IJNS
International Journal of Network Security

ISSN 1816-353X (Print)
ISSN 1816-3548 (Online)

Vol. 26, No. 2 (March 2024)

INTERNATIONAL JOURNAL OF NETWORK SECURITY

PUBLISHING OFFICE

Min-Shiang Hwang
Department of Computer Science & Information Engineering, Asia University, Taichung 41354, Taiwan, R.O.C.
Email: mshwang@asia.edu.tw

International Journal of Network Security is published both in traditional paper form (ISSN 1816-353X) and in Internet (ISSN 1816-3548) at http://ijns.jalaxy.com.tw

PUBLISHER: Candy C. H. Lin

Volume: 26, No: 2 (March 1, 2024)

International Journal of Network Security

A Study on Cypher Assignment Based on Secrecy Capacity

Cheng-Ying Yang[1], Jong-Shin Chen[2], Jenq-Foung JF Yao[3], and Min-Shiang Hwang[4,5]
(Corresponding author: Min-Shiang Hwang)
Department of Computer Science, University of Taipei, Taipei, Taiwan[1]
Department of Information and Communication Engineering, Chaoyang University of Science and Technology, Taiwan[2]
Computer Science, Georgia College and State University, Milledgeville, USA[3]
Department of Computer Science & Information Engineering, Asia University[4]
Fintech and Blockchain Research Center, Asia University, Taiwan (R.O.C.)[5]
500, Lioufeng Rd., Wufeng, Taichung 41354, Taichung, Taiwan (R.O.C.)
Email: mshwang@asia.edu.tw
(Received Oct. 10, 2023; Revised and Accepted Feb. 2, 2024; First Online Feb. 17, 2024)

Abstract

Accessing wireless services is convenient but not secure. The issue of privacy and security is highly demanded on the internet. The information is sent with the undesired threats of eavesdroppers. Secure communication enables the desired receiver to correctly and successfully receive the information without interruption. In the meantime, a secure system protects the transmitted information from the eavesdroppers. Traditionally, encryption, authorization, and authentication schemes could be employed to protect from eavesdroppers. However, the unanticipated attacks have been developing. According to Shannon's perfect communication, the undesired receivers, such as eavesdroppers, could receive an error-free cryptogram. Based on the physical-layer security, it could be expected that secure communication could be implemented without complex computing at the higher level. The physical-layer security coding scheme aims to achieve an extremely low decoding error probability and obtain a critical security level against attackers. The positive secrecy capacity (secrecy rate) could provide secure communication. Hence, a positive secrecy capacity is the primary concern in the system. Besides, physical-layer security coding is not only to help the system achieve a critical level of security but also to obtain an extremely low decoding error probability. However, it decreases the bandwidth efficiency and suffers the system performance. Hence, the tradeoff between the security level and the coding rate is important to lead a secure communication.

Keywords: Bandwidth Efficiency; Physical-Layer Security; Secrecy Capacity; Shannon Perfect Communication

1 Introduction

Recently, mobile devices could access the wireless communications for internet services conveniently. It leads a lot of mobile users and requests for the more services, such as navigation service. However, the wireless transmission is an open but unsecure environment. The issue of privacy and security are highly demanded in the internet. There exist many security threats of eavesdropper on the link between the source station and the destination station. Hence, the security performance of the system is suffered. The objective of a secure communication enables the authentic destination station successfully to receive the correct information. At the meantime, a secure system protects the secret information away from the eavesdroppers and ensures the desired receiver to obtain this information. For the purpose of security, the eavesdropper detection could be the practical solution [1]. However, to detect and to identify the eavesdroppers are difficult works. Traditionally, the encryption is used to protect the eavesdroppers even though the eavesdroppers could receive the same data stream. Besides, a secure system employs the access control schemes with the authorization and authentication schemes [2–4]. These schemes are adopted under the assumption of limited computing resources that the attackers have. Moreover, the unanticipated attacks have been developing. Usually, in the higher-network layer, it adopts the encryption scheme. Without the hardware infrastructure, the complex and difficult encryption schemes could not be developed. For the device with a lower computing resource, such as IoT (Internet of Things), it is not appropriate to apply with encryption scheme [5, 6]. According to Shannon's perfect secrecy [7], it could provide an error-free cryptogram for the open access. Hence, it is expected that the physical-layer coding scheme could

offer a secure communication [8, 9].

The physical-layer coding security comes from the wire-tap channel model [10]. The coding scheme attempt to approach an extremely low error decoding probability at the desired destination. At the same time, this coding scheme provide a critical level of security. Coupling with cryptographic schemes, the scheme gives the solution for the secure communication [11]. The coupling promises the code individually provides error correction because of interference, but allows the coding scheme functions as a security enhancement. The scheme supposes the attackers are confused because of codewords. In Shannon's theorem [7], the positive secrecy capacity could provide a perfect communication. If the mutual information between the source station and the destination station is larger than that between the source station and the eavesdropper, there exists a positive secrecy capacity. In the information theory [12], the mutual information is related to the source entropy and the conditional entropy in the receiver. For the perfect communication, one solution is to maximize the mutual information between the source and the destination but also to minimize that between the source and the eavesdroppers. For the source information, the amount of entropy depends on the probability distribution of source. However, under the wire-tap channel assumption [13] the distorted codeword (cypher) leads the conditional entropy of source given in the codeword. Hence, the codeword mapping is the initial concern in this work.

Not only the physical-layer security coding obtains a critical level of security to against the eavesdroppers, but also benefits to achieve an extremely low error probability at the desired destination [13, 14]. Under the noisy transmission, the destination station receives the distorted signal. It might lead the received the distorted signal and might make decoded error. Also, it degrades the bandwidth efficiency because of coding. Coding rate is the index to evaluate the bandwidth efficiency. Generally, the scheme with a higher coding rate suffers the system performance of decoding error. Hence, he this work concentrates to maximize the mutual information between the codeword and the received information to ensure the secure communication. Therefore, the objective of this work is to analyze the tradeoff between the security and bandwidth efficiency in the physical security coding scheme. In Section 2, based on the information theorem, it describes the secure communication system. Section 3 gives the cypher assignment scheme and the secrecy capacity analysis. Section 4 proposed the coding implementation scheme. Finally, the conclusion is given.

2 Information In Secure Communications

In the wireless communication system, the data are transmitted in the open environment. Each one, including eavesdroppers, could receive the same data. For the concerns of security, it is realized to avoid the undesired receivers. It is reasonable nut difficult to detect who the eavesdroppers are. Instead of detecting the eavesdropper, using cypher to forward the transmitted information might be the solution. In the cryptology, if one wants to protect the confidentiality of data, one transforms the data (denoted as the information X) under control of a secret key K with the encryption algorithm into the cypher C, i.e. $C = E_K(X)$. Without the noisy disruption, the recipient can decrypt the cypher C with the decryption algorithm to obtain the plaintext or $Y = D_K(C) = X$. Access control with authorization and authentication schemes is employed in the secure system [2–4]. The security mechanism, similar to that with cryptology, the physical layer security coding could be implemented efficiently with consideration of cost. Consider a communication system shown in Figure 1.

According to Figure 1, the source X is assigned (coded) to be codeword C. It could be illustrated in Figure 2.

For a possibly mapping from the source X, the codevector c has the probability

$$p(c_j) = \sum_i p(x_i)p(c_j|x_i). \tag{1}$$

The entropy of distorted codeword C is

$$H(C) = \sum_j p(c_j) \log \frac{1}{p(c_j)} \tag{2}$$

The conditional entropy between the information source and codeword

$$H(C|X) = \sum_i p(x_i) \sum_j p(c_j|x_i) \log \frac{1}{p(c_j|x_i)} \tag{3}$$

The mutual information between X and C becomes

$$\begin{aligned} I(C;X) &= H(X) - H(X|C) \\ &= H(C) - H(C|X) \\ &= I(X;C). \end{aligned} \tag{4}$$

On the other hand,

$$\begin{aligned} I(X;C) &= \sum_i \sum_j p(x_i, c_j) \log \frac{p(c_j|x_i)}{p(c_j)} \\ &= \sum_i \sum_j p(x_i, c_j) \log \frac{p(c_j, x_i)}{p(c_j)p(x_i)} \end{aligned} \tag{5}$$

At the destination, the received information denotes Y. Since the received information Y is related to the information source, distorted because of noisy channel, the information $I(X;Y)$ should be positive. Within the coding scheme, it is expected the codeword C to compress X as much as possible. However, in the reliable transmission, it needs as much of the information about Y as possible. The amount of information about Y given under the distorted codeword C is given by

$$\begin{aligned} I(C;Y) &= \sum_k \sum_j p(c_j, y_k) \log \frac{p(c_j, y_k)}{p(c_j)p(y_k)} \\ &\leq I(X;Y). \end{aligned} \tag{6}$$

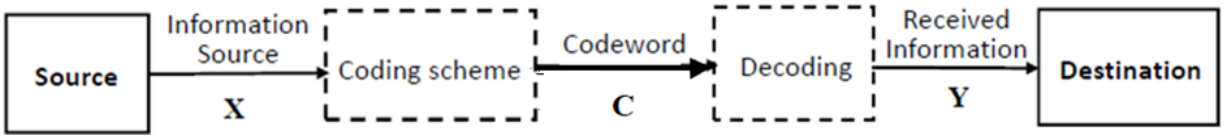


Figure 1: Secure communication system

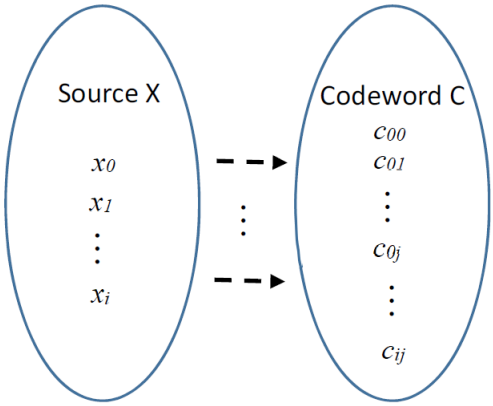


Figure 2: Codeword assignment from the source X

It is obvious that the codeword could not carry the more information than that from the original source. For the secure communication, it leads the maximum the mutual information between C and Y. In Equation (6), there exists a tradeoff between the codeword and the source information. It leads the information is equal at the source X and that at the codeword. With the coding scheme, it is feasible way to deal is to keep a fixed amount of information on Y at the destination and to minimize the information of codeword C. In other words, it needs the maximum the information of codeword C under the source X and minimum the information of codeword C under the condition of the destination Y, as shown in Figure 3.

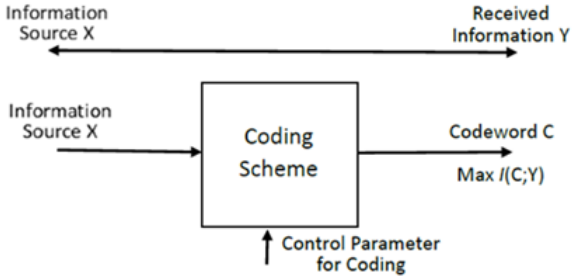


Figure 3: Maximum I(C;Y) with codeword mapping scheme

Hence, the secure transmission could be achieved with the codeword mapping scheme. It is the idea that the source X is coded to the codeword according to the coding scheme with a control parameter [15]. The received information is chosen properly from the received codeword. Initially, the concept of code mapping is to design a function, $C = f(X)$ in a signal processing algorithm. The mapping is typically considered as a table which stored the respective codeword C for each possible information of source X. While the table approach a suitable situation, the application of secure communication could be hold. For example, for a large information sources, the table implementation becomes large according to the coding scheme. It could be thought that the coding scheme is a function corresponding to and denotes as $C = f\theta(X)$ with M parameters $\theta = [\theta_0, \theta_1, \cdots, \theta_{M-1}]$ that optimize the maximum mutual information $I(C;Y)$ in Equation (6).

3 Cypher Assignment

The perfect secrecy makes the theoretical limitation for error-free cryptogram. In fact, physical-layer security coding scheme leads to realize the positive secrecy capacity is the requirement to achieve the level of security [8]. Channel coding is designed to make reliable communications by adding redundant bits to the transmitted data for error detection or error correction. The redundancy is added to the source information to become a codeword. Let l be the number bits of source message and n be the number bits of the codeword. The coding rate for the coding is $R = l/n$ and the code denotes (l, n) code. According to Shannon theory, if the coding rate, if the coding rate of the code is less than the channel capacity, there exists a coding scheme with an extremely low error probability of decoding. Moreover, a physical-layer security code is designed to obtain not only the extremely low error probability of decoding but also to provide a certain level of security against eavesdroppers. Based on the theoretical physical layer security, the secrecy capacity is based on satisfying the low error probability and preventing from the eavesdroppers.

In the system, three random variables, the information source X, distorted codeword (codevector) C and received information Y are considered. These three random variables X, C, Y to form a theoretical chain. Let the information source X with probability $p(x)$ and the distorted codeword space denote C. According to Shannon Secrecy Capacity [7], the positive secrecy capacity C_s should be kept for the secure communication, i.e.

$$C_s \geq I(X;Y) - I(X;C). \tag{7}$$

Bsed on the equal equation in Equation (7), for the secret communication, the coding scheme, one-time pad encryption, it meets the least requirement. In one-time pad encryption [16], the key is kept as long as the source. The code mapping belongs to one-to-one, i.e. $j = 0$ in Figure 2. Also, the interleaving coding scheme with the purpose of error control contributes the secure communication with the same characteristic that one-time pad scheme does. [17]. In the interleaving coding, the number bits of source message are equal to be the number bits of the codeword. It could function as one-time pad encryption does. Besides, if a multiple assignment scheme is chosen for code mapping, it will increase the information of the codeword. For example, binary sources are coded by using m-bit codeword assignment, i.e. $i = 1$, $j = m$. Figure 4 shows the secrecy capacity for the multiple assignment.

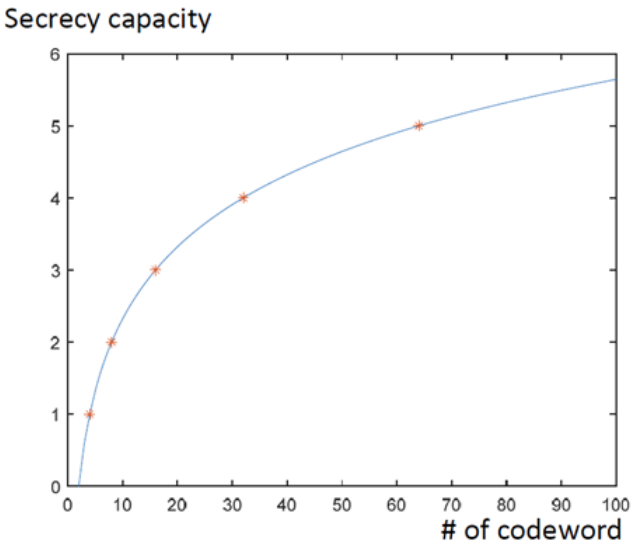


Figure 4: Increasing the number of codewords to increase the secrecy capacity

On the other hand, the coding rate R is related to the bandwidth efficiency and transmission error probability. The lower coding rate could approach to lower error transmission rate. Under the transmission bandwidth limitation, Figure 5 shows the relationship between the secrecy capacity and the coding rate.

