision. CCS 2020 has a total of four papers on adversarial machine learning, all of which are based on image research, three of which are about robustness and defense mechanisms, and only one is about adversarial attack methods. I have compared and summarized several papers of CCS, NIPS, USENIX, ECML PKDD, and JNCA from 2016 to 2020, as shown in Table 2.

Through reading the papers, it can be found that most of the current research in the field of image are optimized and improved based on previous research, and the attack types are generally divided into white-box attack, black-box attack, and physical attack [12].

3.4.2. *Text-Based Adversarial Attack.* Studies have shown that DNN models are susceptible to adversarial samples that lead to false predictions by adding imperceptible per to normal input. The study of adversarial samples in the field of images is abundant, but not enough in the field of text. Table 3 summarizes some of the relevant papers on the research of adversarial machine learning in the text field in recent years.

By reading the literature, the text domain adversarial samples can be divided into character level, word level, and sentence level. Attack types can be classified into white-box attack and black-box attack according to the model access rights. According to the effect after the attack, it can be divided into the targeted attack and untargeted attack. Attack strategies in the text domain generally include reference algorithms in the field of image, transformed into optimization problems, using gradient or designing scoring functions, and training neural network models to automatically generate adversarial samples [13].

TABLE 1: Typical attack algorithms for different application domains.

Method	Access permission	Targeted/nontargeted	Application domain	Metrics/strategies
Papernot et al. 2016 [24]	White box	Nontargeted	Text	Gradient
TextFool 2018 [25]	White and black box	Targeted	Text	Gradient
HotFlip 2018 [26]	White box	Nontargeted	Text	Gradient
Alzantot et al. 2018 [27]	Black box	Targeted	Text	Euclidean distance
DeepWordBug 2018 [28]	Black box	Nontargeted	Text	Scoring function
Zhao et al. 2018 [29]	Black box	Nontargeted	Text and image	WGAN-based
TextBugger 2019 [30]	White and black box	Nontargeted	Text	Confidence coefficient, scoring function
DISTFLIP 2019 [31]	Black box	Nontargeted	Text	Gradient
UPSET 2011 [32]	Black box	Targeted	Universal	l_∞
L-BFGS 2014 [33]	White and black box	Targeted	Image	l_∞
FGSM-based 2015 [34]	White box	Targeted/nontargeted	Universal	l_2, l_∞
JSMA 2015 [35]	White box	Targeted	Image	l_∞
DeepFool 2016 [36]	White box	Nontargeted	Image	l_2, l_∞
BIM and ILCM 2017 [37]	White box	Nontargeted	Image	l_0
One-pixel 2017 [38]	Black box	Targeted	Image	l_0
C&W 2017 [39]	White box	Nontargeted	Image	l_0, l_2, l_∞
Universal perturbations 2017 [40]	White box	Nontargeted	Universal	l_2, l_∞
ANGRI 2017 [41]	Black box	Targeted	Image	l_∞
Houdini 2017 [42]	Black box	Targeted	Image	l_2, l_∞
ATNs 2017 [43]	White box	Targeted	Image	l_∞
MalGAN 2017 [44]	Black box	Targeted	Malware	GAN-based, gradient
SLEIPNIR 2018 [45]	White box	Targeted	Malware	Saddle-point optimization
Kolosnjaji et al. 2018 [46]	White box	Targeted	Malware	Gradient
Song et al. 2020 [47]	Black box	Targeted	Malware	Number of bytes changed
Rosenberg et al. 2020 [48]	Black box	Targeted	Malware	API call-based, GAN
MalRNN 2020 [49]	Black box	Targeted	Malware	Varying the append size

3.4.3. *Malware-Based Adversarial Attack.* In recent years, machine learning has been used to detect malware, and malware developers have a strong incentive to attack the detection model. Table 4 summarizes some of the papers related to adversarial attacks in the field of malicious code in recent years.

Through literature reading, it can be found that attack types are generally divided into attacks on training data and attacks on neural network models. According to the attack scenario, it can be divided into white-box attack, gray-box attack, and black-box attack. In addition, the methods adopted include GAN-based, gradient-based, and heuristic-based algorithms [14].

4. Defense Methods

At present, relevant studies have been conducted to explore the security of AI itself, to ensure the integrity and confidentiality of AI models and data, so that it will not be easily affected by attackers to change judgment results or leak data in different scenarios. Hendrycks and Gimpel [64] proposed three methods for detecting adversarial images. Zhang et al. [65] proposed a hardware-assisted randomization method

against adversarial examples to defend against various adversarial attacks. At present, AI attacks are divided into the evasive attack, poisoning attacks backdoor attack, and model-stealing attack. The backdoor attack is a kind of poisoning attack. Table 5 lists the various defense techniques of the AI system during data collection, model training, and model use phases. Furthermore, we need to continue to study AI interpretability, enhance our understanding of how ML works, and build institutional defense measures to build AI security platforms [66].

4.1. Defense Methods of Evasive Attack

4.1.1. *Adversarial Training.* Adversarial training is an important way to enhance the robustness of neural network models. The basic principle of this technique is to use known attack techniques to generate adversarial samples in the model training stage. Then, the adversarial samples are added to the training set of the model, and the model is iteratively retrained until a new model that can resist disturbance is generated. At the same time, since the synthesis of multiple types of adversarial samples increases the data of the training set, this technique can not only enhance the robustness of the

TABLE 2: Image-based adversarial attack.

Author	Solution	Cores	Shortcomings
Sharif et al. 2016 [50]	Mahmood Sharif et al. propose a class of attack that allows an attacker to avoid identifying or impersonating another individual. In addition, they described a method of automatically generating attacks and achieved it by printing a pair of glasses frames.	<ol style="list-style-type: none"> (1) Three DNNs were used (2) Use gradient descent algorithm to optimize and find appropriate disturbance (3) Facilitate physical realizability by using facial accessories and adjusting the mathematical formula of the attacker's target. 	Their attacks need to be improved in the face of black-box face recognition systems and the most advanced face detection systems.
Nicolas Papernot et al. 2017 [51]	Nicolas Papernot et al. propose a practical black-box attack based on a new substitute training algorithm which is using synthetic data generation to produce adversarial examples misclassified by black-box DNNs.	<ol style="list-style-type: none"> (1) Obtain the training set of the substitute detector (2) Select the appropriate substitute detector model structure (3) Iteratively train the substitute detector (4) Attack the substitute detector to generate adversarial example. 	Adversarial training can effectively defend against this black-box attack algorithm.
Shafahi et al. 2018 [52]	Ali Shafahi et al. introduce "clean-label" poisoning attacks, which do not require attackers to have any control over the labeling of training data. Moreover, in order to optimize the poisoning attack, a "watermark" strategy is proposed.	<ol style="list-style-type: none"> (1) Crafting poisoning data through feature conflict (2) The optimization algorithm uses the forward-backward-splitting iterative procedure (3) Add a low opaque watermark of the target instance to the poisoning instance to enhance the effect of poisoning attack. 	The attack method they proposed will cause the unchanged target instance to be misclassified as a basic, and the side effects of adversarial training are worthy of further study.
Mirsky et al. 2019 [53]	Yisroel Mirsky et al. construct a framework (CT-GAN) based on deep learning. In their strategies, attackers can use the framework to automatically tamper with 3D medical images, injecting/removing lung cancer into/from CT scans.	<ol style="list-style-type: none"> (1) Capture data using attack vectors (2) Select the location of injecting/removing cancer (3) Use 3D spline interpolation to scale (4) Equalization and standardization are achieved by means of histogram and formula (5) Create samples \rightarrow reverse preprocessing \rightarrow add Gaussian noise \rightarrow gain the complete slice \rightarrow repeat steps/return data. 	Medical scans are different from camera images, and further research on how to apply these techniques to detect attacks such as CT-GAN is needed.
Chen et al. 2019 [54]	Shang-Tse Chen et al. propose ShapeShifter, which uses physical perturbations to fool image-based target detectors like Faster R-CNN.	<ol style="list-style-type: none"> (1) In their strategies, by studying the Faster R-CNN algorithm, the nondifferentiability of the model was overcome, and gradient descent and backpropagation were successfully used to perform optimization-based attacks (2) ShapeShifter can generate adversarial perturbed stop signs, which are consistently misdetected by Faster R-CNN as other targets, posing a potential threat to computer vision systems. 	A series of experiments show that their attacks fail to transfer, and further research is needed in the future.
Xiao et al. 2019 [55]	Qixue Xiao et al. propose an attack to automatically generate camouflage images against image-scaling algorithms. Both white-box and black-box scenarios can be applied.	<ol style="list-style-type: none"> (1) The surjective function is applied to generate the attack image from the target image (2) Automatic scaling attack: get coefficient matrix; find the perturbation matrix (3) Disturbance is obtained through concave-convex optimization. 	Several defense strategies need further research and implementation.

TABLE 2: Continued.

Author	Solution	Coress	Shortcomings
Wang et al. 2020 [56]	Yajie Wang et al. describe a black-box attack method based on DNN object detection models, which is called evaporate attack. Moreover, experimental results show that their approach is superior to boundary attack on both 1-stage and 2-stage detectors.	<p>(1) In their research, the GA-PSO algorithm is designed to resolve the issue of attacking black-box object detector with only position and label information</p> <p>(2) Add pixel optimal position guidance and random Gaussian noise to the velocity iteration formula.</p>	If the model owner performs some processing on the output of the model (such as only provides the label of the object), the attack could be affected.
Solano et al. 2020 [57]	Jesús Solano et al. propose an intuitive attack method for mouse-based behavioral biometrics and compare it to black-box adversarial attack.	<p>(1) Feature engineering: angle feature, dynamic feature</p> <p>(2) Authentication system: a set of binary classification model is designed to recognize a specific user's MBB (mouse-based behavioral biometric recognition)</p> <p>(3) Attacks: provides SCRAP and adversarial machine learning black-box attack.</p>	An automated procedure for inverse feature calculation is needed to make the effectiveness of the comparative adversarial method more accurate.