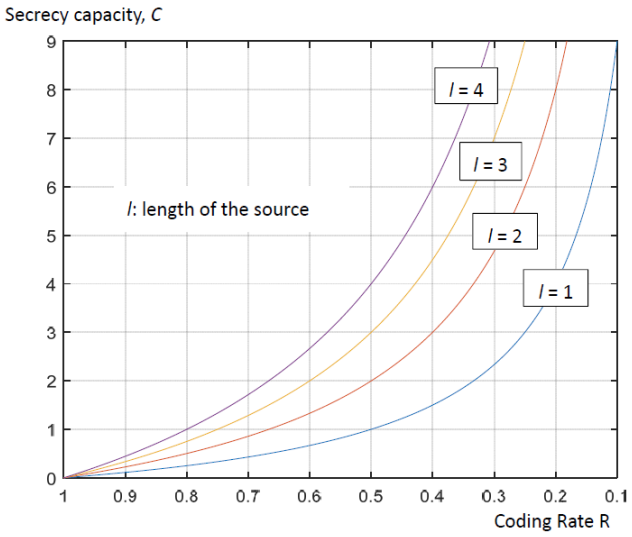


Figure 5: Secrecy capacity increasing with coding rate decreasing

4 Coding Implementation

According to Figure 2, to achieve the maximum information, the codeword should be generated with the equal probability. Hence, based on the binary bit assignment, the length of codword is equal and larger than that of the source. If there are n symbols in the source, with codeword assignment scheme, the maximum information of codeword could be approach as that shown in Figure 6.

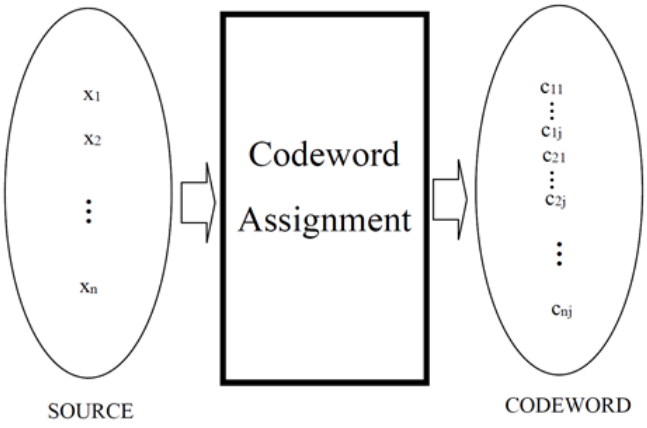


Figure 6: Codeword (Cypher) assignment

If the length of codword is equal to that of the source, i.e. $j = 0$, the numbers of the source are equal to the numbers of codeword, codeword assignment is proposed with one-to-one random assignment scheme. The interleaving coding is an example. In the scheme, the codeword is generated with the position change for those bits in the source code. One-time pad coding is another scheme with the spreading the secret key. These schemes keep the equal length of source and that of codeword. It leads the zero-secrecy rate and provides the minimum requirement for the secure communication.

For each source, the codeword encoding adopts the multiple assignment scheme. For the codeword subset, the codeword subset $\{c_{i1}, c_{i2}, \cdots, c_{ij}\}$ is assigned for the source xi, as that shown in Figure 7.

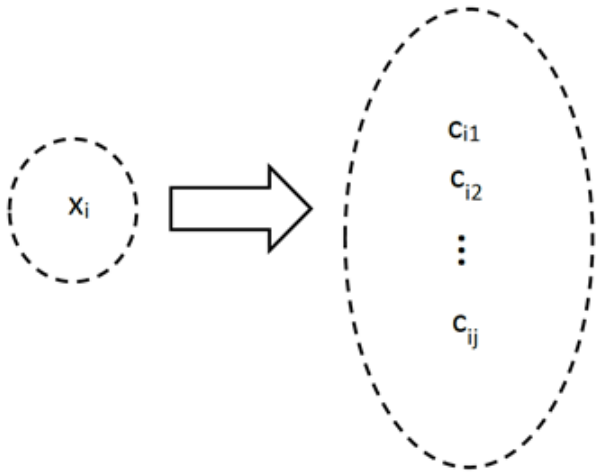


Figure 7: Multiple codeword assignment

All the eigen-vectors of the codeword c_{ij} are corresponding to the source x_i. Hence, the decoding procedure could be implemented according to the eigen-vector calculation of received codeword.

5 Conclusion

The issue of privacy and security becomes important in the wireless environment. This work intends to realize using physical layer coding scheme to improve the secrecy capacity. In fact, the channel coding scheme is used to resist the imperfect transmission environment and to reduce the transmission error. Especially, in the fading channel, it is useful to employ the coding scheme to reduce the suffering because of impact of unstable channel. However, it also provides the opportunity to increase the secrecy capacity and enhance the performance of secret communication. Multiple codeword assignment scheme proposed to increase the secrecy capacity to enhance the critical level of security. Besides, multiple assignment applying with AI algorithm for help to group the codeword subset for the source might be a practical application of the coding/decoding scheme. To develop the effective AI algorithm for coding scheme might be the research topics in the future.

Acknowledgments

The Ministry of Science and Technology partially supported this research, Taiwan (ROC), under contract no.: NSTC 109-2221-E-468-011-MY3, NSTC 111-2622-8-468-001-TM1, NSTC 110-2221-E-845-002, and MOST 111-2221-E-845-003.

References

[1] Rahim, T. Qiu, Z. Ning, J. Wang, N. Ullah, A. Tolba, F. Xia, "Social acquaintance based routing in vehicular social networks", *Future Generation Computer Systems*, vol. 93, pp. 751-760, 2019.

[2] H. T. Pan, S. F. Chiou, C. Y. Yang, M. S. Hwang, "An improved key agreement authentication scheme based on an anonymous password", *International Journal of Electrical and Electronic Engineering & Telecommunications*, vol. 9, no. 3, 2020.

[3] M. S. Hwang, H. W. Yang, C. Y. Yang, "Cryptanalysis of security analysis and enhancements of a remote user authentication scheme", *IOP Conference Series: Materials Science and Engineering*, vol. 719, no. 1, 2020.

[4] S. K. Sood, A. K. Sarje, K. Singh, "Inverse cookie-based virtual password authentication protocol", *International Journal of Network Security*, vol. 13, pp. 172-181, 2016.

[5] T. Pecorella, L. Brilli, L. Mucchi, "The role of physical layer security in IoT: A novel perspective", *Information*, vol. 7, no. 49, 2016.

[6] L. Atzori, A. Iera, G. Morabito, "The internet of things: A survey", *Computer networks*, vol. 54, pp. 2787-2805, 2010.

[7] C. E. Shannon, "Communication theory of secrecy systems", *The Bell System Technical Journal*, vol. 29, pp. 656–715, 1949.

[8] J. S. Chen, C. Y. Yang, J. F. Yao, M. S. Hwang, "Secrecy rate analysis in the cooperative communication system", in *Proceedings of IEEE ICCE-TW'21*, 2021.

[9] M. Bloch, J. Barros, *Physical-Layer Security From Information Theory to Security Engineering*, Cambridge, 2011.

[10] L. H. Ozarow, A. D. Wyner, "Wire-tap channel II", *The Bell System Technical Journal*, vol. 63, no. 10, pp. 2135-2157, 1984.

[11] Y. Zou, "Physical-layer security for spectrum sharing systems", *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 1319-1329, 2017.

[12] M. Stamp, *Information Security Principle and Practice*, 2nd ed., Wiley, 2011.

[13] M. Khoo, T. A. Wood, C. Manzie, I. Shames, "Exploiting structure in the bottleneck assignment problem", *arXiv preprint*, arXiv:2008.10804, 2020.

[14] N. Tish by, F. C. Pereira, W. Bialek, "The information bottleneck method", *arXiv preprint*, physics 0004057, 2000.
[15] A. M. Saxe, Y. Bansal, J. Dapello, M. Advani, A. Kolchinsky, B. D. Tracey, D. D. Cox, "On the information bottleneck theory of deep learning", *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2019, no. 12, 2019.
[16] G. Li, Z. Zhang, J. Zhang, A. Hu, "Encrypting wireless communications on the fly using one-time pad and key generation", *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 357-369, 2020.
[17] D. Stolpmann, C. Petersen, V. Eichhorn, A. Timm-Giel, "Extending on-the-fly network coding by interleaving for avionic satellite links", in *Proceedings of 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, 2018.

Biography

Cheng-Ying Yang (Member, IEEE) received the M.S. degree in Electronic Engineering from Monmouth University, New Jersey, in 1991, and Ph.D. degree from the University of Toledo, Ohio, in 1999. He is a member of the IEEE Satellite & Space Communication Society. Currently, he is a Professor with the Department of Computer Science, University of Taipei, Taiwan. His research interests include performance analysis of digital communication systems, signal processing, error control coding, Petri net applications and computer security.

Jong-Shin Chen was born in 1972. He received the B.S. and Ph.D. degrees in computer science from Feng Chia University, Taiwan, in 1996 and 2003, respectively. Currently, he is an associate professor in the Department of Information and Communication Engineering, ChaoYang University of Technology, Taiwan. His research interests include big-data mining, capacity planning, wireless networking and information security.

Jenq-Foung JF Yao serves as a professor and the coordinator of computer science and data science at Georgia College & State University. Committed to shaping the future of computer science professionals, he has dedicated his career to higher education. With a prolific academic background, Dr. Yao has contributed to the field through the publication of over 30 research papers spanning from 1998 to 2023. His current focus lies in the realms of machine learning and data mining, with a specific emphasis on their applications in cybersecurity. In addition to his academic achievements, Dr. Yao has actively contributed to the accreditation processes of computer science programs. He served as an ABET CAC accreditation program evaluator from February 2004 to August 2018 and assumed the role of an ABET CAC accreditation team chair from April 2012 to July 2017.

Min-Shiang Hwang received M.S. in industrial engineering from National Tsing Hua University, Taiwan in 1988, and a Ph.D. degree in computer and information science from National Chiao Tung University, Taiwan, in 1995. He was a professor and Chairman of the Department of Management Information Systems, NCHU, during 2003-2009. He was also a visiting professor at the University of California (UC), Riverside, and UC. Davis (USA) during 2009-2010. He was a distinguished professor of the Department of Management Information Systems, NCHU, during 2007-2011. He obtained the 1997, 1998, 1999, 2000, and 2001 Excellent Research Award of National Science Council (Taiwan). Dr. Hwang was a dean of the College of Computer Science, Asia University (AU), Taichung, Taiwan. He is currently a chair professor with the Department of Computer Science and Information Engineering, AU. His current research interests include cryptography, Steganography, and mobile computing. Dr. Hwang has published over 300+ articles on the above research fields in international journals.

Research on Blockchain Technology for Security Protection of Network Information Data in the Legal System Background

Dongdong Li

(Corresponding author: Dongdong Li)

Cangzhou Normal University
Cangzhou, Hebei 061001, China
Email: liddongl@outlook.com

(Received Dec. 5, 2022; Revised and Accepted Nov. 15, 2023; First Online Feb. 20, 2024)

Abstract

This paper briefly introduces network information data security protection from a legal perspective. Blockchain technology was integrated with a software-defined network (SDN) as a method to enhance the security of network information transmission. Subsequently, the paper conducts simulation experiments in a laboratory setting to evaluate the detection performance of SDNs that combined blockchain with local blockchain validation and practical byzantine fault tolerance (PBFT) voting validation strategies. The two SDNs were compared with a traditional SDN in terms of information transmission protection performance. The results showed that the SDN combining blockchain with the PBFT voting validation strategy performed better in detection and was more effective in protecting data transmission compared to the traditional SDN.

Keywords: Blockchain; Legal Background; Network Data Protection; Software-Defined Network

1 Introduction

As the Internet develops so quickly, people are enjoying more convenience in their lives. However, this surge in Internet usage has led to a huge increase in information data [8], much of which is spam. Nevertheless, modern big data technology enables the extraction of valuable information from this influx, which may include users' private data [9]. In addition to spam, users often store critical information on the Internet. Unfortunately, the openness of Internet platforms can make this important information vulnerable to malicious actors [11]. Consequently, the rapid development of the Internet not only brings convenience but also poses security risks to information data. The threats of network attacks, data leakage, and the theft of personal information by malicious entities taking advantage of the Internet's openness seriously jeopardize network security and user privacy. Despite legal protection for network information data, including user privacy, the realm of Internet big data faces challenges such as traceability, accountability, and lenient punishment [2].

Blockchain technology, as a decentralized distributed ledger technology, has gained widespread attention and application as a solution to these challenges. With its characteristics of decentralization, non-tampering, traceability, and anonymity, blockchain, when combined with encryption technology, can effectively enhance the security of network data. Its traceability enables swift legal recourse against parties responsible for network security issues, and the non-tampering and transparency features allow network data to serve as judicial evidence [10]. Yazdinejad *et al.* [13] proposed a novel architecture, blockchain-enabled packet parser (BPP). They found that BPP could effectively detect attacks and strategies on the software-defined network (SDN) control plane, thereby efficiently detecting attacks from the packet structure. Yi [14] introduced the use of blockchain to protect logistics security and personal privacy, constructed a logistics blockchain model, and verified its efficiency and security in a distributed platform. Mao *et al.* [6] developed a blockchain evaluation system to enhance food supply chain management. This paper briefly overviews the security protection of network information data from a legal perspective. Blockchain was integrated with SDN as a means to secure network information transmission, followed by laboratory simulation experiments.

2 Network Information Security Protection from a Legal Perspective

The proliferation of the Internet has given rise to significant challenges in the realm of information security. While the openness of the Internet allows users to freely

engage with information, this very openness creates vulnerabilities that can be exploited by malicious actors, posing a threat to network information security. To address the information security challenges posed by the expanding Internet landscape, China has implemented pertinent laws, including the Cyber Security Law of the People's Republic of China, the Cryptography Law of the People's Republic of China, the Data Security Law of the People's Republic of China, and the Personal Information Protection Law of the People's Republic of China. Additionally, there are administrative regulations specifically addressing network information security, such as the Regulations of the People's Republic of China for Safety Protection of Computer Information Systems.

The existence of the aforementioned laws and administrative regulations provides legal support for the protection of network information security, ensuring that those responsible for compromising network security are subject to legal repercussions [7]. However, current laws and regulations have certain deficiencies and shortcomings. They lack a comprehensive and systematic structure, resulting in decentralization and generality in their provisions. The content often takes the form of broad principles to encompass a wide range of scenarios, leading to challenges in determining responsibility and providing proof. Additionally, the nature of information security risks in the realm of the Internet, characterized by suddenness, secrecy, and intelligence, poses challenges. Suddenness refers to the swift outbreak of network information risks with little prior indication. Secrecy involves the covert nature of unlawful activities on the virtual network. Intelligence denotes the advancement of tools used for compromising network security, often with automatic features. These characteristics imply that, despite existing laws and regulations, they may not completely prevent network risks. For instance, the suddenness of network risks can result in damage and loss before their realization, making laws and regulations primarily a basis for recourse. The secrecy of network risks can complicate forensic efforts and recourse, and the intelligence aspect further heightens the threat and covert nature of risks. Therefore, in addition to relying on legislation as a recourse foundation, effective prevention and mitigation of network risks necessitate the use of technical means to minimize potential losses [12].

3 Security Protection of Network Information Data Transmission Based on Blockchain

3.1 Integration of Blockchain with SDN Architecture

The preceding article discussed the protection of network information security from a legal standpoint, emphasizing the importance of establishing relevant laws and regulations to provide a legal foundation for safeguarding network information security. This legal framework has spurred increased attention from network operators and Internet enterprises toward protecting network information security. Simultaneously, the article highlighted the shortcomings of current laws and regulations in addressing network risks, prompting Internet users to recognize the need for enhanced network information security protection. This growing awareness is expected to further encourage network operators and Internet enterprises to prioritize measures for safeguarding network information security [1].

To enhance the protection of network information on the Internet, a strategic approach involves focusing on both information storage and information transmission. Information storage entails constructing a secure database where crucial network information is stored, isolated from the broader Internet environment. Information transmission is ensured through certain means to guarantee the security of network data during the process of transmission. This paper adopts a perspective that emphasizes information transmission to implement security measures for safeguarding network information data.

As illustrated in Figure 1, the SDN controller, situated in the control plane of the SDN, plays a pivotal role in formulating routing policies and dispatching them to the data plane. In the data plane, the SDN switch functions akin to a router, directing data based on the routing policies it receives.

The SDN segregates the control and forwarding functions by centralizing the control function in the control plane and centralizing the switch responsible for forwarding data in the data plane. Alterations to corresponding management rules are facilitated by debugging the SDN controller, without the need to reconfigure all devices in the network. However, this structural convenience also introduces specific network risks. The SDN controller governs switch forwarding through the flow table, and switches follow the rules outlined in the flow table during operation without validating them. Consequently, a potential attacker can intercept the flow table during transmission from the controller and substitute it with erroneous rules. The flow table rules control the forwarding of data by switches, and their security is crucial for ensuring the overall network's information transmission safety [5].

3.2 Protection of Flow Table Rules in SDN Based on Blockchain

Upon integration with blockchain technology, as depicted in Figure 1, the overall structure remains unchanged, with the only difference being that the SDN controller not only issues flow table instructions to the switch [4] but also acts as a node in the blockchain network. The principle of this structure for securing network information transmission is that, while issuing flow table rules, the controller creates a copy and uploads it to the blockchain. Subsequently, during subsequent operations, the controller randomly selects

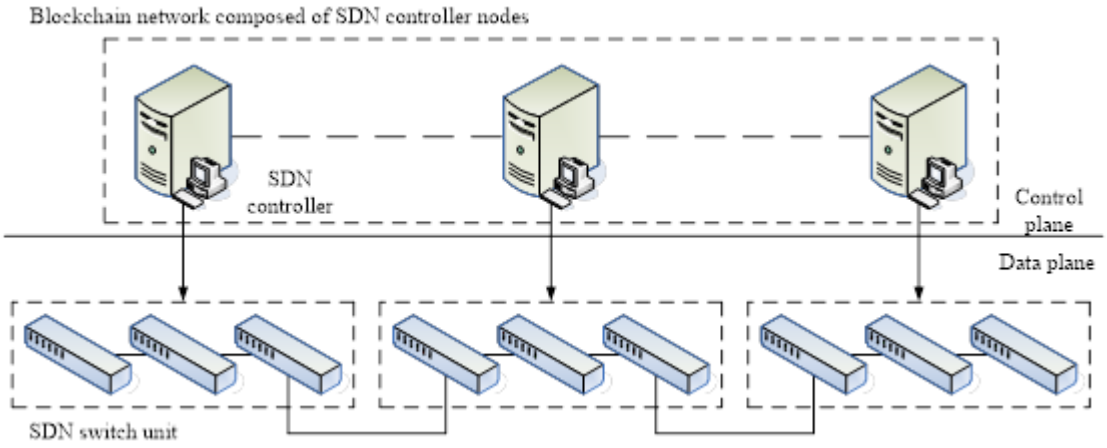


Figure 1: SDN network architecture incorporating blockchain

a flow table rule from the switch and compares it with the version stored in the blockchain to confirm the integrity of the rules within the switch.

The flow of utilizing blockchain to guard the flow table rules in SDN is shown in Figure 2.

1) The SDN controller simultaneously transmits the flow table rules to the switch while generating a copy of these rules and packaging them into the block format needed by the blockchain. The block header [3] holds crucial information, including the version number, random number, timestamp, previous block hash, current block hash, and Merkle root [15]. The block body encompasses data pertinent to the transactions associated with the block, i.e., the duplicated flow table rules in this paper. These rules are digitally signed to ensure their veracity and immutability and aggregated to the Merkle root using a hash.

2) The packaged blocks are broadcast across the blockchain network, and a consensus is performed by the consensus algorithm. In the event of consensus failure, the SDN controller is halted from issuing the flow table rule. Conversely, with a successful consensus, each node deposits the block into its local blockchain. Following the storage of the accurate flow table rules, the subsequent step involves scrutinizing the flow table rules within the SDN.

3) During the protection detection of flow table rules in a switch, the SDN controller initially chooses a switch randomly.

4) A flow table rule is randomly selected from the switch's collection and converted into block format.

5) The SDN controller accesses the blockchain and verifies whether there is a block in the blockchain that matches the selected flow table rule. If a match is found, no action is taken; if not, the SDN controller deletes that flow table rule from the switch.

The critical steps in the blockchain-based flow table rule protection method include uploading the issued flow table and comparing the randomly selected flow table from the switch with the blockchain. In the latter operation, in theory, due to the consistency of the blockchain, the local blockchain of each node where the SDN controller is located should be the same. Therefore, the controller only needs to compare the randomly selected flow table rule with the local blockchain to make a judgment. However, in practice, the consistency between the nodes of the blockchain can be unstable, influenced by factors such as node downtime, node intrusion, and the creation of branch chains due to node uplinking. This inconsistency may lead to misdiagnosis by relying solely on the local blockchain. Therefore, this paper adopts a voting mechanism within the practical byzantine fault tolerance (PBFT) consensus algorithm to validate the flow table rules in the switch. The inspection steps are as follows.

1) A controller node is randomly selected as the master node, and the controller node that needs to validate the switch flow table rules acts as the requesting node to initiate a voting request to the master node.

2) The master node receives the request and sends preparation information to other controller nodes participating in the verification. The verification nodes start entering the voting phase after passing the preparation information and completing confirmation.

3) Each validation node, during the voting phase, uses its respective local blockchain to validate the flow table rules for pending detection. If the same flow table rule exists in the local blockchain, the validation node casts a correct vote to the requesting node; otherwise, it casts an incorrect vote to the requesting node.

4) When the requesting node receives more than half of the number of incorrect votes, it determines that

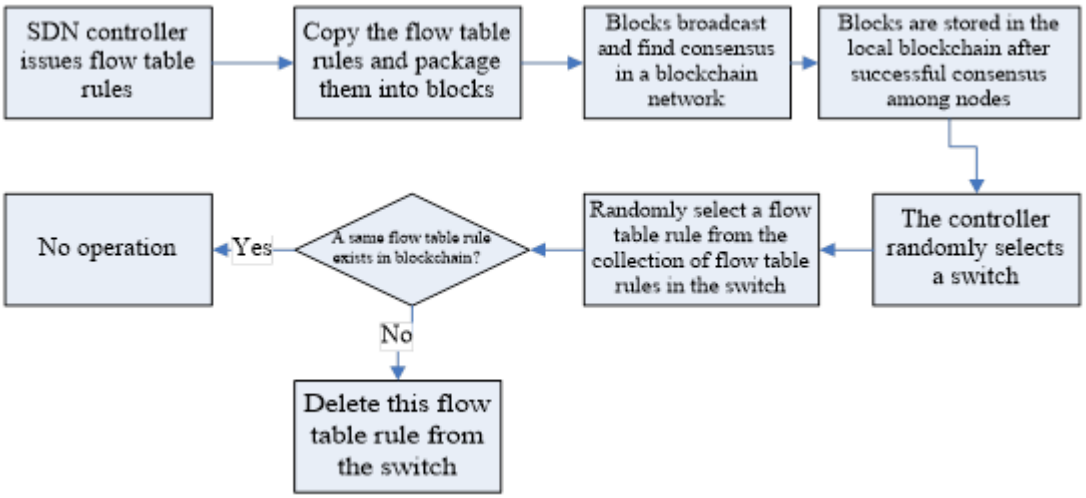


Figure 2: Blockchain-based protection flow of SDN against flow table rules

the flow table rule is erroneous. This triggers the controller of the requesting node to issue a command to delete the flow table rule in the switch. Conversely, if it does not receive a majority of incorrect votes, it takes no action.

4 Simulation Experiments

4.1 Experimental Environment

The experiments were conducted on a laboratory server with a Windows 7 operating system, 16 GB memory, and a Core i7 processor.

4.2 Experimental Setup

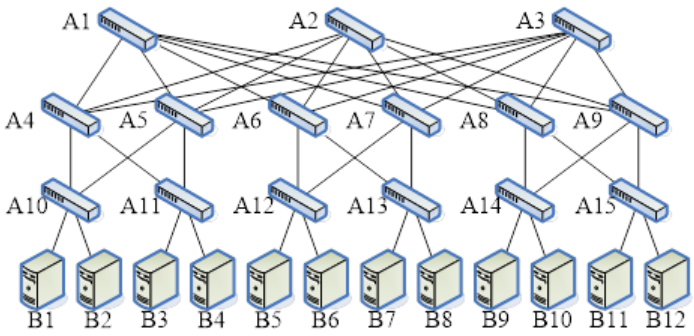


Figure 3: Topology of the devices in the laboratory in the simulation experiment

The network device topology for the simulation experiments in the laboratory is depicted in Figure 3. The setup consisted of a total of 15 switches (A1-A15) and 12 user hosts (B1-B12). The controllers needed to establish the SDN were created through the blockchain platform. In this paper, Ethereum virtual machines were employed as controllers in the SDN, totaling 5 (C1-C5), with each controller overseeing three non-repeatedly numbered switches.

1) Detection performance of error flow table rules in blockchain-based SDN with different verification strategies:

   a. It was assumed that all five controller vnodes operated stably in the blockchain platform and the uplinked flow table rules were consistent. Prior to the commencement of the test, 200 incorrect flow table rules were directly injected into switch A15. Once the test began, the SDN utilized the controllers to inspect flow table rules using two strategies: local blockchain verification and PBFT voting verification. The number of detected incorrect flow table rules was recorded as the detection frequency increased.

   b. The downtime probability was set to 0.01 for the controller node to simulate the condition of blockchain consistency instability during the SDN operation. Prior to the test, 200 incorrect flow table rules were directly injected into switch A15. Once the test began, 12 user hosts randomly sent files to each other to generate correct flow table rules. Simultaneously, the SDN used the controller to inspect flow table rules employing two strategies: local blockchain validation and PBFT voting validation. The false positive rate of flow table rules was recorded as the number of correct flow table rules increased to 100, 200, 300, 400, and 500.

2) Testing the performance of SDN for protection of information transmission with and without blockchain: The SDN without blockchain was compared with the

SDN incorporating blockchain. The structural difference between the SDNs with and without blockchain and the SDN was only that five servers were used as five SDN controllers. User host B1 was required to send a file of 10 GB size to user host B10 for a total duration of 10 s. After 5 seconds of transfer, an error flow table rule was injected into the switch to cause the file to be transferred to user host B12. The file size sent by user host B1 and the file size received by user hosts B10 and B12 in the SDN without blockchain, the local blockchain-validated SDN, and the PBFT voting-validated SDN combined with blockchain were recorded.

4.3 Experimental Results

As shown in Figure 4, the number of erroneous flow table rules detected by the SDN incorporating blockchain increased with the number of detections under the local blockchain validation strategy and the PBFT voting validation strategy, and the growth under both validation strategies was first fast and then slow. Overall the SDN with the PBFT voting validation strategy detected more erroneous flow table rules.

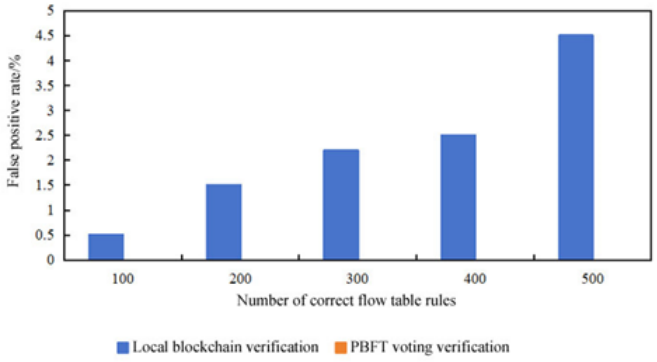


Figure 4: The false positive rate of erroneous flow table rules by SDNs adopting two verification strategies under different numbers of correct flow table rules

As shown in Figure 5, the SDN's false positive rate of incorrect flow table rules under the local blockchain validation strategy increased with the number of correct flow table rules in the switches, whereas the SDN's false positive rate of incorrect flow table rules under the PBFT voting validation strategy stayed the same and was always maintained at 0%.

The three SDNs were tasked with sending a file totaling 10 GB from host B1 to host B10 within 10 s. The introduction of incorrect flow table information into the switch after 5 seconds of transmission resulted in the file being directed to host B12. The transmission and reception outcomes following B1's file transmission are detailed in Table 1. Table 1 reveals that the introduction of the erroneous flow table rule did not impede the transmission from host B1. In all three SDNs, host B1 successfully sent

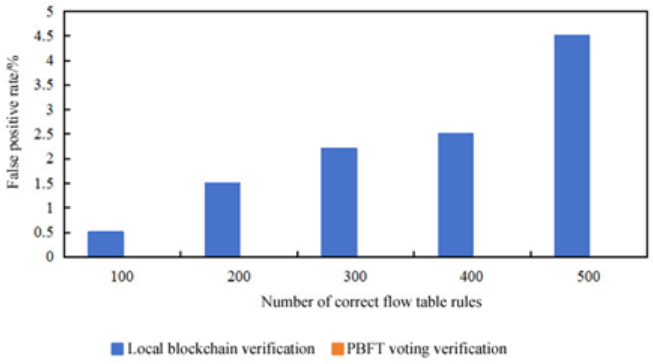


Figure 5: False positive rate of SDNs adopting two verification strategies under different numbers of correct flow table rules

a 10 GB-sized file. However, in terms of file reception, the SDN without blockchain saw host B10 receiving a 5.1 GB-sized file, while host B12 received a 4.9 GB-sized file. In the SDN validated by the local blockchain, host B10 received a 9.3 GB-sized file, and host B12 received a 0.7 GB-sized file. The PBFT voting-validated SDN witnessed host B10 receiving the full 10 GB-sized file, while host B12 received a 0 GB file. These results demonstrated that the traditional SDN, without blockchain support, struggled to transmit and receive files correctly in the presence of erroneous flow table rules. Conversely, the SDN validated by the local blockchain accurately transmitted most of the file, with only a small proportion being transmitted incorrectly. The PBFT voting-validated SDN demonstrated accurate file transmission and reception.