TABLE 3: Text-based adversarial attack

Author	Solution	Cores	Shortcomings
Ebrahimi et al. 2018 [26]	Javid Ebrahimi et al. propose a method of generating white-box adversarial examples, HotFlip, to make the character-level classifier classification errors.	<ol style="list-style-type: none"> (1) Use beam search to find a set of operations (flip, insert, and delete) that obfuscate the classifier (2) Calculate the directional derivative of the operation using the gradient represented by the one-hot input vector to estimate the change in the loss. 	<p>Failure to evaluate the robustness of different character-level models for different tasks The context is not well considered.</p>
Gao et al. 2018 [28]	Ji Gao et al. introduce a new algorithm for generating text perturbed in black-box scenarios: DeepWordBug, which causes the deep learning classifier to misclassify text input.	<ol style="list-style-type: none"> (1) Use the scoring function to determine the importance of each word to the classification results and rank the words according to their ratings (2) Use the transformation algorithm to change the words selected. 	<p>This paper does not discuss the application of the algorithm in the white-box scenario.</p>
Cheng et al. 2018 [58]	In this paper, the Seq2Sick framework is proposed to generate adversarial examples for sequence-to-sequence (seq2seq) model. Nonoverlapping attack and targeted keywords attack are mainly studied.	<ol style="list-style-type: none"> (1) A projection gradient method is proposed to solve the discrete problem of input space (2) Adopting group lasso to enhance the sparsity of distortion (3) Developed a regularization technique to improve the success rate. 	<p>The success rate of targeted one-keyword attack is reduced when the model of subword transformation is attacked.</p>
Li et al. 2019 [30]	This paper proposes a general attack framework for generating adversarial text: TextBugger.	<ol style="list-style-type: none"> (1) White box: find the most important word through the Jacobian matrix, generate five types of bugs, and find the best one based on confidence (2) Black box: find the most important sentences first and then use the scoring function to find the most important words (3) Assessment: sentiment analysis and harmful content detection. 	<ol style="list-style-type: none"> (1) This paper only performs nontarget attack and does not involve target attack (2) The integration of defense systems based on language perception or structure perception can be further explored to improve robustness.
Hang et al. 2019 [59]	In this paper, Metropolis-Hastings sampling (MHA) is proposed to generate adversarial samples for natural language.	<ol style="list-style-type: none"> (1) Black-MHA: select words by traversing the index for conversion operation and select the most likely words according to the score (2) White-MHA: the difference between the white-box attack and the black-box attack is preselection, which introduces gradients into the score calculation. 	<ol style="list-style-type: none"> (1) It may produce incomplete sentences (2) Unrestricted entity and verb substitution also have a negative impact on the adversarial example generation of tasks (such as NLI).
Zang et al. 2020 [60]	In this paper, a new black-box adversarial attack model is proposed to solve the combinatorial optimization problem of word-level adversarial attack.	<ol style="list-style-type: none"> (1) A word substitution method based on the minimum semantic unit sememe is designed to reduce the search space (2) A search algorithm based on particle swarm optimization is proposed to search adversarial examples. 	<p>The improvement of robustness and the use of sememe in defense model need further study.</p>

TABLE 4: Malware-based adversarial attack.

Author	Solution	Cores	Shortcomings
Hu et al. 2017 [44]	This paper proposes a GAN-based malware adversarial example generation algorithm (MalGAN), which can bypass the detection model based on black-box machine learning.	<ol style="list-style-type: none"> (1) Sampling malicious examples (2) Generating adversarial examples (3) Sampling benign examples (4) Labeling (5) Updating the weights according to the gradient. 	This paper does not discuss the application of the algorithm in the white-box scenario.
Raff et al. 2017 [61]	Edward Raff et al. developed the first network architecture that could successfully process over 2 million steps of raw byte sequences.	<p>Architecture features:</p> <ol style="list-style-type: none"> (1) Expand with sequence length (2) The ability to consider local and global environments when examining the entire file (3) Helps to analyze the interpretive ability of flagged malware. 	The standardization of batch processing needs to be further explored.
Al-Dujali et al. 2018 [45]	This paper proposes the SLEIPNIR framework, which uses saddle-point optimization to learn the malware detection model of executable files represented by binary encoding features.	<ol style="list-style-type: none"> (1) Frame construction based on saddle-point optimization (2) Add randomization to the method (3) An on-line measurement method is introduced. 	No instructions were given on how to locate benign samples.
Kolosnjaji et al. 2018 [46]	This paper proposes a gradient-based evading attack.	<ol style="list-style-type: none"> (1) Adds a set of bytes to the end of the binary file to generate adversarial examples that do not break the malicious functionality of the source file (2) Initializes the iteration counter, repeatedly sets the number of filled bytes and calculates the gradient. 	The dataset is not large enough. The grain size is not fine.
Song et al. 2020 [47]	This paper presents a systematic framework for creating and evaluating real malware in order to achieve evasive attack.	<ol style="list-style-type: none"> (1) Adversarial example generation: design action set and verification function (2) Minimize action sequence (3) Feature interpretation. 	The defend methods and robustness of the framework are less discussed.
Rosenberg et al. 2020 [48]	In this paper, a black-box attack against API-based machine learning malware classifiers is proposed.	<ol style="list-style-type: none"> (1) Use valid parameters with no operation effect (2) Determine the increase in the number of API calls using the method of logarithmic transformation backtracking (3) Use GAN to select generated API calls (4) Use the adaptive evolutionary algorithm to realize the attack with high query efficiency based on the score. 	Defense mechanisms are not discussed.
Ebrahimi et al. 2020 [49]	This paper presents MalRNN, a novel deep learning-based approach to automatically generate evasive malware variants.	<ol style="list-style-type: none"> (1) Obtain data through system sampling (2) Learn the language model from benign malware binaries using character-level sequence-to-sequence RNN (3) Ensure the ability to generate malware variants 	<ol style="list-style-type: none"> (1) There is no discussion of defense mechanisms (2) The antivirus avoidance method is simple
Nguyen et al. 2020 [22]	Thien Duc Nguyen et al. demonstrate that federated learning-based IoT intrusion detection systems are vulnerable to backdoor attacks and proposed a new kind of data poisoning attack.	<p>By injecting a small amount of malicious data into the training process using only the compromised IoT device (rather than the gateway/client) and remaining undetected, the model is gradually backdoor.</p>	Existing defense methods are ineffective against this attack, so new defense mechanisms are needed to defend against it.

TABLE 4: Continued.

Author	Solution	Co-res	Shortcomings
Demetrio et al. 2020 [62]	Luca Demetrio et al. propose a general framework called RAMEn for performing black and white-box adversarial attacks on Windows malware detectors based on static code analysis.	<p>(1) Two new attacks—Extend and Shift—were proposed to extend the DOS header and transfer the contents of the first part, respectively, according to the adversarial load of the injection</p> <p>(2) The experimental results show that the proposed attack improves the tradeoff between the probability of avoidance and the number of bytes manipulated in the white-box and black-box attack settings.</p>	Attackers cannot arbitrarily add adversarial loads because proposed content injection attack must adhere to certain restrictions imposed by the format.
Chen et al. 2020 [63]	This paper presents Android HIV, an automated tool for creating adversarial examples on the Android Malware Detector based on machine learning.	<p>(1) Attack on MAMADROID: optimize the target function and modify the C&W algorithm; Jacobian matrix is calculated and JSMA algorithm is refined</p> <p>(2) Attack on DREBIN: generate adversarial examples based on Jacobin.</p>	There is no in-depth analysis of defense mechanisms against such attacks. Nor has the effectiveness of the different alternative model architectures been compared.

TABLE 5: AI security defense technology.

Type	Data collection phase	Phase Model train phase	Model usage phase
Evasive attack	Generating adversarial examples	Network distillation; adversarial training	Adversarial examples detection; input reconstruction; DNN model validation
Poisoning attack	Filtering training data; regression analysis	Integration analysis	
Back door attack		Model pruning	Input preprocessing
Model-stealing attack	Differential privacy	Privacy aggregation teacher model; model watermarking	

newly generated model but also enhance the accuracy and standardization of the model [67].

Ju et al. [68] propose E-ABS (analysis-by-synthesis) which can extend the ABS robust classification model to more complex image domains. The core contents include the following: (1) generation model: Adversarial Auto Encoder (AAE) is used to evaluate the class-conditional probability; (2) discriminative loss: use the discriminative loss during training to expose the conditional generation model to unevenly distributed samples; (3) variational inference: the ABS-like model estimates the likelihood of each category by maximizing the likelihood estimation; and (4) lower bound for the robustness of E-ABS: the lower bound of the nearest adversarial example to E-ABS is derived by using the ABS model. Nevertheless, the generation model is sensitive to image similarity measurements. And the reasoning and operation efficiency of ABS-like model on large datasets are low.