5 Discussion

The advent of the Internet has significantly enhanced people's lives, providing convenience and access to vast amounts of user information, often containing sensitive privacy data. However, this openness also poses risks to network information security. To address these challenges, China has enacted laws and regulations, as mentioned earlier. While these legal frameworks provide a foundation for Internet management, there are shortcomings, including insufficient systemization, decentralization, and the generality of provisions. This results in challenges such as unclear responsibility attribution and proof difficulties in legal pursuits. The sudden, secretive, and intelligent nature of Internet risks further complicates management and prevention. To address these inadequacies in laws and regulations on network information security, several suggestions are proposed.

1) The refinement of legislation in the network field should be accelerated to enhance the vertical system of the legal framework for networks.

2) Rules for handling data, especially personal informa-

Table 1: File transmission and reception results for three SDNs under the interference of erroneous flow table rules

	Blockchain-free SDN	Local blockchain-validated SDN	PBFT voting-validated SDN
Size of the file sent by B1	10 GB	10 GB	10 GB
Size of the file received by B10	5.1 GB	9.3 GB	10 GB
Size of the file received by B12	4.9 GB	0.7 GB	0 GB

tion, on the Internet, should be clarified, and institutional rules should be standardized for data management by Internet platforms.

3) Internet-related departments should stay updated and enact timely and specialized regulations for managing network information in their respective domains.

4) The coordination and harmonization of relevant laws and regulations in the cyber domain should be strengthened to reduce ambiguity in responsibility attribution.

Beyond legal perspectives, network information and data security can also be approached from a technological standpoint. This paper introduced blockchain technology into the SDN structure to secure network information transmission. The decentralized and tamper-proof characteristics of blockchain were leveraged to store flow table rules in SDN switches, serving as a basis for detecting tampering. Simulation experiments in a laboratory assessed the performance of SDNs with different verification strategies and compared the security protection of network information transmission in the traditional SDN and the SDNs enhanced with blockchain under various verification strategies. The results are presented above.

When the number of incorrect flow table rules was fixed, as the number of detections increased, SDN with blockchain detected more incorrect flow table rules. However, there was a trade-off, as the detection process became slower. It is because as more incorrect rules were identified, the remaining ones became fewer, making them harder to spot-check in random selections by the SDN controller. Concerning the false positive rate, the SDN with local blockchain validation experienced an increase as the number of correct flow table rules in the switch rose. In contrast, the SDN utilizing PBFT voting validation maintained a consistent false positive rate of 0%. The reason behind this discrepancy lies in the instability of blockchain consistency. With the increase in flow table rules, some nodes might not record the changes. Local blockchain validation might incorrectly judge correct rules as incorrect due to this inconsistency. However, PBFT voting verification required a majority consensus, and more than half of the nodes could not have problems simultaneously. Results from network information transfer experiments indicated that SDNs incorporating blockchain securely transferred data to the correct addresses, with PBFT voting validation demonstrating superior performance. The traditional SDN lacked the inherent ability to judge the correctness of flow tables, allowing tampered flow tables to redirect data to manipulated addresses. The integration of blockchain enabled the assessment of flow table correctness, and the PBFT voting validation strategy minimized false positive rates effectively.

6 Conclusion

This paper provides a brief overview of securing network information data from a legal perspective. Blockchain technology was integrated with SDNs as a means to enhance the security of network information transmission. The detection performance of blockchain-combined SDNs adopting local blockchain verification and PBFT voting verification strategies was tested using simulation experiments in a lab. Moreover, they were compared with a traditional SDN. It was found that the number of detected incorrect flow table rules increased with the increase in the number of detections, showing an initial rapid growth followed by a slower rate. With the growth in the number of correct flow table rules, the false positive rate rose for the SDN with local blockchain authentication, while remaining consistently at 0 for the one with PBFT voting authentication. SDNs with blockchain demonstrated a more secure data transmission to the correct address, particularly when employing PBFT voting authentication.

References

[1] Z. Hua, Y. Zhou, C. M. Pun, C. L. P. Chen, "2D sine logistic modulation map for image encryption," *Information Sciences*, vol. 297, no. C, pp. 80-94, 2015.

[2] Y. Huo, C. Meng, R. Li, T. Jing, "An overview of privacy preserving schemes for industrial internet of things," *China Communications*, vol. 17, no. 10, pp. 1-18, 2020.

[3] S. S. Kamble, A. Gunasekaran, M. Goswami, J. Manda, "A systematic perspective on the applications of big data analytics in healthcare management," *International Journal of Healthcare Management*, vol. 12, no. 3, pp. 226-240, 2019.

[4] L. Koh, A. Dolgui, J. Sarkis, "Blockchain in transport and logistics – paradigms and transitions," *In-*

ternational Journal of Production Research, vol. 58, no. 7, pp. 2054-2062, 2020.

[5] Y. Liu, S. Tang, R. Liu, L. Zhang, Z. Ma, "Secure and robust digital image watermarking scheme using logistic and RSA encryption," *Expert Systems with Applications*, vol. 97, pp. 95-105, 2018.

[6] D. Mao, F. Wang, Z. Hao, H. Li, "Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain," *International Journal of Environmental Research & Public Health*, vol. 15, no. 8, pp. 1-21, 2018.

[7] N. Martindale, S. L. Stewart, N. A. McGirl, M. B. Adams, G. Westphal, J. R. Garner, "Enabling computation on sensitive data in international safeguards with privacy-preserving encryption techniques," *Journal of Nuclear Materials Management*, vol. 49, no. 2, pp. 16-25, 2021.

[8] H. N. Nguyen, H. A. Tran, S. Fowler, S. Souihi, "A survey of blockchain technologies applied to software-defined networking: Research challenges and solutions," *IET Wireless Sensor Systems*, vol. 11, no. 6, pp. 233-247, 2021.

[9] D. B. Rawat, "Fusion of software defined networking, edge computing, and blockchain technology for wireless network virtualization," *IEEE Communications Magazine*, vol. 57, no. 10, pp. 50-55, 2019.

[10] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *13th International Conference on Service Systems and Service Management (ICSSSM'16)*, pp. 1-6, 2016.

[11] M. A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, "A survey on the adoption of blockchain in IoT: Challenges and solutions," *Blockchain Research*, vol. 2, no. 2, pp. 49, 2021.

[12] X. A. Wang, F. Xhafa, W. Cai, J. Ma, F. Wei, "Efficient privacy preserving predicate encryption with fine-grained searchable capability for Cloud storage," *Computers & Electrical Engineering*, vol. 56, pp. 871-883, 2016.

[13] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, K. K. R. Choo, "P4-to-Blockchain: A secure blockchain-enabled packet parser for software defined networking," *Computers & Security*, vol. 88, pp. 1-15, 2019.

[14] H. Yi, "A secure logistics model based on blockchain," *Enterprise Information Systems*, vol. 15, no. 7, pp. 1002-1018, 2021.

[15] Y. Ziegler, V. Uli, "Supply chain management and blockchain: bridging the antecedents of the technology with the status quo of use case applications," *International Journal of Value Chain Management*, vol. 12, no. 3, pp. 267-284, 2021.

Biography

Dongdong Li is a lecturer of Cangzhou Normal University and graduated from China University of Political Science and Law. Her research interests include civil law, commercial law and economic law. She has published more than 10 papers.

Design and Research of Off-line Transaction Protocols in Remote Areas Under Smart Contracts

Jian Zhou, Shi-Hua Huang, and Shi Yan

(Corresponding author: Shi-hua Huang)

School of Management Science and Engineering, Anhui University of Finance and Economics
No.962, Caoshan Road, Longzihu District, Bengbu 233030, China
Email: 2532400875@qq.com

(Received Apr. 9, 2023; Revised and Accepted Nov. 22, 2023; First Online Feb. 23, 2024)

Abstract

To tackle the issues of expensive fees and inadequate security in online trading for remote regions. In this paper, we propose a method for automated trading using blockchain smart contracts called Non-Online Commodity Trading Agreements (NTA). By designing constraints and NTA metrics using smart contracts, integrating digital trading with offline functions, establishing a cost relationship between the three based on gas consumption, function call method, and variable storage, and finally comparing them with several existing schemes. The proposed scheme fulfills the requirements for automated transactions in offline mode, providing functionality, anonymity, traceability, and verifiability for commodity transactions while ensuring security. Additionally, it establishes an effective method for cost control. The tests conducted on the Remix IDE platform indicate that the proposed scheme effectively supports offline transactions. Additionally, the regression method based on NTA metrics optimizes transaction costs.

Keywords: Blockchain; Commodity Trading; Gas Consumption; Smart Contracts

1 Introduction

As of June 2022, China's overall internet penetration rate had reached 74.4%. However, the rural areas of China have only achieved an internet penetration rate of 58.8%, indicating that almost half of these regions are still without internet access [1]. This has posed a significant obstacle to promoting high-quality economic development in China and implementing the strategy for rural revitalization. Buyers and sellers cannot realize information exchange instantly, which becomes the main challenge of non-online commodity trading. The main solutions currently include (1) ensuring comparable quality of service (QoS) between rural and urban communication sites include increasing hardware infrastructure, such as the BS deployment and resource management methods proposed by [2] for remote and rural areas, which obviously has huge investment cost and offer little benefit. (2) To establish mobile storage forwarding strategies, such as [3, 4] establishing delay-tolerant networks or self-organizing networks by drones or cars carrying mobile storage devices to transmit transaction information to areas with networks, this approach would require new network protocols and the forwarding devices are easily intercepted and the information is easily tampered with. (3) Satellite communication approach, [5] researched the use of massive MIMO technology installed on existing infrastructure of TV towers to cover large rural areas with a radius of tens of kilometers to provide sparse area connectivity, but suffers from the disadvantage of neglecting cost control. All of the aforementioned strategies can be observed to suffer from the requirement to build hardware facilities, high costs, and poor security.

Smart contract technology in blockchain is expected to solve this problem. The automatic execution of smart contracts when pre-defined conditions are met perfectly addresses the pain points of offline transactions. First proposed by Szabo in the 1990s, smart contracts are defined as "a set of digitally specified promises, including agreements between parties to fulfill them" [6]. Smart contracts enable the establishment of contractual terms that can be executed automatically on the blockchain, without the need for a third-party intermediary. This is achieved by converting the formulated rules into a blockchain program in the form of code programming, which is then compiled and deployed on blockchain nodes [7]. Smart contracts can significantly enhance the quality of transactions and trading environments. For instance, the community-based smart virtual power plant (CVPP) smart contract trading platform enables users to trade energy based on a contract without the need for a third-party organization. This platform addresses the trust issue between the two

parties and reducing the energy cost per household [8]. [9] researched blockchain-based financial transaction verification and secure service management with smart contracts, which gave cost control but was not suitable for remote rural transaction characteristics. [10] proposes a delayed and fault-tolerant network through UAV-assisted blockchain offline transactions to transmit transaction information from remote areas to locations with networks, but does not incorporate smart contracts for cost control. Despite the current research trend, few studies that have applied smart contracts to remote areas. However, smart contract technology is gradually gaining attention for its potential to improve transactions in harsh environments, particularly offline transactions. The use of smart contracts, traceability, and anonymity in blockchain can address the efficiency and security issues that arise in transactions in remote areas.

Current research on blockchain-based offline transactions has primarily focused on delay-tolerant applications and the proposed system architecture [11–13], while largely overlooking the potential application of smart contracts in the transaction process. [14] proposed a service transaction ecosystem called STEB that utilizes a dual-chain architecture and a new set of smart contracts. The ecosystem contains two types of blockchains: TraChain and SerChain. The dual-chain architecture, implemented through three smart contracts, provides varying levels of access to the data to ensure the integrity and security of transactional data. In contrast, the protocol proposed in this paper consolidates the services necessary for the transaction process into a single contract, with the primary emphasis on offline performance. Research on the implementation of smart contracts in various industries has concentrated on enhancing the convenience and security of the transaction process by utilizing their decentralization, automatic enforcement of contract terms, and assurance of data security and traceability. However, ignoring the nonlinearity involved in developing blockchain smart contracts . In this paper, we propose an offline commodity trading protocol (NTA) based on blockchain smart contracts. The objective is to facilitate economic development in remote areas with poor network connectivity. The NTA solution is programmed in the Solidity language and deployed and tested on the Remix IDE platform. The merchant, who deploys the contract, writes the code that includes publishing and updating information about item numbers, owners, and prices. They also provide function call entry points for payers to register, log in, query, and trade, as well as set conditions for commodity transactions. The commodity trading smart contract was deployed using the Ethereum test account provided by the Remix IDE platform. The test was conducted with the computer network disconnected, and the results demonstrated the successful trading of the contract in remote areas with poor network conditions. Furthermore, the cost and security analysis of the solution indicate that using smart contracts for commodity trading is a reasonable option.

2 Agreement Design

Second-generation blockchain platforms, such as Ethereum, enable the automatic execution of contract terms by writing code in the form of smart contracts. This feature provides peer-to-peer transactions that are free from third-party interference for both parties involved in the transaction. In this paper, we propose a non-online transaction agreement (NTA) based on smart contracts. The NTA is designed to facilitate remote transactions that connect merchants, payers, and commodity information through a decentralized Ethernet network.

The identity authentication function within the contract content establishes the necessary prerequisites for the transaction. The contract owner must preset the information upload and query function, which allows users to access accurate transaction content even when offline. The transfer function executes once the preset conditions are met, and the contract automatically completes the transfer of the commodity ownership to the ID upon completion of the transaction.

2.1 Role Definition

NTA has three primary roles, which are described below.

Merchant S (referred to as S_R for merchants in remote areas and S_N for those in non-remote areas) is responsible for deploying the contract, setting and publishing the commodity transaction contract, including the price and quantity of the commodity. They are also responsible for providing registration and login services, balance inquiry, commodity price inquiry, and transaction transfer entrance for the payer.

The payer P is denoted as P_R for payers in remote areas and S_N for those in non-remote areas. The entity has the right to utilize the contract and can invoke its functions to fulfill authentication, information retrieval, and payment requirements.

The product G, which is recorded by the merchant as data to be included in the contract, contains information such as its ID, price, and owner.

2.2 Smart Contract NTA Architecture

While some online trading platforms have established secure and trustworthy trading environments, they require stable network support throughout the trading process. This means that remote areas with poor network conditions may not be able to successfully complete online trading. NTA integrates digital transactions and offline functions by pre-setting constraints through smart contracts; the automation of smart contracts is used to execute the agreements content when both sides of the transaction reach the pre-set conditions, reducing the disputes arising from the transaction; moreover, the transparency of smart contracts makes each transaction traceable, improving the security and robustness of the transaction.

The NTA is depicted in the sequence diagram as a sequence of function calls and events, illustrating the interaction between each role and the contract in Figure 1. The transaction flow is as follows.

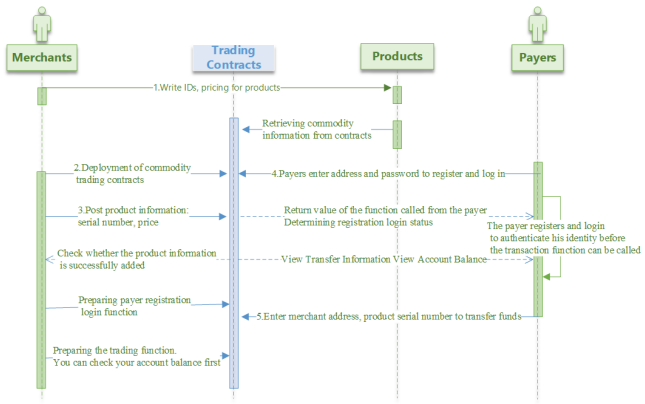


Figure 1: Smart contract commodity trading sequence diagram

1) Contract Deployment:Merchant S develops a commodity transaction agreement and deploys the contract. The contract includes information such as the commodity's quantity, pricing details, and predefined execution conditions for transactions with payers.