Chen et al. [69] are the first to evaluate and train the verifiable robust properties of PDF malware classifiers. They proposed a new distance metric in the PDF tree structure to construe robustness, that is, the number of different subtrees of depth 1 in two PDF trees. Furthermore, their experimental results show that the most advanced and new adaptive evolutionary attackers need 10 times the L0 feature distance and 21 times the PDF operation to evade the robustness model. However, the tradeoff between multiple robustness attributes and training costs needs further study.

4.1.2. Network Distillation. Distillation is a method of compacting the knowledge of a large network into smaller networks. Specialist models means, for a large network, multiple specialized networks can be trained to improve the model performance of the large network. The practice of distillation is generally to train a large model (teacher network) first and then heat the large model. The output of the large model is used as a soft target, and the real label of data is used as a hard target. The two are combined to train the small model (student network) [70].

The basic principle of the network distillation technique is to series multiple DNNs in the model training stage, in which the classification results generated by the former DNN are used to train the latter DNN. Papernot et al. [71] found that the transfer knowledge could reduce the sensitivity of the model to subtle disturbances to some extent and improve the robustness of the AI model. Therefore, network distillation technology is proposed to defend against evasive

attacks, and it is tested on MNIST and CIFAR-10 datasets. It is found that network distillation technology can reduce the success rate of specific attacks (such as JSMA and FGSM).

4.1.3. Adversarial Example Detection. The principle of adversarial example detection is to detect whether the example to be judged is an adversarial example by adding the detection component of the external detection model or the original model in the usage stage of the model. Before the input example reaches the original model, the detection model will determine whether it is an adversarial example. The detection model can also extract relevant information from each layer of the original model and synthesize various information to carry out detection. Various detection models may use different criteria to determine whether the input is an adversarial example [72].

Shumailov et al. [73] propose a new provable adversarial example detection protocol, the Certifiable Taboo Trap (CTT). They extended the Taboo Trap method. Moreover, three different CTT modes (CTT-lite, CTT-loose, and CTT-strict) are also discussed. However, this scheme cannot be used to defend against a specific adversarial example, thus resulting in a more flexible and universal defense mechanism.

4.1.4. Input Reconstruction. The principle of input reconstruction is that the input samples are transformed to resist evasive attack in the use stage of the model, and the transformed data will not affect the normal classification function of the model. Reconstruction methods include noising, denoising, preprocessing, gradient masking, and using auto-encoder to change the input examples [74]. At the same time, I think the metamorphosis of the sample has some similarities with the evolution of malicious code. Interestingly, 8 papers presented at the ICLR 2018 conference used gradient masking, but researchers quickly cracked 7 of them.

4.1.5. DNN Verification. Similar to software verification analysis technology, DNN verification technology uses solvers to verify various properties of DNN models, such as verifying that there is no adversarial example within a specific perturbation range. Nevertheless, the DNN model is usually verified as an NP-complete problem, and the efficiency of solver is low. Through selection and optimization, such as priority selection of model node validation, sharing of validation information, and validation by region, the operation efficiency of DNN verification can be further improved [75].

4.1.6. Data Augmentation. In reality, we often encounter the situation of insufficient data. The essence of data augmentation is to expand the original training set with generated adversarial samples when massive data is lacking, so as to ensure effective training of the model [76].

4.2. Defense Methods of Poisoning Attack

4.2.1. Training Data Filtering. This technique focuses on the control of the training dataset and uses detection and purification methods to prevent the poisoning attack from affecting the model. Specific directions include the following [77]: finding possible poisoning attack data points according to the label characteristics of the data and filtering these attack points during retraining; the model contrast filtering method was used to reduce the sampling data that could be used by poisoning attack, and the filtering data was used to against poisoning attack.

4.2.2. Regression Analysis. This technique is based on statistical methods that detect noise and outliers in datasets. Specific methods include defining different loss functions for the model to check outliers, using the distribution characteristics of data for detection [78], etc.

4.2.3. Ensemble Learning. Ensemble learning is to build and combine multiple machine learning classifiers to improve the ability of the machine learning system to resist poisoning attacks. Multiple independent models jointly constitute the AI system. And the possibility of the whole system being affected by the poisoning attack is further reduced due to the different training datasets adopted by multiple models [79].

Liao et al. [80] design an adaptive attack method to study the effectiveness of integrated defense based on transformation for image classification and its reasons. They propose two adaptive attacks to evaluate the integrated robustness of reversible transformation: TAA (adaptive attack based on transferability) and PAA (perturbation aggregation attack). Moreover, the ensemble evaluation method is used to evaluate the ensemble robustness of the irreversible transformation. However, the experimental results show that the integrated defense based on transformation is not enough to resist the antagonistic samples, the defense method is not reliable, and further efforts are needed.

4.2.4. Iterative Retraining. Iterative retraining refers to the iterative training of neural networks. Adversarial examples are generated according to any attack model and added to training data. Then, the neural network model is attacked, and the process is repeated [81].

4.3. Defense Methods of Back Door Attack

4.3.1. Input Preprocessing. The purpose of this method is to filter the input that can trigger the back door and reduce the risk of the input triggering the back door and changing the model judgment [82]. Data can be divided into discrete and continuous types. The image data is continuous and easy to encode as a numerical vector. The pretreatment operation is linear and differentiable, and there are many operation methods, such as mean standardization. Text data is discrete

and symbolized. The preprocessing operation is nonlinear and nondifferentiable. One-hot is generally used for pretreatment.

4.3.2. Model Pruning. Pruning in neural networks is inspired by synaptic pruning in the human brain. Synaptic pruning, complete decline and death of axons and dendrites, is a synaptic elimination process that occurs between childhood and the onset of puberty in many mammals, including humans. The principle of model pruning is to cut off the neurons of the original model appropriately, reducing the possibility of the backdoor neurons working under the condition that normal function is consistent. Using a fine-grained pruning method [83], the neurons that make up the backdoor can be removed, and the backdoor attack can be prevented.

4.4. Defense Methods of Model-Stealing Attack

4.4.1. PATE. The basic principle of PATE is to divide the training data into multiple datasets without intersection in the model training stage, and each set is used to train an independent DNN model (called teacher model). These independent DNN models are then used to vote together to train a student model [84]. This technology ensures that the judgment of the student model will not disclose the information of a particular training data, so as to ensure the privacy of the training data.

4.4.2. Differential Privacy. In the model training stage, the method is used to add noise to the data or the model training step by conforming to the differential privacy [85]. For example, Giraldo et al. [86] are the first to solve the adversarial classification problem in a system that uses differential privacy to protect the user's privacy. They find an optimal fake data injection attack that reduces the system's ability to detect anomalies, while allowing the attacker to remain undetected by "hiding" the fake data in the differential privacy noise. Besides, they design the optimal defense method to minimize the impact of such attack. They also show how the optimal DP-BDD (differential privacy-bad-data detection) algorithm achieves a Nash equilibrium between attackers trying to find the optimal attack distribution and defenders trying to design the optimal bad-data detection algorithm. Yet, the trade-offs between security, privacy, and practicality need to be further explored. Differential privacy adds noise to sensitive data or calculations performed on sensitive data to ensure privacy without unduly reducing the utility of the data.

4.4.3. Model Watermarking. The technique is to embed special labels in the original model during the model training stage. If a similar model is found, a special input sample can be used to identify whether the similar model was obtained by stealing the original model. Adi et al. [87] proposed a black-box deep neural network watermarking method. The robustness of the watermarking algorithm is evaluated under black-box and gray-box attacks.

In addition to the defensive measures mentioned above, there are other ways to improve the model's robustness against attacks, such as data compression, data randomization, data secondary sampling, outliers removal, model

TABLE 6: Common datasets for image adversarial attack.

Type of dataset	Data source	Application instances
Publicly accessible dataset	ImageNet	Xiao et al. 2019 [55]; Ma et al. 2019 [92]
	MNIST	Demontis et al. 2019 [20]; Ling et al. 2019 [93]; Fang et al. 2020 [94]; Ma et al. 2019 [92]; Moosavi-Dezfooli et al. 2016 [36]; Yang et al. 2019 [95]
	CIFAR-10	Ling et al. 2019 [93]; Shafahi et al. 2018 [52]; Ma et al. 2019 [92]; Moosavi-Dezfooli et al. 2016 [36]; Yang et al. 2019 [95]
	CH-MNIST; Fashion-MNIST; Breast Cancer Wisconsin	Fang et al. 2020 [94]
	VidTIMIT database	Korshunov et al. 2018 [96]
	WebFace; VGGFace2	Shan et al. 2019 [97]
	FaceScrub	Yang et al. 2019 [95]; Shan et al. 2019 [97]
	PubFig	Sharif et al. 2016 [50]; Shan et al. 2019 [97]
	Cora; Citeseer; Polblogs	Jin et al. 2020 [98]
	Social Face Classification (SFC) dataset	Taigman et al. 2014 [99]
	MS-COCO	Chen et al. 2019 [54]
	CelebA	Yang et al. 2019 [95]
	MS-COCO 2017; PASCAL VOC 2007; PASCAL VOC 2012	Wang et al. 2020 [56]
	Labeled Faces in the Wild (LFW) database	Demontis et al. 2019 [20]; Taigman et al. 2014 [99]; Ma et al. 2019 [92]
	YouTube Faces (YTF) dataset	Taigman et al. 2014 [99]
LIDC-IDRI dataset	Mirsky et al. 2019 [53]	
ILSVRC 2012	Simonyan et al. 2015 [100]; Moosavi-Dezfooli et al. 2016 [36]	
Commercial dataset	Fugazi	Din et al. 2018 [101]
Artificially generated dataset	Generated by toolkits manually	Yu et al. 2020 [102]

regularization, deep contractive network, biologically inspired conservation [32], attention mechanism [88], GAN-based, magnet [89], and high-level representation guided denoiser (HGD) [90].

Each of the above defense techniques has specific application scenarios and cannot completely defend against all the adversarial attacks. We can consider the above defense technology in parallel or serial integration to see whether the defense effect is better. For instance, data augmentation has the flexibility to easily plug in other defense mechanisms [91].

5. Additional Complements for Adversarial Machine Learning Research

Apart from focusing on the research methods of adversarial attack and defense, we also need to know other sides of this field.

5.1. The Choice of Dataset. By analyzing the already published articles, there are three types of datasets used in the adversarial machine learning research community currently. The common dataset for image adversarial machine learning research is shown in Table 6. The application of the text adversarial machine learning dataset is shown in Table 7.

And Table 8 shows the application of the malware adversarial machine learning dataset.

5.1.1. Publicly Accessible Dataset. At present, the majority of published papers use publicly accessible datasets from the Internet. These datasets are free to use and are maintained and updated by researchers in the field of computer science.

5.1.2. Commercial Dataset. Commercial datasets are generally not freely utilized or publicly available.

5.1.3. Artificially Generated Dataset. Other datasets are manually generated or crawled from the website by researchers using special tools.

5.2. General Adversarial Machine Learning Tools. Some commonly used tools can be used to assist experimental verification in the experimental phase of adversarial machine learning research. Common tools for adversarial ML include sandboxes, Python-based tools, and Java-based tools.

5.2.1. Sandbox. The Sandbox is a virtual system application that allows the user to run a browser or other application in a Sandbox environment, so the changes that result from running it can be deleted later. It creates a separate operating environment that restricts program behavior according to

TABLE 7: Common datasets for text adversarial attack.

Type of dataset	Data source	Application instances
Publicly accessible dataset	AG's news; SST	Ebrahimi et al. 2018 [26]; Sato et al. 2018 [103]
	IMDB	Gao et al. 2018 [28]; Zhang et al. 2020 [104]; Zang et al. 2020 [60]; Li et al. 2019 [105]; Neekhara et al. 2018 [104]
	SNLI	Zhang et al. 2020 [104]; Zang et al. 2020 [60]
	SST-2	Zang et al. 2020 [60]
	Enron spam emails	Gao et al. 2018 [28]
	Rotten Tomatoes Movie Reviews	Li et al. 2019 [105]
	DUC2003; DUC2004; IGAWORD	Cheng et al. 2020 [58]
Commercial dataset	Sogou News; DBPedia; Yahoo! Answers; Amazon Review	Sato et al. 2018 [103]
	Kaggle	Li et al. 2019 [105]

TABLE 8: Common datasets for malware adversarial attack.

Type of dataset	Data source	Application instances
Publicly accessible dataset	VirusShare; Citadel; APT1	Kolosnjaji et al. 2018 [46]; Al-Dujaili et al. 2018 [45]
	VirusTotal	Song et al. 2020 [47]; Huang et al. 2019 [106]; Suciu et al. 2019 [107]
	Drebin	Xu et al. 2020 [108]; Chen et al. 2020 [63]; Demontis et al. 2019 [20]; Arp et al. 2014 [109]
	https://malwr.com/	Hu et al. 2017 [44]
	NSL-KDD	Zhang et al. 2020 [110]
	MAMADROID	Chen et al. 2020 [63]
	EMBER	Suciu et al. 2019 [107]
Commercial dataset	MasterDGA; Alexa site	Alaeiyan et al. 2019 [111]
	The Kaggle Malware dataset of Microsoft	Salem et al. 2019 [112]; Yan et al. 2018 [113]
	McAfee Labs	Huang et al. 2019 [106]
	FireEye; Reversing Lab	Suciu et al. 2019 [107]
Artificially generated dataset	Microsoft's antimalware team	Stokes et al. 2018 [114]
Artificially generated dataset	Generated by toolkits manually	Suciu et al. 2019 [107]

security policies, and programs that run inside of it do not permanently affect the hard disk. In cyber security, a sandbox is a tool used to handle untrusted files or applications in an isolated environment. For instance, Hu et al. used the Cuckoo Sandbox to process malware samples.

5.2.2. Machine Learning Tools Based on Python. Python is regarded as the best suited programming language for ML. Therefore, a series of Python-based machine learning and deep learning tools have been developed by researchers in the adversarial ML.

5.2.3. TensorFlow. TensorFlow is an end-to-end open source machine learning platform. It has a comprehensive and flexible ecosystem of tools, libraries, and community resources that will help researchers drive the development of advanced machine learning technologies. Besides, it enables developers to easily build and deploy applications powered by machine learning.

5.2.4. Keras. Keras is a high-level neural network API written in Python. It runs with TensorFlow, CNTK, or Theano as a backend. The focus of Keras development is to support rapid experimentation. Being able to turn ideas into results with minimal delay is the key to carry out research. With it, deep network can be built quickly and training parameters can be selected flexibly.

5.2.5. PyTorch. PyTorch is based on Torch and is used for applications such as natural language processing. It is a tensor library optimized using GPU and CPU. Moreover, it can be regarded as a powerful deep neural network with automatic derivation function.

5.2.6. NumPy. NumPy is a basic package for scientific computing using Python. It can be used to store and process large matrices and support a large number of dimension arrays and matrix operations. In addition, it also provides a large number of mathematical libraries for array operations.

TABLE 9: The connections between papers.

Type	Author	Time/published in	Connection
Image	Mahmood Sharif et al. [50]	2016/CCS	In the field of image, papers of CCF A and B conferences and top journals in the field of security were selected, covering the papers of nearly five years from 2016 to 2020, involving offense and defense, and being able to understand the frontier research in the field of adversarial machine learning.
	Nicolas Papernot et al. [51]	2017/CCS	
	Ali Shafahi et al. [52]	2018/NIPS	
	Yossi Adi et al. [87]	2018/USENIX	
	Yisroel Mirsky et al. [53]	2019/USENIX	
	Shang-Tse Chen et al. [54]	2019/ECML PKDD	
	Qixue Xiao et al. [55]	2019/USENIX	
	Yajie Wang et al. [56]	2020/JNCA	
	Jesús Solano et al. [57]	2020/CCS	
	Chang Liao et al. [80]	2020/CCS	
Text	Iliia Shumailov et al. [73]	2020/CCS	In the field of text, 6 papers including [30] are selected, with [30] as the core. Among the 40 related papers, 6 papers are selected, among which three [26, 58, 115] quoted by [30] are cited by [59, 60].
	An Ju et al. [68]	2020/CCS	
	Javid Ebrahimi et al. [26]	2018/ACL	
	Ji Gao et al. [115]	2018/SPW	
	Minhao Cheng et al. [58]	2018/AAAI	
	Jinfeng Li et al. [30]	2019/NDSS	
Malware	Huangzhao Zhang et al. [59]	2019/ACL	These papers are about malware adversarial machine learning found through connected papers. Among them, [44–46] are the papers based on windows platform. [48] is the paper related to binary malware adversarial examples. [47, 49] are similar to the same review on Windows PE file generation adversarial examples. The remaining papers include top conference papers, top journal papers, and arXiv in the field of security, among which [69] is about robustness research paper.
	Yuan Zang et al. [60]	2020/ACL	
	Weiwei Hu et al. [44]	2017/arXiv	
	Edward Raff et al. [61]	2017/arXiv	
	Abdullah Al-Dujaili et al. [45]	2018/arXiv	
	Bojan Kolosnjaji et al. [46]	2018/arXiv	
	Wei Song et al. [47]	2020/arXiv	
	Ishai Rosenberg et al. [48]	2020/ACSAC	
	Mohammadreza Ebrahimi et al. [49]	2020/AAAI	
	Thien Duc Nguyen et al. [22]	2020/DISS	
Luca Demetrio et al. [62]	2020/arXiv		
Xiao Chen et al. [63]	2020/TIFS		
Yizheng Chen et al. [69]	2020/USENIX		

5.2.7. *Scikit-Learn*. Scikit-Learn is a machine learning tool based on Python with simplicity and efficiency. It can perform data mining and data analysis. Everyone can access it, and it is open source. It includes the following six basic functions: classification, regression, clustering, dimensionality reduction, model selection and preprocessing [115].

5.2.8. *Machine Learning Tools Based on Java*. Java-based machine learning platforms include WEKA, KNIME, and RapidMiner. WEKA provides Java’s graphical user interface, command-line interface, and Java API interface. It is probably the most popular Java machine learning library. Apache OpenNLP is a toolkit for processing natural language text. It provides methods for natural language processing tasks such as tokenization, segmentation, and entity extraction.

5.3. *The Connections between Papers*. Table 9 shows the relationships among some of the literatures listed in this paper.

6. Discussion

The competition between offense and defense in the security field is endless. The previous sections provide an introduction to adversarial attacks and defenses, so that the reader can learn about them. Next, there is our discussion and outlook in this area.

6.1. *Adversarial Example Generation Based on Malware*. First, let us introduce the “feature engineering” of malicious code:

- (1) Digital feature extraction: scale, normalize, and MinMaxScaler
- (2) Text feature extraction: word set model and word bag model
- (3) Data extraction: CSV is the most common format.