2) Edit commodity information: Information regarding the commodity "G" that will be traded is linked to the contract, allowing both parties involved in the transaction to access and review the current status of the commodity.

3) Authentication: Develop a contract for merchants to upload commodity information and another contract for payers to log in and register.

4) Querying transaction conditions: Prior to initiating the transaction, the payer must verify if their account meets the merchant's pre-set transaction conditions. If the account meets the conditions, the payer can proceed to the next step. However, if the account does not meet the conditions, the payer must query the additional conditions required and perfect them accordingly.

5) Transaction completion: Once the merchant and the payer have agreed on the contract details, the payer transfers the money to the merchant based on the product information and becomes the owner of the product. The merchant accepts the transfer and transfers the ownership of the product to the payer, thus completing the transaction.

The real-life example in the sequence diagram is as follows: Alice, a merchant, has developed an NTA protocol using Solidity to facilitate offline trading of goods in remote areas with poor network connectivity. Bob calls the contract function to find out the price of G. If the price is as expected, he prepares the transaction, first authenticating himself as the payer with his own account and setting a login password. Bob logs in as the payer and navigates to the transaction window. He enters his account information, Alice's account information, and the quantity and price of G. Once he confirms that there are no errors, the transfer is processed. After the transfer, ownership of G is transferred from Alice to Bob, and the transaction is completed.

3 Algorithm Design

3.1 NTA Metrics

In this paper, we aim to decrease gas consumption in NTA by focusing on three aspects: variable storage, function calls, and loop and if structures. Our approach is based on analyzing the Ether Yellow Book, opcodes, and GasMet metrics to identify correlations between source code parameters and gas consumption [15–18].

3.1.1 Variable Storage

Storing data on the blockchain can be costly as it requires payment of gas fees for every instance of data retrieval. The cost of gas is controlled by optimizing the SSTORE opcode, primarily through two aspects.

One important consideration is the choice of variable type. In Solidity, regardless of how a uint variable is defined, 256 bits of storage space will be reserved for it. For instance, if only a uint32 or uint64 is required, the EVM will still allocate the full 256 bits and fill the remaining bits with zeros. This can result in unnecessary gas consumption, making the selection of variable type crucial for optimizing gas usage.

The second factor to consider is the order of variables. Solidity contracts utilize consecutive 32-byte slots for variable storage. When we place multiple variables in a single container, it is called variable packing. If the packed variable exceeds the 32-byte limit of the current slot, it will be stored in a new slot. This is because using each slot consumes Gas. Variable packing optimizes gas consumption by reducing the number of slots required for the contract. Hence, it is essential to determine the variables that complement each other to minimize space wastage and reduce gas consumption.

3.1.2 Function Cost

There are two types of function calls in Solidity: internal and external. The internal call is implemented as a straightforward EVM jump, which utilizes the data in the context directly. This means that it calls the function directly by using its name. The external call, which is implemented as a message call to the contract, uses the *ContractName.Function()*. An external call between two completely separate contracts deployed on the network can be initiated by prefixing the function call with

this.function(). When a function is called externally, all of its arguments are copied into memory and then passed to the function. In contrast, an internal function call does not require the formal parameters to be copied into memory again. The protocol described in this article does not require multiple contracts. To minimize gas consumption, internal calls are utilized for functions due to the memory footprint of function calls.

3.1.3 Statement Structure

The opcodes, source code parameters, and gas consumption correlation function indicate that the use of loop code is strongly associated with an increase in gas consumption. If the loop expression uses a storage variable, the SSTORE opcode can lead to excessive gas consumption during each iteration of the loop. In contrast, the "if" structure does not have a direct correlation with gas consumption. Therefore, the NTA scheme avoids the use of looping statements and replaces them with "if" statements.

Regression analysis was conducted using the NTA indicator as the independent variable and gas consumption as the dependent variable. The objective was to identify significant parameters in the indicator that contribute to significant variations in gas consumption. There are multiple factors that affect gas consumption, therefore, control variables are necessary for multiple regression analysis. This paper proposes a linear regression model (Equation (1)) to analyze the impact of these factors on changes in gas consumption:

$$Y = c + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 \quad (1)$$

Here c is the constant term, $\beta_i (i = 1, 2, 3, 4)$ is the coefficient of the independent variable, and $X_i (i = 1, 2, 3, 4)$ is the NTA indicator. X_1 is the variable data type selection, X_2 is the function call method, X_3 is the variable order change, and X_4 is the statement structure selection.

3.2 NTA Algorithm

A smart contract deployed on the blockchain can store information indefinitely and will execute according to its internal terms when invoked, as long as the contract remains active [19]. The deployment of smart contracts is similar to signing a contract offline. In this case, one of the parties proposes the transaction and provides the contract. After negotiation between the two parties, the contract is finally signed to conclude the transaction. In a commodity transaction, the merchant takes on the responsibility of initiating the contract and provides callable functions for the payer to manage the contract. The NTA contract is comprised of four parts: product release, customer registration and login, product transaction, and account balance inquiry. The transaction amount is measured in wei, with 1ETH in ethereum being equal to 10^{18}wei.

Algorithm 1 Product Release

```
Begin
Input: good ID and price.
if Goods are ready then.
    Save good information into the good
     mapping array.
    Enter the good ID.
    Enter price.
    The owner of good ID is the current
     function caller.
    Call the add good function.
    Good added successfully.
end if
if User wants to know price then
     Enter the good ID.
end if
```

Merchants publish their goods using Algorithm 1. The serial number (123456) and price (10^{19}wei) are defined as "uint" variables and stored in the Good structure. Two mapping relationships are also declared: the first maps each product's information to the Goods structure, while the second maps the product ID to the address of the product owner. This allows for easy querying of the current owner's address by the good ID. The *modifier()* function of *onlygoodToOwner()* defines that only the item owner (contract deployer) can modify the item information, thus ensuring that only the merchant can update and delete the item information. The "AddGood" event is created to indicate the addition of a product. The function for adding a product has the same name as the event. It sets the product's ID and price, and identifies the owner of the product as msg.sender, which is the address of the currently called function: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4. After adding the product information, the user can input the product ID to retrieve the price of the product using the *getPrice()* function. If the product ID has not been added, the function will return a price of 0.

Algorithm 2 Payer Register

```
Begin
Input: payee address and password.
if The payee address has registered then.
    Return has registered.
    else
        Store user information in the users
         map array.
        Enter the payer address.
        Enter password.
        Call the register function.
        Registration success.
end if
```

Algorithm 2 and Algorithm 3 explain the processes of payer registration and login. The declaration of the

"payable" keyword in the registration and login functions indicates that these functions can accept Ether from the caller. This ensures that the transfer will be successful when the item is traded. After the merchant deploys the contract to publish the product information, the payer can check whether the product exists and its price by using the product ID. If they decide to purchase the product, they must register and log in to their Ether account address to inform the merchant of their intention to buy the product. If the payer's account is already registered, they can log in directly without having to register again. Otherwise, they will need to register first. When a user registers, the account address "0xAb8483F64d9C6d1EcF9 b849Ae677dD3315835cb2" is defined as an "address" variable, which is a 20-byte Ethereum address. The password "123" is defined as a "uint" variable. The address information for all registered payers is linked to their user accounts. The structure includes the payer's account address, password, registration status (hasRegistered), and login status (hasLoggedIn). The registration process displays the registered address and password. The registration function can be accessed directly by entering the account address and password. The function first checks whether the account address is registered. If it is not registered, the account address and password will be stored in the users mapping array, and hasRegistered will be set to "true". This indicates that the registration was successful. The login event and function are similar to the registration process, but the function involves a more extensive verification process. After entering the account address and password, the login function should verify whether the account is registered. If it is, the function should proceed to verify whether the password is correct. If the password is correct, the login is successful. If the password is incorrect, the user should be prompted to reenter the password.

Algorithm 3 Payer Login

```
1: Begin
2: Input: payee address and password.
3: if The payee address has registered then.
4:     Enter the payee address.
5:     Enter password.
6:     Call the login function.
7:     if Password is right then
8:         Login successful.
9:     else
10:        Wrong password, Login failed.
11: else
12:    Unregistered, Login failed.
13: end if
```

Algorithm 4 explains the process of merchandise transactions. The transaction event's content includes the account addresses of the merchant and payer, product ID, and product price. The transaction function is called by the payer. The function first determines whether the payer's account balance is greater than or equal to the commodity price. After entering the payer's account (0xAb8483F64d9C6d1EcF9b849Ae677dD3315835 cb2), the merchant's account (0x5B38Da6a701c568 545dCfcB03FcB875f56beddC4), the commodity serial number (123456), and the price (10^{19} wei), the function checks the account balance. If the balance is less than the price of the product, the transaction will fail due to insufficient funds. However, if the balance is sufficient to cover the cost, the payer will transfer the amount matched with the product ID to the merchant account of the product owner. The "*fallback()*" and "*receive()*" functions, which are marked as payable, ensure that the account is capable of accepting transfers. This means that Ether can be transferred from the payer's account to the merchant's account. To ensure a successful transaction, the payer must verify that their account balance is sufficient to cover the transfer amount before initiating the transaction. This can be done by calling the *getBalance()* function, as demonstrated in Algorithm 5. Prior to completing the transaction, the payer should review their account balance and the payment amount to confirm that the transfer can be executed accurately. The *getBalance()* function can be used to check the balance of both accounts after the transaction is completed. This helps determine whether the transfer was successful or not, which is an important indicator of completion.

Algorithm 4 Transaction

```
1: Begin
2: Input: payer address, good To Owner
   address, good ID and price.
3: if The payer address has registered then.
4:     if Payer's balance is greater than the price
       then
5:         Enter the payer address.
6:         Enter the good To Owner address.
7:         Enter the good ID.
8:         Enter the price.
9:         Call the transfer function, transfer to
           contract owner.
10:    else
11:        Not sufficient funds and transfer failed.
12: else
13:    Transfer cannot be made.
14: end if
```

Algorithm 5 Balance Inquiry

```
1: Begin
2: Input: address.
3: if Not sure if the balance can be traded then
4:     Enter the address.
5:     Call the get balance function.
6:     Get the balance.
7: end if
```

4 Experimental Results Analysis

4.1 Contract Compilation Results

NTA smart contract was written in the Solidity programming language. The experimental environment was configured on a computer with a 1.60 GHz CPU, 4.0 GB of RAM, and a 64-bit operating system. The smart contract transactions were implemented using Remix IDE version v0.8.13 while disconnected from the computer network. Remix IDE is an open source tool that provides a web-based platform for writing, deploying, and testing Ethereum smart contracts [20].

In the proposed scheme, there are four possible transaction combinations based on the location of the merchants and payers: $\{S_R, P_R\}$ transactions between remote area merchants and payers, $\{S_R, P_N\}$ transactions between a remote area merchant and a non-remote area payer, $\{S_N, P_R\}$ transactions between a non-remote area merchant and a remote area payer, and $\{S_N, P_N\}$ transactions between non-remote area merchants and payers. In the simulation scenario, there are a total of 15 user accounts. Out of these, 5 are merchant accounts and 10 are payer accounts. Each account has 100 ETH pre-stored. The merchants have prepared 5 different types of products, each with unique prices and IDs. To address the challenge of conducting transactions in remote areas with poor network connectivity, this paper proposes a solution that leverages the unique features of blockchain technology and smart contracts. Blockchain wallets can facilitate transactions even when they are completely offline, similar to writing a check and mailing it to the bank. If a single node in the blockchain goes offline, regardless of the duration, it will recover the missing blocks by comparing its local blockchain with that of its peer node. In this paper, we build a local node.js environment to enable the use of the smart contract compilation platform without an internet connection. The contract includes conditions for identity authentication and account confirmation, ensuring that a transaction can only be initiated when both parties meet the predetermined requirements. The blockchain stores information in a block when a transaction is not yet connected to the network. Once connected, the blockchain broadcasts the newly generated block to the entire network. The transaction information is then permanently stored on the main chain of the blockchain, making it non-tamperable and traceable. As depicted in Figure 2, the merchant account with the address "0x5B38Da6a7 01c568545dCfcB03FcB875f56beddC4" has successfully deployed the contract, resulting in a unique transaction hash that can be utilized in the blockchain to distinctly identify the deployment of contract transactions. Meanwhile, the customized function port in the contract will appear on the left side of the Remix IDE, as shown in Figure 3. Merchants and payers can use their Ether accounts to call the function and complete the commodity transaction process.

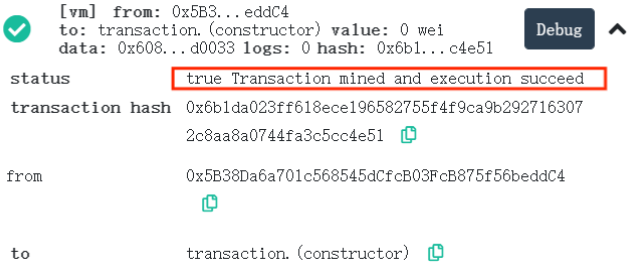


Figure 2: Smart contract deployment result

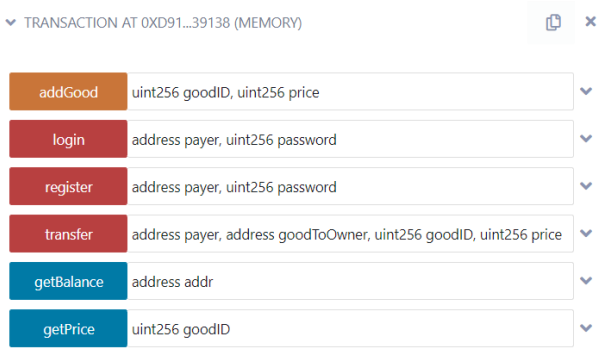


Figure 3: Functions formulated by commodity trading smart contracts

The *getprice()* function can be used to check the entire product transaction in real-time and detect any changes in the account balance. In this experiment, the price of product 123456 is 10^{19} wei. Therefore, the payer who wishes to purchase product 123456 must transfer 10^{19} wei to the merchant's account to initiate the transfer of the product ID. The comparison of the account balance before and after the transaction in Table 1 indicates that the payer successfully transferred the exact amount of the product price to the merchant account. Additionally, the ownership of the good ID was transferred from the merchant to the payer, confirming the completion of the entire transaction.

4.2 Transaction Scenarios

The user registers and logs in as a payer. When the user enters their account address and password, the function will look up their account information. If the account has already been registered, the function will return the string "Has registered". As depicted in Figure 4, the "decoded output" signifies that the account information has been successfully registered and cannot be registered again. Therefore, the login function can be accessed directly. To ensure the authenticity and trustworthiness of a transaction, both parties must establish their identities. The merchant is both the owner of the product and the deployer of the contract, and therefore holds the initiative in the transaction. However, the identity of the payer is unknown, so it is necessary to designate their account address as the payer by calling the login function, in order to

Table 1: Account balances before and after transactions

Account	Merchant	Payer
Address	0x5B38Da6a701c568545d CfcB03FcB875f56beddC4	0xAb8483F64d9C6d1EcF9 b849Ae677dD3315835cb2
Before transaction	100eth	100eth
After transaction	109.99999999999201648eth	89.99999999999842108eth

inform the merchant. When the login function is called, both the account address and password must be provided. There are two types of login errors: "Unregistered" or "Wrong password". The transaction function can only be invoked and the merchant can only make a transaction when the payer's account is successfully registered. If the login fails, the transaction cannot be completed. This is a security measure for both parties.