Adversarial machine learning is a widely used technique in the image domain. The adversarial attack technology in

the field of the image is becoming more and more mature. In the future, we plan research adversarial attack samples in the field of malicious code. Since the structure of malicious code is similar to that of text data, we can consider transferring the text adversarial attack algorithm to the field of malicious code. There are two main ways to generate text adversarial samples. One is to generate adversarial samples directly through text editing operations such as insert, delete, and replace by using the characteristics of the text. The other is to map the text data into continuous data and generate the adversarial samples by using some algorithms in the field of computer vision for reference. Yan et al. [116] propose a genetic algorithm-based malicious code adversarial sample generation method to static rewrite PE files. The atomic rewrite operation screened by the fuzzy test is similar to the text edit operation.

6.2. Adversarial Example Generation Based on Swarm Intelligence Evolutionary Algorithm. Swarm intelligence evolutionary algorithm is a heuristic computing method that simulates the swarm behavior of insects, birds, and fish in the biological world, including genetic algorithm, ant colony algorithm, particle swarm algorithm, and cultural algorithm. Currently, Liu et al., Yan et al. [116], and Wang et al. [56] have all generated adversarial samples by improving swarm intelligence evolutionary algorithm. However, the literature review found that there are few articles about the cultural algorithm, among which no one has conducted the research of adversarial sample generation based on cultural algorithm. This is one of our future research directions.

6.3. Malware Evolution. Adversarial sample generation in the domain of malicious code is, in my opinion, similar to the evolution of malicious code. In order to counter the network security protection system, malicious code makers continue to use new technologies and new methods to create new malicious code. As a result, the malicious code is constantly evolving to ensure that it can evade security systems. Taking the evolutionary process of a family sample as an example, the sample population within a family can be regarded as a spatiotemporal set sequence, and the sample sets generated at different stages have different functional characteristics. Samples within each set will adopt different evolutionary methods to carry out internal upgrading, and different sets will also adopt collaboration methods to carry out coevolution. The goal of its evolution is to ensure its continued survival ability and attack ability to complete destructive tasks under different network security protection environments. The generated adversarial samples can be seen as a form of evolution of the malicious code. More attention can be paid to this research in the future.

6.4. Improve the Transportability. Transportability does not mean that a program can be written without modification to any computer, but rather that a program can be written without many modifications when conditions change. Transportability is one of the system quality assurances. It reflects the universality of the model. And transportability means that an adversarial sample generated by a neural network

model on one dataset can also successfully attack another neural network model or dataset. Generally divided into three types: (1) the same architecture, different datasets (for example, both are based on Windows platform but use PE file and APK file, two types of datasets, respectively); (2) the same dataset with different architectures (for example, both are PE files but are applied to Windows and iOS architectures); and (3) different datasets and architectures. Although some models have successfully achieved portability, performance is still declining. Therefore, it is worth studying to improve the portability of the model.

6.5. Automation. Although some researchers have achieved automatic adversarial sample generation, many others craft adversarial samples manually. The artificial way is time-consuming and laborious and does not conform to the trend and new requirements of the development of The Times. In the future, with the efforts of researchers, I believe this problem will be greatly improved.

6.6. Possible Defensive Measures. In order to ensure system security in the field of AI, how to defend against attacks is the focus of current research. Many good researchers have designed powerful attacks but have not come up with effective countermeasures to defend them. The attack mentioned in this article must be carried out on the premise that the adversary can access the software or system. If the security of the access control is done well, it is helpful to protect the security of AI. In the stage of access control, identity authentication technology is one of the most important links. Secure multiparty computation (MPC) and homomorphic encryption (HE) are important privacy protection technologies in identity authentication systems [117–121]. I envision a combination of MPC and fully homomorphic encryption (FHE) to defend against attacks. MPC and FHE have high security. Zheng et al. [122] design and build Helen, a system that can achieve malicious security collaborative learning. They greatly reduced the model training time for achieving stochastic gradient descent (SGD) under MPC's SPDZ protocol by using the alternating direction multiplier method (ADMM) and singular value decomposition (SVD). Giraldo et al. [86] have solved the adversarial classification problem in a system that uses differential privacy to protect user privacy. Differential privacy is a noise-based MPC. Besides, the homomorphic encryption model is an effective way to improve data security and availability, which means the behaviors of users will not be leaked when trusted third parties help users process their data. To sum up, it is worth trying to combine secure multiparty computing and fully homomorphic encryption to defend against attacks. In addition, the blockchain technology has been mature and widely used in various fields, which can be regarded as a solution for examining malicious input and can be combined with MPC [123–125].

7. Comparison with Other Similar Reviews

As shown in Table 10, there are several similar surveys of the adversarial attack. The differences between this article and the other are as follows:

TABLE 10: Shortcomings of similar reviews.

Author	Main content	Shortcomings
Guofu Li et al. 2018 [126]	This article introduces the concepts and types of adversarial machine learning. It mainly reviews the attack and defense methods in the field of deep learning. And several new research directions, such as generative adversarial networks, are presented. The adversarial attack strategies in complex scenarios, such as reinforcement learning and physical attack, are also briefly recommended.	This paper mainly introduces the problem of image classification in the field of computer vision. There are few researches in the field of text and malware in the article. The research on the nonconvolutional structure is less, either.
Naveed Akhtar et al. 2018 [127]	This paper reviews the adversarial attack work of deep learning in computer vision. It mainly introduces the adversarial attack and defensive measures under deep learning. In addition, the security application literature provides a broader prospect for the research direction of adversarial attack in retrospect.	It mainly introduces the serious threat to deep learning models caused by perturbations to images in the field of computer vision. Examples of creating adversarial samples for text and malware classification are only briefly mentioned.
Shilin Qiu et al. 2019 [128]	This paper summarizes the latest research progress of adversarial attack and defense techniques in deep learning. It mainly reviews the adversarial attack of the target model in the training stage and the test stage and concludes the application of adversarial attack in the four fields of image, text, cyber space security, and physical world as well as the existing defense methods.	The adversarial attack is not analyzed in terms of the result of the attack.
Wei Emma Zhang et al. 2019 [129]	This paper is the first to make a comprehensive summary of the text deep neural network model adversarial attacks. It mainly reviews the adversarial attack and deep learning in the field of natural language processing, briefly introduces the defense methods, and discusses some open issues.	In this paper, the research of generating textual adversarial examples on DNNs in the field of natural language processing are summarized. However, it seldom introduces the architecture of deep neural network.
Wei Jin et al. 2020 [98]	This paper gives a comprehensive introduction to the research of graph neural network adversarial attack algorithm classification and defense strategy classification. The performance of different defense methods under different attacks is also empirically studied, and a repository of representative algorithms is developed.	It summarizes the adversarial attack and defense technology of graphic data but does not introduce the adversarial attack of other types of data.
Wenqi Wang et al. 2020 [130]	This essay comprehensively summarizes the research of textual adversarial examples in different fields. It mainly concludes the attack and defense classification of DNN in the text. Also, it discusses how to build a robust DNN model through testing and validation.	The adversarial attack and defense techniques in the field of images and malicious code are not analyzed.
Han Xu et al. 2020 [131]	This paper reviews the attack and defense methods on DNN models for image, graph, and text data. The algorithms and defense strategies for generating adversarial samples of three types of data are reviewed.	From the prospective of application field, image classification and natural language processing are introduced comprehensively, while malicious code detection is only briefly mentioned.
Jiliang Zhang et al. 2020 [132]	This paper gives a comprehensive summary of the existing adversarial example generation methods. This paper mainly introduces the basic concept of adversarial example, the comparison of different adversarial attack methods and defensive measures.	Like most reviews, this paper introduces and compares several typical attack algorithms such as L-BFGS, FGSM, and C&W. There is no introduction to adversarial attacks in the text and malicious code domains.

- (1) This paper follows the route of “Why? → What? → How?” and does not put forward any new concepts, intended to let beginners quickly enter the field of adversarial attack and defense under the guidance of this essay
- (2) This paper did not carry out adversarial attack studies from the L-BFGS method, FGSM-based attack, basic and least-likely-class iterative methods, JSMA attack, C&W method, and DeepFool method, as most of the review did. Instead, the research methods of adversarial attack are classified from the fields of image, text, and malicious code to assist researchers to discover the breakthrough point for their research
- (3) This paper is a systematic introduction of influential papers published after 2010 to ensure the advanced and comprehensive of the essay. Researchers can quickly find their interest points by browsing this article, improving the efficiency of the study.

8. Conclusions

In the field of AI security, it is a constant battle between attack and defense. To help researchers quickly enter the field of adversarial attack, this review is based on high-quality articles published since 2010. We summarize the typical adversarial attacks in the fields of text, images, and malware to help researchers locate their own research areas. Also, we introduce defense technologies against attacks. Finally, we present some discussions and open issues. Adversarial learning has a long history in the field of security. It is hoped that under the guidance of this paper, new researchers can effectively establish the framework of adversarial attack and defense.

Data Availability

Previously published articles were used to support this study, and these prior studies and datasets are cited at relevant places within the article.

Conflicts of Interest

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

Funding

This work was supported by the National Key Research & Development Program of China (2020YFB1712104), Major Scientific and Technological Innovation Projects of Shandong Province (2020CXGC010116), the National Natural Science Foundation of China (No. 61876019, No. U1936218, No. 62072037), and Zhejiang Lab (No. 2020LE0AB02).