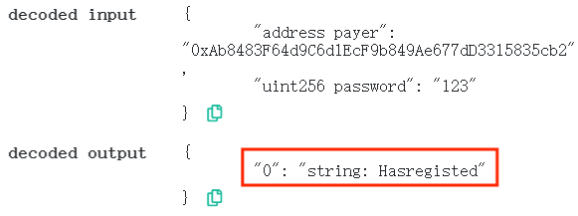


Figure 4: Duplicate account registration

Figure 5: Calling the trading function fails

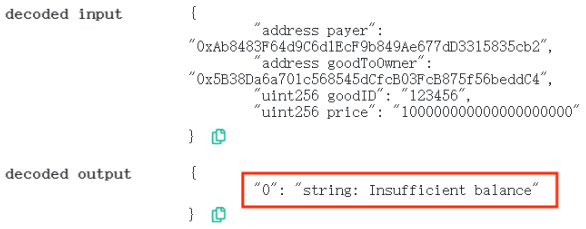


Figure 6: Insufficient account balances

The process of product transactions. Before calling the transaction function to make a payment, the payer must meet one condition: their account address must be logged in. If the account address is not logged in, the call to the transaction function will fail, as shown in Figure 5. In this case, the payer must call the registration and login functions again to mark their account address as the payer. The call to the transaction function is failing for another reason: the account-related function in the contract has not been defined with the "payable" keyword declaration. If the payer's account has been registered and logged in correctly, the function will automatically compare the account balance with the price of the product when the transaction function is called. If the account balance is less than the price of the product, the transfer will be unsuccessful, and the function will return the string "Insufficient balance", as shown in Figure 6.

5 Analysis of Results

In this paper, we propose a smart contract scheme called NTA for offline commodity transactions in remote areas. This scheme enables online commodity transactions to be performed even with intermittent network interruptions. During the simulation, five merchant accounts and ten payer accounts were able to perform transactions normally. The commodity transaction process was completed without any issues in all four conditions: $\{S_R, P_R\}$, $\{S_R, P_N\}$, $\{S_N, P_R\}$, and $\{S_N, P_R\}$. The primary operations involved in the commodity transaction process are depicted in the scheme, which includes commodity posting, payer registration and login, and transfer transactions. It is essential to analyze the cost and security concerns associated with the implementation of the scheme.

Based on the multivariate relationship model between NTA metrics and gas consumption proposed in Section 2.1, a regression analysis was conducted using the "*ls()*"

function of the linear model in EVIEWS. In the linear model function, regression results are calculated based on the target and predictor variables. Control variables were used to extract data based on the contract content, resulting in 50 sets of gas consumption cost data. The residuals and variables were analyzed using stepwise regression. The confounding variables X_3 and X_4 were removed, and the data was smoothed. The Equation (2) is used for regression calculations in EVIEWS:

$$ls\ DY\ c\ AR_{X_1}(2)\ AR_{X_2}(1) \tag{2}$$

Regression result Equation (3) is obtained:

$$\begin{aligned} DY = {} & 55.8128489775+ \\ & 0.00232833792674 * AR_{X_1}(2) \\ & + 0.994973138872 * AR_{X_2}(1) \end{aligned} \tag{3}$$

The dependent variable Y in the regression analysis is the consumption of gas under different variable types. X_1 represents the consumption of gas caused by changes in function invocation method, while X_2 represents the consumption of gas caused by changes in the order of variables. Where DY and $AR_{X_2}(1)$ are the first-order differences of Y and X_2, respectively, and $AR_{X_1}(2)$ is the second-order difference of X_1, the graph of the regression equation is depicted in Figure 7.

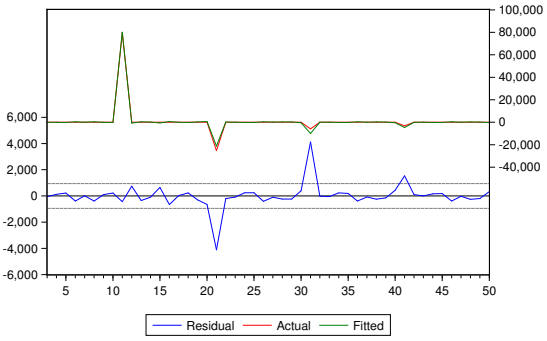


Figure 7: Regression results

The coefficient of determination (R^2) in multiple linear regression is used to measure the proportion of the variance in the dependent variable that can be explained by the independent variable(s). R^2 ranges from 0 to 1, where a value of 0 indicates that the independent variable(s) do not explain any of the variance in the dependent variable, and a value of 1 indicates that the independent variable(s) explain all of the variance in the dependent variable. When the value of R^2 is close to 1, it indicates that the model is a good fit for the data and can accurately predict the desired outcome of the dependent variable. The R^2 value of the NTA indicator regression equation is 0.9942, indicating a strong fit of the equation. The accompanying t-test probabilities of t-tests for $AR_{X_2}(1)$ and $AR_{X_1}(2)$ are 0.0000 and 0.0252, respectively, both less than 0.05, which suggests a high level of significance for the equation. Based on the regression analysis, the NTA indicators proposed in this paper, specifically X_1 (variable data type selection) and X_2 (function invocation method), have a significant and positive impact on Y (gas consumption). The regression coefficients indicate that the mode of function invocation has a significant impact on gas consumption, particularly when multiple function invocations are required during contract trading. Additionally, the selection of variable data types has a weak but still significant impact on gas consumption, which can be attributed to the limited number of variables used in the contract.

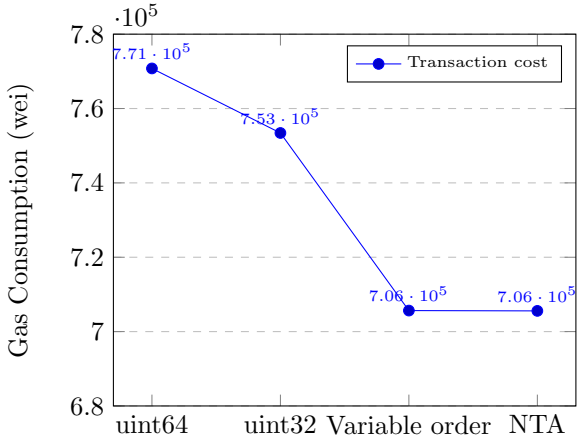


Figure 8: Line chart of variable storage and gas consumption

Each operation in the Ethernet network incurs a specific cost measured in gas and gwei. One gwei is equivalent to 10^{-9} ETH [21]. As shown in Figure 8, the trend of gas consumption following the deployment of the contract for the NTA scheme in order to optimize is displayed. It is evident from the figure that gas consumption decreases significantly after optimization and aligns with the regression equation suggested by the NTA metric.

Table 2 displays the cost of gas required to execute all functions of the proposed smart contract scheme in this paper, along with its corresponding price in Chinese Yuan (RMB). Based on the data presented in Table 2, the NTA appears to be reasonable. The total cost ranges from 56.8 to 41.5 RMB assuming smooth transactions, with the cost of contract deployment removed and the cost of executing each function call ranging from 0 to 5.4 RMB. Since the cost of running the contract is only related to the market unit price of the function and gas used to execute the contract, the cost of using the smart contract-based NTA solution is essentially fixed.

Table 3 presents a comparative analysis of the proposed NTA and other schemes in terms of cost, confidentiality, anonymity, and traceability. Small base stations, as well as large-scale MIMO, require significant investment costs for establishing hardware facilities with minimal benefits. UAV-assisted blockchain incurs not only the cost of flying and maintaining the equipment, but also the cost of incentivizing trust. The Blockchain delay tolerance scheme

Table 2: Gas costs for commodity trading contracts, calculated in RMB

	Function calls	**Transaction Costs**	**Fast Trans. (RMB)**	**Average Trans. (RMB)**	**Slow Trans. (RMB)**
Merchant	Contract Deployment	705570	41.928	33.996	30.596
	Commodity Posting	90754	5.393	4.373	3.935
	Balance Inquiry	0	0	0	0
Payer	Register	91373	5.430	4.403	3.962
	Login	28887	1.717	1.392	1.253
	Trade Transfer	37494	2.228	1.807	1.626
	Product Price Inquiry	0	0	0	0
	Balance Inquiry	0	0	0	0
	Total	954078	56.696	45.971	41.372

Table 3: Comparison of offline trading solutions in remote areas

Method	**Cost**	**Confidentiality**	**Anonymity**	**Traceability**
Small base station (BS) [2]	Θ_{COMP}(t)	Not supported	Not supported	Not supported
UAV-assisted [10]	Base cost + incentive cost	Weak	Not supported	Yes
Large-scale MIMO [5]	6800 USD	Weak	Not supported	Not supported
Blockchain latency tolerance [9]	Gas cost $+C_R$+$C_N X_s$	Strong	High	Yes
NTA	Gas cost	Strong	High	Yes

includes mining costs, gas costs, and the payment system operator's costs ($C_R + C_N X_s$). While the cost of the NTA scheme is primarily determined by gas consumption, a comparison shows that the cost required for NTA is lower than that of the schemes described in the literature [2, 5, 9, 10]. On the other hand, the nature of smart contracts in the proposed NTA scheme results in significantly higher overall security compared to other schemes.

6 Conclusion

This paper discusses the use of blockchain smart contracts to facilitate offline commodity transactions in remote areas, offering a solution to the challenges of traditional online transactions in areas with intermittent network connectivity. The merchant is responsible for deploying the contract and owns the goods. They are also responsible for writing the content of the smart contract in Solidity language. The payer, on the other hand, uses their Ether account to call the contract function and complete the authentication and goods transaction. Finally, the simulation experiments conducted on the Remix IDE platform demonstrate that the proposed scheme can run successfully. Furthermore, upon analyzing the cost and security of the proposed scheme, it can be concluded that the scheme is cost-effective, secure, and reliable when compared to existing schemes.

The process of commodity transactions is complex, and there are several other factors that merchants and payers must consider when engaging in blockchain smart contract-based commodity transactions. For example, issues such as whether the quality of goods matches their price, after-sales problems, and the lack of third-party supervision and punishment in peer-to-peer transactions between merchants and payers can lead to various problems such as poor quality goods, fraudulent transactions, and false transactions. In order to effectively address the complex challenges that arise in commodity trading, it is imperative that we enhance the content of our contracts. This can be achieved by incorporating algorithms for commodity quality control and credit evaluation into our trading agreements. By doing so, we can better regulate the behavior of merchants and payers, ensuring that all parties adhere to the terms of the contract.

Acknowledgement

This study was supported by the National Natural Science Foundation of China (61402001); the Natural Fund of Anhui Province Higher Education Foundation (KJ2020A0013, KJ2019A0657, J2018A0441); the Key Project of Anhui University of Finance and Economics (ACKYB21018, ACKYB19012); the Graduate Research Innovation Fund of Anhui University of Finance and Economics (ACYC2021430).

References

[1] J. Peng, K. Li, and Y. Gao, "How the internet affects china's green consumption development: Empirical research based on baidu index data," *Sustainability*, vol. 15, no. 1, p. 50, 2022.

[2] T. Dlamini and S. Vilakati, "Remote and rural connectivity: Infrastructure and resource sharing principles," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–12, 2021.

[3] S. Perumal, V. Raman, G. N. Samy, B. Shanmugam, K. Kisenasamy, and S. Ponnan, "Comprehensive literature review on delay tolerant network (dtn) framework for improving the efficiency of internet connection in rural regions of malaysia," *International Journal of System Assurance Engineering and Management*, vol. 13, no. Suppl 1, pp. 764–777, 2022.

[4] E. Yaacoub, K. Abualsaud, T. Khattab, and A. Chehab, "Secure transmission of iot mhealth patient monitoring data from remote areas using dtn," *IEEE Network*, vol. 34, no. 5, pp. 226–231, 2020.

[5] T. Taheri, R. Nilsson, and J. Van De Beek, "The potential of massive-mimo on tv towers for cellular coverage extension," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–14, 2021.

[6] S. Ahluwalia, R. V. Mahto, and M. Guerrero, "Blockchain technology and startup financing: A transaction cost economics perspective," *Technological Forecasting and Social Change*, vol. 151, p. 119854, 2020.

[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, 2018.

[8] M. Guo, K. Zhang, S. Wang, J. Xia, X. Wang, L. Lan, and L. Wang, "Peer-to-peer energy trading and smart contracting platform of community-based virtual power plant," *Frontiers in Energy Research*, vol. 10, p. 1007694, 2023.

[9] Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon, and A. Seneviratne, "A delay-tolerant payment scheme based on the ethereum blockchain," *IEEE Access*, vol. 7, pp. 33159–33172, 2019.

[10] R. Xing, Z. Su, T. H. Luan, Q. Xu, Y. Wang, and R. Li, "Uavs-aided delay-tolerant blockchain secure offline transactions in post-disaster vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 11, pp. 12030–12043, 2022.

[11] S. Shahab and Z. Allam, "Reducing transaction costs of tradable permit schemes using blockchain smart contracts," *Growth and Change*, vol. 51, no. 1, pp. 302–308, 2020.

[12] J. Lu, S. Wu, H. Cheng, B. Song, and Z. Xiang, "Smart contract for electricity transactions and charge settlements using blockchain," *Applied stochastic models in business and industry*, vol. 37, no. 3, pp. 442–453, 2021.

[13] K. Narendra and G. Aghila, "Fortis-ámyna-smart contract model for cross border financial transactions," *ICT Express*, vol. 7, no. 3, pp. 269–273, 2021.

[14] W. Liu, W. Feng, M. Huang, Y. Xu, and X. Zheng, "Steb: A secure service trading ecosystem based on blockchain," *Plos one*, vol. 17, no. 6, p. e0267914, 2022.

[15] T. Wang, H. Hua, Z. Wei, and J. Cao, "Challenges of blockchain in new generation energy systems and future outlooks," *International Journal of Electrical Power & Energy Systems*, vol. 135, p. 107499, 2022.

[16] Q. Wang and M. Su, "Integrating blockchain technology into the energy sector—from theory of blockchain to research and application of energy blockchain," *Computer Science Review*, vol. 37, p. 100275, 2020.

[17] A. Kumar, R. Kumar, and S. S. Sodhi, "A novel privacy preserving blockchain based secure storage framework for electronic health records," *Journal of Information and Optimization Sciences*, vol. 43, no. 3, pp. 549–570, 2022.

[18] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu, "Privacy preservation in permissionless blockchain: A survey," *Digital Communications and Networks*, vol. 7, no. 3, pp. 295–307, 2021.

[19] J. S. Yadav, N. S. Yadav, and A. K. Sharma, "Security analysis of smart contract based rating and review systems: the perilous state of blockchain-based recommendation practices," *Connection Science*, vol. 34, no. 1, pp. 1273–1298, 2022.

[20] Y. Jiang, Y. Zhong, and X. Ge, "Smart contract-based data commodity transactions for industrial internet of things," *IEEE Access*, vol. 7, pp. 180856–180866, 2019.

[21] I. A. Omar, H. R. Hasan, R. Jayaraman, K. Salah, and M. Omar, "Implementing decentralized auctions using blockchain smart contracts," *Technological Forecasting and Social Change*, vol. 168, p. 120786, 2021.

Biography

Jian Zhou, born in 1979. He is a post-doctoral researcher at Beijing University of Post and Telecommunications, and an professor and M.S. supervisor at Anhui University of Finance and Economics. His research interests include key management, security and privacy of mobile systems, cognitive radio networks and secure protocol design in wireless networks, etc.

Shi-hua Huang, born in 1999, master's degree, her main research directions are data mining, business intelligence, etc.

Shi Yan, born in 1998, master student, his main research directions are data mining, business intelligence, etc.

A Lightweight Authentication Protocol for Mobile RFID

Tao Pan[1], Kai-Zhong Zuo[2,3], Tao-Chun Wang[2,3], and Chun-Hong Deng[1]
(Corresponding author: Tao Pan)

College of Internet and Communication, Anhui Technical College of Mechanical and Electrical Engineering[1]
No.16, Wenjin West Rd., Yijiang Dist., Wuhu City 241002, Anhui Province, China
College of Computer and Information, Anhui Normal University[2]
Anhui Key Laboratory of Network and Information Security[3]
No.1, Beijing East Rd., Jinghu Dist., Wuhu City 241000, Anhui Province, China
Email: ahjdpt@126.com
(Received Apr. 24, 2023; Revised and Accepted Nov. 23, 2023; First Online Feb. 23, 2023)

Abstract

Recently, Radio Frequency Identification (RFID) has been widely used. A lightweight security authentication protocol for mobile RFID is proposed to aim at the problems of high complexity and system security in existing mobile RFID authentication protocols. The tag identity is encrypted by the matrix's arrangement and combination of column vectors based on column pseudonyms, which can effectively reduce tag computational complexity. The tag is required to mainly store its identity and shared keys, which can effectively reduce tag storage complexity. During the authentication process, the proposed protocol generates dynamic authentication keys without changing shared keys, which are different in each session. The protocol uses XOR operation to transfer privacy data based on the dynamic authentication keys. This method can effectively reduce the computational complexity of the protocol while protecting privacy data. The protocol requires the receiver to verify the random number in time after receiving information, which can effectively solve the system security problem. Formal proof and analysis results show that the proposed protocol has good security and can resist attacks. The experimental results indicate that the protocol has low complexity, which can effectively reduce the burden of tag operation and storage. It has good value for mobile RFID systems.

Keywords: Arrangement and Combination; Authentication Protocol; Dynamic Authentication Key; Mobile RFID; Random Number

1 Introduction

RFID is a non-contact automatic identification technology which was born in the 20th century. In recent years, Internet of Things (IoT) technology has attracted extensive attention, because it can greatly improve the quality of people's lives. RFID is becoming more and more popular as one of the key technologies of IoT. As the RFID system has low cost and high reliability, it is now widely used and combined with everyday life [1], such as health, agriculture, and so on. Its market capitalization is expected to rise to $ 16.23 billion by 2029 [5, 6].

RFID uses radio signals to identify a product, animal or person. In addition to identifying objects, RFID system also plays an important role in tracking and managing objects [3]. RFID authentication technology is the basis of its applications. A typical RFID system consist of three parts: RFID tag, reader and database. When RFID authentication begins, RFID tag responses to the incident RF energy transferred from the reader. Then the tag sends out the identity information. After receiving the information, the reader can decode and modulate it. Then the reader transmits it to the database. Finally, the database verifies the legitimacy of the tag identity. Through identity authentication, we can confirm whether the tag is a legitimate user registered in the system. As the increasing demand on privacy protection and system security, RFID security authentication technology has become particularly important, and it has more and more attention [23].

Generally, the traditional RFID authentication is regarded as fixed RFID authentication and the RFID reader cannot be moved, which is not suitable for mobile application scenarios. It has been unable to meet people's need. Thus, the mobile RFID authentication is recommended. For example, in animal husbandry, people used to count the growth information of animal artificially in the past. This method cannot feedback growth information in time making it difficult to guide business improvement. The mobile RFID authentication can realize automatic registration and identification of multiple objects. People only need to hold the mobile reader within the specified

range. Then the mobile reader can quickly receive the information and identify a large amount of tag identity. As a result, it greatly improves management level. Mobile RFID authentication brings convenience to people's life and the production of industry and agriculture. However, it brings new challenges. Mobile RFID authentication puts forward new requirements for protocol complexity and system security.

This paper proposes a lightweight authentication protocol for mobile RFID. The rest of the paper is organized as follows. The second section introduces the characteristics of mobile RFID authentication mode and analyzes the challenges of the mode. The third section briefly reviews the typical RFID authentication protocols and analyzes that the current protocols, which are not suitable for mobile RFID system. The fourth section defines some prior knowledge of data encryption required in the authentication process. The fifth section describes detail authentication process of the protocol. The formal proof based on BAN logic of protocol security performance are provided in the sixth section, alongside with the security comparison with existing protocols. The seventh section compares and analyzes the complexity of the protocol through experiments. Finally, the eighth section gives the conclusion of the paper.

2 Authentication Mode of Mobile RFID

In the mobile RFID system, there are three entities, including the database, the mobile reader and the tag. Both the database and the reader have strong computing power and large storage space. They can perform a variety of complex operations. Unlike traditional RFID reader, the mobile RFID reader can be moved randomly. The RFID tag chip has small area and simple hardware structure [2]. Thus, the storage space of the tag is limited, and the computing power is poor. The traditional encryption algorithms with high complexity are not suitable for the tag [9]. The authentication mode of mobile RFID is shown in Figure 1.

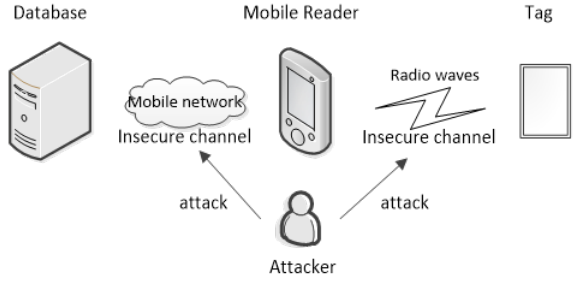


Figure 1: Authentication mode of mobile RFID

At present, there are two modes to authenticate the legitimacy of tag identity. One mode is that the database authenticates the tag identity. When receiving the tag identity, the mobile reader sends it to the database. Then the database authenticates the tag identity. The other mode is that the reader directly authenticates the tag identity. This scheme does not require too much participation of the database. The reader completes the tag identity authentication. It can reduce the number of wireless communications and the risk of communication. However, the mobile reader still needs a small amount of communication with the database in the second mechanism, while increasing the amount of computation of the mobile reader. People usually use the first mode to authenticate the tag identity, rather than using the second mode.

Since the mobile reader is removable, the wired communication channel is no longer suitable for mobile RFID system. The mobile reader communicates with the tag through radio waves. The communication between the database and the reader is based on mobile network. All communication channels are wireless. Due to the weakness of wireless channel, mobile RFID is more vulnerable to illegal attacks than fixed RFID. The attacker can perform signal interference on the channel, which interrupts normal communication. Sometimes, the attacker monitors the channel, intercepts and restores the encrypted data to the plaintext data. System security and privacy protection are the primary problems to be solved.

In fact, the rapid movement of the tag in mobile application scenarios will inevitably affect the efficiency of information reading [19]. It is also difficult to solve the low complexity computing problem of the protocol in mobile RFID system effectively.

3 Related Research Works

In recent years, a variety of RFID security authentication protocols have been proposed. Xu *et al.* proposed an ID-updated mutual authentication protocol for mobile RFID system in Reference [22]. In the protocol, the one-way hash function protects privacy data, and the identity update operation solves the tracking attacks of the tag. Due to the insecure channel of mobile system, it is likely that the data will be out of synchronous. Besides, the identity of the reader is transmitted on the insecure channel. This would suffer information leakage. Shen *et al.* proposed an improved anti-counterfeit complete RFID tag grouping proof generation protocol in Reference [18]. The protocol adopts a one-way pseudo-random function as the basic encryption method. Later, Reference [12] points out that it cannot prevent tag forgery and replay attacks. Tewari *et al.* proposed secure timestamp-based mutual authentication protocol in Reference [20]. The protocol uses timestamps and bitwise operation to provide security against disclosure. The subsequent identity authentication is performed after the initial judgment of whether the communication is legal according to the timestamp value. As the pseudonym information of tag identity is transmitted on the channel directly, the attacker can send

query signal for many times to obtain tag responses. And then, the attacker can obtain timestamp data easily to obtain legitimate authentication of the database. The protocol cannot prevent replay attacks. The reader does not verify the correctness of the information sent by the tag. It is vulnerable to denial-of-service attacks. Besides, the protocol assumes that the channel between the reader and the server is secure. It is not suitable for mobile RFID system. Chegeni *et al.* proposed a lightweight RFID mutual authentication protocol based on hybrid cryptography in Reference [8]. In the protocol, the data is encrypted by advanced encryption standard (AES) and the AES secret key is encrypted by Elliptic-curve (ECC). Since the ECC algorithm is asymmetric cryptography, the secret key is much secure. As reader's identity is not verified, the protocol is prone to replay attacks and denial of service attacks. Liu et al. proposed a mobile RFID authentication protocol in Reference [12]. The protocol adopts bitwise operation to encrypt the information, and requires tag to perform bit-wise operations multiple times, which increase the tag operation cost. It seems that the attacker can easily crack the database identity. The protocol cannot prevent impersonation attacks. The attacker can implement asynchronous attacks by signal interference. Other similar protocols, such as the literature [4, 11, 15, 17, 21].

Through the above analysis, it can find that the public key cryptography and the hash function cryptography are widely used for the current authentication protocols. These encryption methods increase computational cost and reduce the computational efficiency. It is particularly unsuitable for the low-cost RFID tag. Meanwhile, the current protocols face various security problems, such as replay attacks, tag forgery, and so on. All the above protocols are not applicable to the mobile RFID system. Therefore, it is an urgent problem to design a secure and low complexity authentication protocol for the mobile RFID system.

4 Preliminaries

We start to describe some prior knowledge of data encryption, which will be used in the proposed protocol.

4.1 Tag Identity Encryption

To ensure that the sensitive information of the tag cannot be decoded by the attacker, it is necessary to encrypt the identity of the tag. To facilitate the description, we use $Mvp(\ )$ to represent the arrangement and combination of column vectors of matrix. There are two parameters in $Mvp(\ )$, matrix X and parameter a, that is $Mvp(X,\ a)$. Assume that X is the binary number of length L, and the value of column parameter a is known. We first calculate the value of b and d, where b=L/a, d=L mod a, and judge whether d is equal 0. If d is equal 0, X can be expressed as the following equation,

$$X = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1a} \\ x_{21} & x_{22} & \cdots & x_{2a} \\ \vdots & \vdots & \cdots & \vdots \\ x_{b1} & x_{b2} & \cdots & x_{ba} \end{bmatrix}.$$

$Mvp(\ )$ encrypts the data in this way that arranges the column vectors in a sequential order. It is easy to get new data Y, that is, Y=$Mvp(X,\ a)$=$(x_{11}, x_{21}, \cdots, x_{b1}, x_{12}, x_{22}, \cdots, x_{b2}, \cdots, x_{1a}, x_{2a}, \cdots, x_{ba})$. If d is not equal 0, a certain number of binary number 0/1 is filled into X. In this way, the data after X transformation can be expressed as $(x_{11}, x_{12}, \cdots, x_{1a}, x_{21}, x_{22}, \cdots, x_{2a}, \cdots, x_{b1}, x_{b2}, \cdots, x_{ba}, x_{(b+1),1}, \cdots, x_{(b+1),d}, \varphi)$, where $\varphi = \{0,1\}^{(b+1)*a-L}$. Then it gets new data $Y = Mvp(X, a) = (x_{11}, x_{21}, \cdots, x_{b1}, x_{(b+1),1}, x_{12}, x_{22}, \cdots, x_{b2}, x_{(b+1),2}, \cdots, x_{1d}, x_{2d}, \cdots, x_{bd}, x_{(b+1),d}, x_{1,(d+1)}, x_{2,(d+1)}, \cdots, x_{b,(d+1)}, \theta, \cdots, x_{1a}, x_{2a}, \cdots, x_{ba}, \theta)$, where θ is 0 or 1.

Give an example, let X=(11110000) and a=4, then L=8, b=2, d=0. Finally, Y=$Mvp(X,\ a)$=(10101010). It is shown in Figure 2.

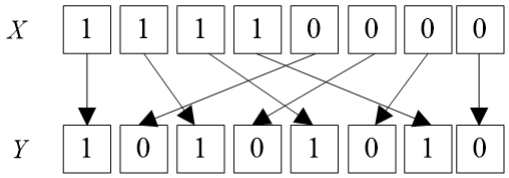


Figure 2: Encryption operation of Mvp()

4.2 Dynamic Authentication Key

In the authentication process, to protect the privacy data, the protocol generates dynamic authentication keys without changing the shared key.

Suppose K_u is a shared key whose binary length is S, it can conveniently use K_{uL} and K_{uR} to represent the dynamic authentication key, where u is a natural number.

Select m-bit binary numbers from the key K_u in order from left to right. The selected numbers are used as the high-bit numbers of K_{uL}. The remainder of K_{uL} is filled with 0. In a similar way, select n-bit binary numbers from the key K_u in order from right to left. The selected numbers are used as the low-bit numbers of K_{uR}. The remainder of K_{uR} is filled with 1.

For example, if K_u = (111001111111), m = 2, n = 6, then the dynamic authentication keys are K_{uL} = $(11\{0\}^{10})$, $K_{uR} = (\{1\}^{6}111111)$. It is shown in Figure 3.

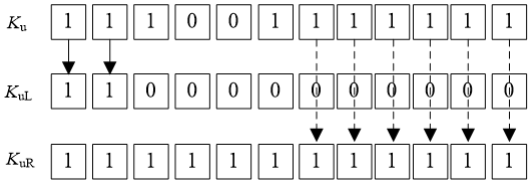


Figure 3: Dynamic authentication key

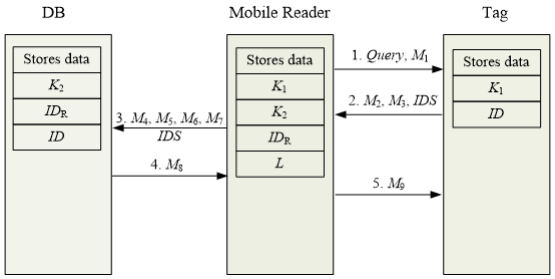


Figure 4: A lightweight authentication protocol for mobile RFID

5 The Proposed Authentication Protocol

5.1 Initial Conditions and Symbols

The tag is usually embedded in products. Sometimes it will be pasted on the object. The tag has low computing power and small storage space. It stores ID and K_1. The mobile reader has strong computing power and large storage space. It stores the binary length of ID, K_1, K_2 and its identity ID_R. The database stores ID, ID_R, K_2. It can verify the legitimacy of tag identity.