References

- [1] Y. Gao, C. Xu, D. Wang, S. Chen, D. C. Ranasinghe, and S. Nepal, “STRIP: a defence against Trojan attacks on deep neural networks,” in *Proceedings of the 35th Annual Computer Security Applications Conference*, pp. 113–125, New York, NY, USA, 2019.
- [2] B. Biggio and F. Roli, “Wild patterns: ten years after the rise of adversarial machine learning,” *Pattern Recognit.*, vol. 84, pp. 317–331, 2018.
- [3] C. Esposito, M. Ficco, and B. B. Gupta, “Blockchain-based authentication and authorization for smart city applications,” *Information Processing & Management*, vol. 58, no. 2, p. 102468, 2021.
- [4] D. Li, L. Deng, B. B. Gupta, H. Wang, and C. Choi, “A novel CNN based security guaranteed image watermarking generation scenario for smart city applications,” *Information Sciences*, vol. 479, pp. 432–447, 2019.
- [5] C. Szegedy, W. Zaremba, I. Sutskever et al., “Intriguing properties of neural networks,” in *2nd International Conference on Learning Representations, ICLR 2014*, Banff, Canada, 2014 <https://nyuscholars.nyu.edu/en/publications/intriguing-properties-of-neural-networks>.
- [6] X. Liu, J. Zhang, Y. Lin, and H. Li, “ATMPA: attacking machine learning-based malware visualization detection methods via adversarial examples,” in *Proc. IEEE/ACM Int. Symp. Qual. Service*, Phoenix, AZ, USA, June 2019.
- [7] M. Zhou, J. Wu, Y. Liu, S. Liu, and C. Zhu, “DaST: data-free substitute training for adversarial attacks,” in *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Seattle, WA, USA, 2020.
- [8] Z. Guan, Z. Lv, X. Sun et al., “A differentially private big data nonparametric Bayesian clustering algorithm in smart grid,” *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 2631–2641, 2020.
- [9] J. Dong, Z. Guan, L. Wu, X. Du, and M. Guizani, “A sentence-level text adversarial attack algorithm against IIoT based smart grid,” *Computer Networks*, vol. 190, article 107956, 2021.
- [10] J. L. Di Wu, S. K. Das, J. Wu, Y. Ji, and Z. Li, “A novel distributed denial-of-service attack detection scheme for software defined networking environments,” in *2018 IEEE international conference on communications (ICC)*, Kansas City, MO, USA, 2018.
- [11] B. Zhou, J. Li, J. Wu, S. Guo, Y. Gu, and Z. Li, “Machine-learning-based online distributed denial-of-service attack detection using spark streaming,” in *IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA, 2018.
- [12] W. Han, J. Xue, Y. Wang, S. Zhu, and Z. Kong, “Review: build a roadmap for stepping into the field of anti-malware research smoothly,” *IEEE Access*, vol. 7, pp. 143573–143596, 2019.
- [13] N. Carlini, G. Katz, C. Barrett, and D. Dill, “Ground-truth adversarial examples,” 2017, <https://arxiv.org/abs/1709.10207>.
- [14] M. Nasr, R. Shokri, and A. Houmansadr, “Comprehensive privacy analysis of deep learning: passive and active white-box inference attacks against centralized and federated learning,” in *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 739–753, San Francisco, CA, USA, 2019.
- [15] W. Xiao, H. Jiang, and S. Xia, “A new black box attack generating adversarial examples based on reinforcement learning,” in *2020 Information Communication Technologies Conference (ICTC)*, pp. 141–146, Nanjing, China, 2020.

- [16] Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: integration of blockchain and edge computing," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 43–57, 2020.
- [17] Z. Katzir and Y. Elovici, "Why blocking targeted adversarial perturbations impairs the ability to learn," 2019, <https://arxiv.org/abs/1907.05718>.
- [18] A. Wu, Y. Han, Q. Zhang, and X. Kuang, "Untargeted adversarial attack via expanding the semantic gap," in *2019 IEEE International Conference on Multimedia and Expo (ICME)*, pp. 514–519, Shanghai, China, 2019.
- [19] H. S. Anderson, A. Kharkar, B. Filar, D. Evans, and P. Roth, "Learning to evade static PE machine learning malware models via reinforcement learning," 2018, <https://arxiv.org/abs/1801.08917>.
- [20] A. Demontis, M. Melis, M. Pintor et al., "Why do adversarial attacks transfer? Explaining transferability of evasion and poisoning attacks," in *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pp. 321–338, USA, 2019.
- [21] B. Wang, Y. Yao, S. Shan et al., "Neural cleanse: identifying and mitigating backdoor attacks in neural networks," in *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 707–723, San Francisco, CA, USA, 2019.
- [22] T. D. Nguyen, P. Rieger, M. Miettinen, and A.-R. Sadeghi, "Poisoning attacks on federated learning-based iot intrusion detection system," in *Workshop on Decentralized IoT Systems and Security (DISS) @ NDSS Symposium 2020*, pp. 23–26.02, San Diego, USA, 2020.
- [23] J. Monteiro, Z. Akhtar, and T. Falk, "Generalizable adversarial examples detection based on bi-model decision mismatch," in *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)*, pp. 2839–2844, Bari, Italy, 2019.
- [24] N. Papernot, P. McDaniel, A. Swami, and R. E. Harang, "Crafting adversarial input sequences for recurrent neural networks," in *MILCOM 2016-2016 IEEE Military Communications Conference*, pp. 49–54, Baltimore, MD, USA, 2016.
- [25] D. Jin and Z. Jin, *Text Fool: Fool your Model with Natural Adversarial Text*, 2019.
- [26] J. Ebrahimi, A. Rao, D. Lowd, and D. Dou, "Hot flip: white-box adversarial examples for text classification," in *Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics (Volume 2: Short Papers)*, pp. 31–36, Melbourne, Australia, 2018.
- [27] M. Alzantot, Y. Sharma, A. Elgohary, B.-J. Ho, M. Srivastava, and K.-W. Chang, "Generating natural language adversarial examples," in *Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing*, Brussels, Belgium, 2018.
- [28] J. Gao, J. Lanchantin, M. L. Soffa, and Y. Qi, "Black-box generation of adversarial text sequences to evade deep learning classifiers," in *2018 IEEE Security and Privacy Workshops (SPW)*, pp. 50–56, San Francisco, CA, USA, 2018.
- [29] Z. Zhao, D. Dua, and S. Singh, "Generating natural adversarial examples," 2018, <https://arxiv.org/abs/1710.11342>.
- [30] J. Li, S. Ji, T. Du, B. Li, and T. Wang, "Text bugger: generating adversarial text against real-world applications," in *Proceedings 2019 Network and Distributed System Security Symposium*, San Diego, CA, USA, 2019.
- [31] Y. Gil, Y. Chai, O. Gorodissky, and J. Berant, "White-to-black: efficient distillation of black-box adversarial attacks," in *Proceedings of the 2019 Conference of the North, Minneapolis, Minnesota*, 2019.
- [32] S. Das and P. N. Suganthan, "Differential evolution: a survey of the state-of-the-art," *IEEE Transactions on Evolutionary Computation*, vol. 15, no. 1, pp. 4–31, 2011.
- [33] D. C. Liu and J. Nocedal, "On the limited memory BFGS method for large scale optimization," *Mathematical Programming*, vol. 45, no. 1-3, pp. 503–528, 1989.
- [34] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," 2014, <https://arxiv.org/abs/1412.6572>.
- [35] N. Papernot, P. McDaniel, S. Jha, M. Fredrikson, Z. B. Celik, and A. Swami, "The limitations of deep learning in adversarial settings," in *2016 IEEE European Symposium on Security and Privacy (EuroSecP)*, pp. 372–387, Saarbruecken, Germany, 2015.
- [36] S. M. Moosavi-Dezfooli, A. Fawzi, and P. Frossard, "DeepFool: a simple and accurate method to fool deep neural networks," in *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 2574–2582, Las Vegas, NV, USA, 2016.
- [37] A. Kurakin, I. Goodfellow, and S. Bengio, "Adversarial examples in the physical world," in *Artificial Intelligence Safety and Security*, pp. 99–112, OpenReview.net, Toulon, France, 2016.
- [38] J. Su, D. V. Vargas, and K. Sakurai, "One pixel attack for fooling deep neural networks," *IEEE Transactions on Evolutionary Computation*, vol. 23, no. 5, pp. 828–841, 2019.
- [39] N. Carlini and D. Wagner, "Towards evaluating the robustness of neural networks," in *2017 IEEE Symposium on Security and Privacy (SP)*, pp. 39–57, San Jose, CA, USA, 2017.
- [40] S.-M. Moosavi-Dezfooli, A. Fawzi, O. Fawzi, and P. Frossard, "Universal adversarial perturbations," in *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 86–94, Honolulu, HI, USA, 2017.
- [41] S. Sarkar, A. Bansal, U. Mahbub, and R. Chellappa, "UPSET and ANGRI : breaking high performance image classifiers," 2017, <https://arxiv.org/abs/1707.01159>.
- [42] M. Cisse, Y. Adi, N. Neverova, and J. Keshet, "Houdini: fooling deep structured visual and speech recognition models with adversarial examples," *Advances in neural information processing systems*, vol. 30, 2017.
- [43] S. Baluja and I. Fischer, "Adversarial transformation networks: learning to generate adversarial examples," 2017, <https://arxiv.org/abs/1703.09387>.
- [44] W. Hu and Y. Tan, "Generating adversarial malware examples for black-box attacks based on GAN," 2017, <https://arxiv.org/abs/1702.05983>.
- [45] A. Al-Dujaili, A. Huang, E. Hemberg, and U. M. O'Reilly, "Adversarial deep learning for robust detection of binary encoded malware," in *2018 IEEE Security and Privacy Workshops (SPW)*, pp. 76–82, San Francisco, CA, USA, 2018.
- [46] B. Kolosnjaji, A. Demontis, B. Biggio et al., "Adversarial malware binaries: evading deep learning for malware detection in executables," in *2018 26th European Signal Processing Conference (EUSIPCO)*, pp. 533–537, Rome, Italy, 2018.
- [47] W. Song, X. Li, S. Afroz, D. Garg, D. Kuznetsov, and H. Yin, "Automatic generation of adversarial examples for interpreting malware classifiers," 2020, <https://arxiv.org/abs/2003.03100>.
- [48] I. Rosenberg, A. Shabtai, Y. Elovici, and L. Rokach, "Query-efficient black-box attack against sequence-based malware

- classifiers,” in *Annual Computer Security Applications Conference*, pp. 611–626, Austin, TX, USA, 2020.
- [49] M. Ebrahimi, N. Zhang, J. Hu, M. T. Raza, and H. Chen, “Binary black-box evasion attacks against deep learning-based static malware detectors with adversarial byte-level language model,” 2020, <https://arxiv.org/abs/2012.07994>.
- [50] M. Sharif, S. Bhagavatula, L. Bauer, and M. K. Reiter, “Accessorize to a crime: real and stealthy attacks on state-of-the-art face recognition,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1528–1540, Vienna, Austria, 2016.
- [51] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik, and A. Swami, “Practical black-box attacks against machine learning,” in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, pp. 506–519, Abu Dhabi, United Arab Emirates, 2017.
- [52] A. Shafahi, W. R. Huang, M. Najibi et al., “Poison frogs! Targeted clean-label poisoning attacks on neural networks,” 2018, <https://arxiv.org/abs/1804.00792>.
- [53] Y. Mirsky, T. Mahler, I. Shelef, and Y. Elovici, “CT-GAN: malicious tampering of 3D medical imagery using deep learning,” in *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pp. 461–478, USA, 2019.
- [54] S. T. Chen, C. Cornelius, J. Martin, and D. H. P. Chau, *Shape Shifter: Robust Physical Adversarial Attack on Faster R-CNN Object Detector: Recognizing Outstanding*, [Ph.D. thesis], Springer, 2019.
- [55] Q. Xiao, Y. Chen, C. Shen, Y. Chen, and K. Li, “Seeing is not believing: camouflage attacks on image scaling algorithms,” *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pp. 443–460, USENIX Association, Santa Clara, CA, 2019.
- [56] Y. Wang, Y. Tan, W. Zhang, Y. Zhao, and X. Kuang, “An adversarial attack on DNN-based black-box object detectors,” *Journal of Network and Computer Applications*, vol. 161, p. 102634, 2020.
- [57] J. Solano, C. Lopez, E. Rivera, A. Castelblanco, L. Tengana, and M. Ochoa, “SCRAP: synthetically composed replay attacks vs. adversarial machine learning attacks against mouse-based biometric authentication,” in *CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security*, pp. 37–47, 2020.
- [58] M. Cheng, J. Yi, P. Y. Chen, H. Zhang, and C. J. Hsieh, “Seq2-Sick: evaluating the robustness of sequence-to-sequence models with adversarial examples,” *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 34, no. 4, pp. 3601–3608, 2020.
- [59] H. Zhang, H. Zhou, N. Miao, and L. Li, “Generating fluent adversarial examples for natural languages,” in *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*, Florence, Italy, 2019.
- [60] Y. Zang, F. Qi, C. Yang et al., “Word-level textual adversarial attacking as combinatorial optimization,” in *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*, 2019.
- [61] E. Raff, J. Barker, J. Sylvester, R. Brandon, B. Catanzaro, and C. Nicholas, “Malware detection by eating a whole EXE,” 2017, <https://arxiv.org/abs/1710.09435>.
- [62] L. Demetrio, B. Biggio, G. Lagorio, F. Roli, and A. Armando, “Functionality-preserving black-box optimization of adversarial windows malware,” 2020, <https://www.semanticscholar.org/paper/32ff17fb274e7c455587c30cc092d42ccce53a80>.
- [63] X. Chen, C. Li, D. Wang et al., “Android HIV: a study of repackaging malware for evading machine-learning detection,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 987–1001, 2020.
- [64] D. Hendrycks and K. Gimpel, “Early methods for detecting adversarial images,” in *Proc. Int. Conf. Learn. Represent. (ICLR)*, pp. 1–9, Toulon, France, 2017.
- [65] J. Zhang, S. Peng, Y. Hu et al., “HRAE: hardware-assisted randomization against adversarial example attacks,” in *2020 IEEE 29th Asian Test Symposium (ATS)*, Penang, Malaysia, 2020.
- [66] “HUAWEI, ‘ai-security-white-paper-cn,’” <http://huawei.com/-/media/corporate/pdf/cyber-security/ai-security-white-paper-cn.pdf>.
- [67] J. Wang, T. Zhang, S. Liu et al., *Beyond Adversarial Training: Min-Max Optimization in Adversarial Attack and Defense*, 2019, <http://arxiv.org/abs/1906.03563>.
- [68] J. An and D. Wagner, “E-ABS: extending the analysis-by-synthesis robust classification model to more complex image domains,” in *CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security*, pp. 25–36, 2020.
- [69] Y. Chen, S. Wang, D. She, and S. Jana, “On training robust PDF malware classifiers,” in *29th USENIX Security Symposium (USENIX Security 20)*, pp. 2343–2360, 2020, <https://www.usenix.org/conference/usenixsecurity20/presentation/chen-yizheng>.
- [70] Z. Zhang and T. Wu, “Adversarial distillation for ordered top-k attacks,” 2019, <https://arxiv.org/abs/1905.10695>.
- [71] N. Papernot, P. McDaniel, X. Wu, S. Jha, and A. Swami, “Distillation as a defense to adversarial perturbations against deep neural networks,” in *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 582–597, San Jose, CA, USA, 2016.
- [72] A. G. Amato, “Adversarial examples detection in features distance spaces: subvolume B,” in *European Conference on Computer Vision*, Munich, Germany, 2019.
- [73] I. Shumailov, Y. Zhao, R. Mullins, and R. Anderson, “Towards certifiable adversarial sample detection,” in *Proceedings of the 13th ACM Workshop on Artificial Intelligence and Security*, pp. 13–24, USA, 2020.
- [74] S. Gu and L. Rigazio, “Towards deep neural network architectures robust to adversarial examples,” 2015, <https://arxiv.org/abs/1412.5068>.
- [75] Y. G. Qian, X. M. Zhang, B. Wang et al., “Towards robust DNNs: a Taylor expansion-based method for generating powerful adversarial examples,” 2020, <https://arxiv.org/abs/2001.08389>.
- [76] Y. Shi and Y. Han, “Schmidt: image augmentation for black-box adversarial attack,” in *2018 IEEE International Conference on Multimedia and Expo (ICME)*, pp. 1–6, San Diego, USA, 2018.
- [77] R. Laishram and P. V. V. Curie, *A Method for Protecting SVM Classifier from Poisoning Attack*, CoRR, 2016.
- [78] M. Jagielski, A. Oprea, B. Biggio, C. Liu, C. Nita-Rotaru, and B. Li, “Manipulating machine learning: poisoning attacks and countermeasures for regression learning,” in *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 19–35, San Francisco, CA, USA, 2018.
- [79] D. Li and Q. Li, “Adversarial deep ensemble: evasion attacks and defenses for malware detection,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3886–3900, 2020.

- [80] C. Liao, Y. Cheng, C. Fang, and J. Shi, "Where does the robustness come from?: a study of the transformation-based ensemble defence," in *Proceedings of the 13th ACM Workshop on Artificial Intelligence and Security*, pp. 1–12, USA, 2020.
- [81] S. KIM and H. Kim, "Zero-centered fixed-point quantization with iterative retraining for deep convolutional neural network-based object detectors," *IEEE Access*, vol. 9, pp. 20828–20839, 2021.
- [82] Y. Liu, X. Yang, and A. Srivastava, "Neural Trojans," in *2017 IEEE 35th International Conference on Computer Design (ICCD)*, Boston, MA, USA, 2017.
- [83] L. Kang, B. Dolan-Gavitt, and S. Garg, "Fine-pruning: defending against backdooring attacks on deep neural networks," in *International Symposium on Research in Attacks, Intrusions, and Defenses*, Springer, Cham, 2018.
- [84] N. Papernot, M. Abadi, U. Erlingsson, I. Goodfellow, and K. Talwar, "Semi-supervised knowledge transfer for deep learning from private training data," 2016, <https://arxiv.org/abs/1610.05755>.
- [85] M. Abadi, A. Chu, I. Goodfellow et al., "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, <https://dl.acm.org/doi/10.1145/2976749.2978318>.
- [86] J. Giraldo, A. Cardenas, M. Kantarcioglu, and J. Katz, "Adversarial classification under differential privacy," in *Network and Distributed System Security Symposium*, San Diego, California, 2020.
- [87] Y. Adi, C. Baum, M. Cisse, B. Pinkas, and J. Keshet, "Turning your weakness into a strength: watermarking deep neural networks by backdooring," in *27th {USENIX} Security Symposium ({USENIX} Security 18)*, USENIX Association, USA, 2018.
- [88] H. Yakura, S. Shinozaki, R. Nishimura, Y. Oyama, and J. Sakuma, "Neural malware analysis with attention mechanism," *Computers & Security*, vol. 87, pp. 101592.1–101592.15, 2019.
- [89] G. Machado, R. Goldschmidt, and E. Silva, "MultiMagNet: a non-deterministic approach based on the formation of ensembles for defending against adversarial images," in *21st International Conference on Enterprise Information Systems*, Heraklion, Crete, Greece, 2019.
- [90] F. Liao, M. Liang, Y. Dong, T. Pang, X. Hu, and J. Zhu, "Defense against adversarial attacks using high-level representation guided denoiser," in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Salt Lake City, UT, USA, 2018.
- [91] Z. Yi, J. Yu, S. Li, Y. Tan, and Q. Wu, "Incremental learning of GAN for detecting multiple adversarial attacks," in *Lecture Notes in Computer Science*, Springer, 2019.
- [92] S. Ma, Y. Liu, G. Tao, W.-C. Lee, and X. Zhang, "NIC: detecting adversarial samples with neural network invariant checking," in *Presented at the Network and Distributed System Security Symposium*, San Diego, CA, 2019.
- [93] X. Ling, S. Ji, J. Zou et al., "DEEPSEC: a uniform platform for security analysis of deep learning model," in *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 673–690, San Francisco, CA, USA, May 2019.
- [94] M. Fang, X. Cao, J. Jia, and N. Gong, "Local model poisoning attacks to byzantine-robust federated learning," *29th {USENIX} Security Symposium ({USENIX} Security 20)*, USENIX Association, 2019.
- [95] Z. Yang, J. Zhang, E.-C. Chang, and Z. Liang, "Neural network inversion in adversarial setting via background knowledge alignment," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 225–240, London United Kingdom, 2019.
- [96] P. Korshunov and S. Marcel, "Deep Fakes: a new threat to face recognition? Assessment and detection," 2018, <https://arxiv.org/abs/1812.08685>.
- [97] S. Shan, E. Wenger, J. Zhang, H. Li, H. Zheng, and B. Y. Zhao, "Fawkes: protecting privacy against unauthorized deep learning models," *29th {USENIX} Security Symposium ({USENIX} Security 20)*, USENIX Association, 2020.
- [98] W. Jin, Y. Li, H. Xu, Y. Wang, and J. Tang, "Adversarial attacks and defenses on graphs: a review and empirical study," 2020, <https://arxiv.org/abs/2003.00653>.
- [99] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "Deep face: closing the gap to human-level performance in face verification," in *2014 IEEE Conference on Computer Vision and Pattern Recognition*, pp. 1701–1708, Columbus, OH, USA, 2014.
- [100] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2015, <https://arxiv.org/abs/1409.1556>.
- [101] Z. A. Din, H. Venugopalan, and J. Park, "Boxer: preventing fraud by scanning credit cards," in *29th USENIX Security Symposium (USENIX Security 20)*, pp. 1571–1588, USENIX Association, 2020, <https://www.usenix.org/conference/usenixsecurity20/presentation/din>.
- [102] H. Yu, K. Yang, T. Zhang, Y.-Y. Tsai, T.-Y. Ho, and Y. Jin, "Cloud leak: large-scale deep learning models stealing through adversarial examples," in *presented at the Network and Distributed System Security Symposium*, San Diego, CA, 2020.
- [103] M. Sato, J. Suzuki, H. Shindo, and Y. Matsumoto, "Interpretable adversarial perturbation in input embedding space for text," in *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence*, Stockholm, 2018.
- [104] P. Neekhara, S. Hussain, S. Dubnov, and F. Koushanfar, "Adversarial reprogramming of text classification neural networks," in *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP)*, Hong Kong, China, 2018, <https://arxiv.org/abs/1809.01829>.
- [105] D. Li, D. V. Vargas, and K. Sakurai, "Universal rules for fooling deep neural networks based text classification," in *2019 IEEE Congress on Evolutionary Computation (CEC)*, pp. 2221–2228, Wellington, New Zealand, 2019.
- [106] Y. Huang, U. Verma, C. Fralick, G. Infante-Lopez, B. Kumar, and C. Woodward, "Malware evasion attack and defense," in *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, pp. 34–38, Portland, OR, USA, 2019.
- [107] O. Suci, S. E. Coull, and J. Johns, "Exploring adversarial examples in malware detection," in *2019 IEEE Security and Privacy Workshops (SPW)*, pp. 8–14, San Francisco, CA, USA, 2019.
- [108] P. Xu, B. Kolosnjaji, C. Eckert, and A. Zarras, "MANIS: evading malware detection system on graph structure," in

- Proceedings of the 35th Annual ACM Symposium on Applied Computing*, New York, NY, USA, 2020.
- [109] D. Arp, M. Spreitzenbarth, M. Hübner, H. Gascon, and K. Rieck, "Drebin: effective and explainable detection of Android malware in your pocket," in *Presented at the Network and Distributed System Security Symposium*, San Diego, CA, 2014.
- [110] S. Zhang, X. Xie, and Y. Xu, "A brute-force black-box method to attack machine learning-based systems in cybersecurity," *IEEE Access*, vol. 8, pp. 128250–128263, 2020.
- [111] M. Alaeiyan and S. Parsa, "Detection of algorithmically-generated domains: an adversarial machine learning approach," *Computer Communications*, vol. 160, pp. 661–673, 2020.
- [112] A. Salem, Y. Zhang, M. Humbert, P. Berrang, M. Fritz, and M. Backes, "ML-Leaks: model and data independent membership inference attacks and defenses on machine learning models," in *presented at the Network and Distributed System Security Symposium*, San Diego, CA, 2019.
- [113] J. Yan, Y. Qi, and Q. Rao, "Detecting malware with an ensemble method based on deep neural network," *Security and Communication Networks*, vol. 2018, Article ID 7247095, 16 pages, 2018.
- [114] J. W. Stokes, D. Wang, M. Marinescu, M. Marino, and B. Bussone, "Attack and defense of dynamic analysis-based, adversarial neural malware detection models," in *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*, pp. 1–8, Los Angeles, CA, USA, 2018.
- [115] "scikit-learn," <https://scikit-learn.org.cn/>.
- [116] Y. A. N. Jia, Y. A. N. Jia, N. I. E. Chujiang, and S. U. Purui, "Method for generating malicious code adversarial samples based on genetic algorithm," *Journal of Electronics and Information Technology*, vol. 42, no. 9, pp. 2126–2133, 2020.
- [117] H. Krawczyk, "HMQV: a high-performance secure Diffie-Hellman protocol," in *Advances in Cryptology-CRYPTO 2005: 25th Annual International Cryptology Conference*, Santa Barbara, California, USA, 2005.
- [118] D. Wang, W. Li, and P. Wang, "Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4081–4092, 2018.
- [119] S. Qiu, D. Wang, G. Xu, and S. Kumari, "Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2020.
- [120] D. Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bound," *IEEE Transactions on Dependable & Secure Computing*, vol. 15, no. 4, pp. 708–722, 2018.
- [121] S. Qiu, G. Xu, H. Ahmad, and L. Wang, "A robust mutual authentication scheme based on elliptic curve cryptography for Telecare medical information systems," *IEEE Access*, vol. 6, pp. 7452–7463, 2018.
- [122] W. Zheng, R. A. Popa, J. E. Gonzalez, and I. Stoica, "Helen: maliciously secure cooperative learning for linear models," in *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 724–738, San Francisco, CA, USA, May 2019.
- [123] M. Pawlicki, M. Chora, and R. Kozik, "Defending network intrusion detection systems against adversarial evasion attacks," *Future Generation Computer Systems*, vol. 110, no. 11, pp. 148–154, 2020.
- [124] W. Li, Y. Wang, J. Li, and M. H. Au, "Toward a blockchain-based framework for challenge-based collaborative intrusion detection," *International Journal of Information Security*, vol. 20, no. 2, pp. 127–139, 2021.
- [125] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: a review," *IEEE Access*, vol. 6, pp. 10179–10188, 2018.
- [126] G. Li, P. Zhu, J. Li, Z. Yang, N. Cao, and Z. Chen, "Security matters: a survey on adversarial machine learning," 2018, <https://www.semanticscholar.org/paper/6ede8b02b817a1354b8bde1ab7af07b0ddb02acf>.
- [127] N. Akhtar and A. Mian, "Threat of adversarial attacks on deep learning in computer vision: a survey," *IEEE Access*, vol. 6, pp. 14410–14430, 2018.
- [128] S. Qiu, Q. Liu, S. Zhou, and C. Wu, "Review of artificial intelligence adversarial attack and defense technologies," *Applied Sciences*, vol. 9, no. 5, p. 909, 2019.
- [129] W. E. Zhang, Q. Z. Sheng, A. Alhazmi, and C. Li, "Adversarial attacks on deep learning models in natural language processing: a survey," 2019, <https://arxiv.org/abs/1901.06796>.
- [130] W. Wang, L. Wang, R. Wang, Z. Wang, and A. Ye, "Towards a robust deep neural network in texts: a survey," 2020, <https://arxiv.org/abs/1902.07285>.
- [131] H. Xu, Y. Ma, H. C. Liu et al., "Adversarial attacks and defenses in images, graphs and text: a review," *International Journal of Automation and Computing*, vol. 17, no. 2, pp. 151–178, 2020.
- [132] J. Zhang and C. Li, "Adversarial examples: opportunities and challenges," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 7, pp. 2578–2593, 2020.