The definitions of the symbols used in protocol are shown in Table 1.

Table 1: Symbol definitions

Symbol	Description
ID	Identity of the tag
IDS	Encrypted ciphertext of ID
ID_R	Identity of the reader
L	The binary length of ID
K_1	Private key shared between the reader and the tag
K_2	Private key shared between the database and the reader
K_{1L}	The left part of K_1
K_{1R}	The right part of K_1
K_{2L}	The left part of K_2
K_{2R}	The right part of K_2
r_1	A random number generated by the reader
r_2	A random number generated by the tag
r_3	The other random number generated by the reader
$Mvp()$	The arrangement and combination of column vectors of matrix
$\oplus$	XOR operator
$\|\|$	Connection operator
$\triangleq$	Comparison operator

5.2 Authentication Process

The protocol authentication process is shown in Figure 4.

The authentication steps are described as follows.

Step 1. The reader generates a random number r_1, where $r_1 \in (2, L-1)$. It calculates $M_1 = (K_1 \oplus (r_1/2))||(L \oplus r_1)$. M_1 is divided into two parts. The value of $K_1 \oplus (r_1/2)$ can be marked as M_{1F}. And the value of $L \oplus r_1$ can be marked as M_{1S}. The reader sends query signal and M_1 to active the tag.

Step 2. After receiving the query signal from the reader, the tag performs the following operations.

1) The tag calculates $u_1 = M_{1F} \oplus K_1$ based on the private key, and calculates $u_2 = M_{1S} \oplus L$. It compares the values of u_1 and $u_2/2$ to determine whether they are equal. If they are equal, the tag gets r_1. Otherwise, RFID system suffers from counterfeiting attacks.
2) The tag calculates $p = L/r_1$, $q = Lmodr_1$. Then it uses K_1 and r_1 to calculate the value of a dynamic authentication key K_{1L}. It uses K_1 and p to calculate K_{1R}.
3) The tag calculates $IDS = Mvp(ID, r_1)$.
4) The tag ID is divided into p modules. Each module contains r_1-bit binary numbers. The remaining numbers are stored in the variable δ, if $L > p * r_1$. Then it performs odd check on each module to obtain check bits. These check bits are combined with variable δ to get a new number m.
5) The tag generates a random number r_2 and calculates $M_2 = K_{1R} \oplus r_1$, $M_3 = K_{1L} \oplus (m||r_2)$. Finally, it sends M_2, M_3 and IDS to the reader.

Step 3. After receiving the tag response, the reader performs the following operations.

1) The reader calculates $u_3 = L/r_1$. It uses K_1 and r_1 to calculate the value of a dynamic authentication key K'_{1L}. It also can use K_1 and u_3 to calculate K'_{1R}.
2) The reader calculates $u_4 = M_2 \oplus K'_{1R}$ and compares it with r_1, $u_4 \triangleq r_1$. If they are not equal, the reader determines that the information has been changed by the attacker.

3) The reader calculates $u_5 = M_3 \oplus K'_{1L}$. It is divided into two parts, one of which can be marked as m and the other as r_2. The reader stores r_2 to prevent replay attacks.

4) The reader generates a random number r_3, where $r_3 \in (2, L-1)$, and calculates $u_6 = L/r_3$. Then it uses K_2 and r_3 to calculate the value of a dynamic authentication key K_{2L}. It uses K_2 and u_6 to calculate K_{2R}.

5) The reader calculates $M_4 = K_2 \oplus r_3$, $M_5 = K_{2L} \oplus ID_R$, $M_6 = r_1 \oplus r_3$, $M_7 = r_1 \oplus m$, and sends the message IDS, M_4, M_5, M_6, M_7 to the database.

Step 4. The database verifies the legitimacy of the tag identity and sends response to the reader.

1) The database calculates $u_7 = M_4 \oplus K_2$, and stores it. Next time, it checks whether u'_7 is equal to u_7. If both are equal, the database terminates the authentication. The system suffers replay attacks.

2) The database uses K_2 and r_3 to calculate the value of a dynamic authentication key K'_{2L}. It uses K_2 and L/r_3 to calculate K'_{2R}.

3) The database calculates $u_8 = M_5 \oplus K'_{2L}$ and checks whether u_8 is equal to ID_R to verify the legitimacy of the reader identity.

4) The database calculates $u_9 = M_6 \oplus u_7$ and then calculates $u_{10} = M_7 \oplus u_9$.

5) First, the database gets plaintext of ID using the corresponding decryption, that is $ID = Mvp'(IDS, u_9)$. Later, it verifies the correctness of ID by m. If ID is incorrect, the authentication is terminated. Otherwise, the database verifies the legitimacy of tag identity by matching data ID in the database.

6) If the authentication is success, the received data are correct and legal. The database calculates $M_8 = K_{2R} \oplus (r_3||m)$ and sends it to the reader.

Step 5. The reader verifies the response information from the database at first, and then sends the latest reply about the legitimacy of the tag identity.

1) The reader calculates $u_{11} = M_8 \oplus K_{2R}$. The value of u_{11} is divided into two parts, u_{11F} and u_{11S}.

2) Verify the correctness of u_{11F} and u_{11S}. If there is $u_{11F} = r_3$, it indicates that the information is a reply to the request which is sent by the reader just now. And if there is $u_{11S} = m$, it indicates that the information is a response to the authentication of the current tag identity.

3) The reader calculates $M_9 = K_{1R} \oplus (u_3||r_2)$ and sends it to the tag.

Step 6. The tag calculates $u_{12} = M_9 \oplus K_{1R}$. The value of u_{11} is divided into two parts, u_{12F} and u_{12S}. The tag compares u_{12F} with p, $u_{12F} \triangleq p$. If it is the same, the tag determines that the received information is a reply to the current query. Then the tag compares u_{12S} with r_2, $u_{12S} \triangleq r_2$. If it is the same, the authentication is successful. Otherwise, the authentication fails.

6 Security Analysis and Comparisons

6.1 Formal Proof

BAN logic uses knowledge and belief to describe and reason authentication protocol. It is a kind of modal logic reasoning rule, which can effectively prove the security of the protocols [7]. In this paper, the security of the protocol is proved by using BAN logic formal proof. The proof of BAN logic has four steps. Firstly, establish the idealized protocol model. Secondly, give a reasonable protocol initial assumption. Thirdly, give expected safety objectives of protocol. Finally, proof the security of the protocol according to reasoning rules.

For the convenience of proof, we make the following provisions. The database, mobile reader and tag are represented by DB, R and T respectively. $a \oplus b$ can be seen as $\{a\}_b$ or $\{b\}_a$. $Mvp(ID, a)$ can be seen as $\{ID\}_a$. The inference rules of BAN logic used in the proof are introduced as follows.

Message-meaning rule R1: $\frac{P|\equiv P \overset{K}{\leftrightarrow} Q, P \lhd \{X\}_K}{P|\equiv Q|\sim X}$

Nonce-verification rule R2: $\frac{P|\equiv \#(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$

Jurisdiction rule R3: $\frac{P|\equiv Q \Longrightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$

Seeing rule R4: $\frac{P \lhd (X,Y)}{P \lhd X}$

Session-key rule R5: $\frac{P|\equiv \#(K), P|\equiv Q|\equiv X}{P|\equiv P \overset{K}{\leftrightarrow} Q}$, and X is a necessary factor of K.

1) An Idealized Protocol Model

Through analysis, the idealized model of the protocol can be expressed as follows.

$M\_1 : R \rightarrow T : (\{r_1\}_{K_1}, \{r_1\}_L)$

$M\_2 : T \rightarrow R : \{r_1\}_{K_1}, \{(m, r_2)\}_{K_1}, \{ID\}_{r_1}$

$M\_3 : R \rightarrow DB : \{r_3\}_{K_2}, \{ID_R\}_{K_2}, \{r_1\}_{r_3}, \{m\}_{r_1}, \{ID\}_{r_1}$

$M\_4 : DB \rightarrow R : \{(r_3, m)\}_{K_2}$

$M\_5 : R \rightarrow T : \{(r_1, r_2)\}_{K_1}$

2) Original Hypothesis

Initial assumptions of the protocol can be expressed as follows.

P1: $DB \mid\equiv DB \overset{K_2}{\leftrightarrow} R$. It means that DB believes DB and R use the shared key K_2 to communicate each other.

P2: $DB \mid\equiv \#(r_1)$. It means that DB believes r_1 is fresh.

P3: $DB \mid\equiv \#(r_3)$. It means that DB believes r_3 is fresh.

P4: $DB \mid\equiv \#(ID)$. It means that DB believes ID is fresh.

P5: $DB \mid\equiv R \Longrightarrow D$. It means that DB believes R has jurisdiction over ID.

P6: $R \mid\equiv T \mid\Longrightarrow r_1$. It means that R believes T has jurisdiction over r_1.

P7: $R \mid\equiv (\#r_1)$. It means that R believes r_1 is fresh.

P8: $R \mid\equiv T \overset{K_1}{\leftrightarrow} R, T \mid\equiv R \overset{K_1}{\leftrightarrow} T$. It means that R and T may use the shared key K_1 to communicate each other.

P9: $T \mid\equiv R \mid\Longrightarrow r_2$. It means that T believes R has jurisdiction over r_2.

P10: $T \mid\equiv (\#r_2)$. It means that T believes r_2 is fresh.

3) The expected safety objectives

G1: $DB \mid\equiv ID$. It means that DB believes ID is correct. That is to say, the tag identity authentication is successful.

G2: $R \mid\equiv r_1$. It means that R believes r_1 is correct. That is to say, the reader receives the legitimate data from the tag.

G3: $T \mid\equiv r_2$. It means that T believes r_2 is correct. That is to say, the tag receives the successful authentication responses from the reader.

4) Formal proof

With massage M_4, using seeing-key rule R4:$\frac{DB \lhd \{(r_3,m)\}_{K_2}}{DB \lhd \{r_3\}_{K_2}}$. With initial assumptions P1, using message-meaning rule R1: $\frac{DB \mid\equiv DB \overset{K_2}{\leftrightarrow} R, DB \lhd \{r_3\}_{K_2}}{DB \mid\equiv R \mid\sim r_3}$. With initial assumptions P3, using nonce-verification rule R2: $\frac{DB \mid\equiv \#(r_3), DB \mid\equiv R \mid\sim r_3}{DB \mid\equiv R \mid\equiv r_3}$. With initial assumptions P3, using session-key rule R5: $\frac{DB \mid\equiv \#(r_3), DB \mid\equiv R \mid\equiv r_3}{DB \mid\equiv DB \overset{r_3}{\leftrightarrow} R}$. With massage M_3, using message-meaning rule R1:$\frac{DB \mid\equiv DB \overset{r_3}{\leftrightarrow} R, DB \lhd \{r_1\}_{r_3}}{DB \mid\equiv R \mid\sim r_1}$. With initial assumptions P2, using nonce-verification rule R2:$\frac{DB \mid\equiv \#(r_1), DB \mid\equiv R \mid\sim r_1}{DB \mid\equiv R \mid\equiv r_1}$. With initial assumptions P2, using session-key rule R5:$\frac{DB \mid\equiv \#(r_1), DB \mid\equiv R \mid\equiv r_1}{DB \mid\equiv DB \overset{r_1}{\leftrightarrow} R}$. With massage M_3, using message-meaning rule R1: $\frac{DB \mid\equiv DB \overset{r_1}{\leftrightarrow} R, DB \lhd \{ID\}_{r_1}}{DB \mid\equiv R \mid\sim ID}$. With initial assumptions P4, using nonce-verification rule R2:$\frac{DB \mid\equiv \#(ID), DB \mid\equiv R \mid\sim ID}{DB \mid\equiv R \mid\equiv ID}$. With initial assumptions P5, using Jurisdiction rule R3:$\frac{DB \mid\equiv R \Longrightarrow ID, DB \mid\equiv R \mid\equiv ID}{DB \mid\equiv ID}$. we can obtain result $DB \mid\equiv ID$.

Using a similar method, we can obtain results $R \mid\equiv r_1, T \mid\equiv r_2$. All objectives are proved.

6.2 Security Analysis

1) Brute force attack. The attacker can acquire communication data via eavesdropping. Then it implements a brute force attack on the data stolen. Most information is encrypted using XOR operation based on the shared key. The key K_1 and K_2 are privacy keys, which are not disclosed to anyone. Even if the attacker gets M_1, M_2, M_3 and M_9, it is impossible to obtain any plaintext data because there is no K_1. Even if the attacker gets M_4, M_5 and M_8, it is impossible to obtain any plaintext data because there is no K_2. If M_6, M_7, IDS are obtained, the attacker cannot get plaintext data because of the lack of a random number r_1. M_6, M_7, IDS are encrypted by XOR operation. If a number has 128 bits, the guessed probability is 2^{128} which is very small. Based on the above analysis, the proposed protocol can prevent brute force attack.

2) Impersonation attack. The attacker can masquerade as the reader or the tag to pass legal authentication [13]. In the protocol, the attacker fakes the tag and sends M_2, M_3, IDS to the reader. After receiving the information, the reader first verifies the correctness of the number r_1 generated by itself. Since K_{1R} and r_1 are random numbers, the number M_2 sent by the attacker cannot be the same as the value of $K_{1R} \oplus r_1$. The attacker failed to fake the tag.

Later, the attacker fakes the reader and sends query signal and M_1 to the tag. The tag verifies the correctness of the number r_1 after receiving the query. The number r_1 is a random number, which is different in each session. The attacker cannot obtain the values of K_1 and L by analyzing the previous M_1. The attacker failed to fake the reader.

In the mobile RFID system, the attacker may impersonate the reader to send information to the database. The protocol requires the database to use dynamic authentication key K_{2L} to detect the reader identity ID_R. It can effectively prevent fake reader attack initiated by the attack.

Based on the above analysis, it is found that the proposed protocol can effectively resist impersonation attack.

3) Replay attack. The attacker collects data through listening channels, then it uses them to obtain legal identity authentication. In the protocol, the attacker acquires M_2, M_3, IDS, and sends them to the reader. When receiving the information, the reader first verifies the correctness of r_1. After that, the reader verifies r_2. Since r_1 and r_2 are random numbers, their values are different for each authentication. The attacker failed to replay the tag information.

In the mobile RFID system, the attacker may attempt to replay the reader request information IDS, M_4, M_5, M_6, M_7 to the database. The database first

calculates $u_7 = M_4 \oplus K_2$. Then it compares u_7 with the stored r_3 to determine whether the information is replayed. So, the protocol can resist replay attack.

4) Asynchronous attack.The encryption operation in the protocol is mainly based on the private keys $K_1, K_2, K_{1L}, K_{1R}, K_{2L}, K_{2R}$. The value of the keys K_1, K_2 are not update after each authentication. K_{iL}, K_{iR} are obtained by transforming K_i, where $i \in (1, 2)$. They are set up temporarily during the execution of the protocol. There will be no asynchronous update of the shared key. So, the protocol can resist asynchronous attack.

5) Forward security. If the secret key is exposed or leaked during current session, the attacker can predict the secrets of previously exchanged messages [14]. In the protocol, suppose that the attacker obtains the encrypted data M_1, M_4, M_6, M_7, IDS is the number by using XOR operation based on the random number, and M_2, M_3, M_5, M_8, M_9 are the numbers by using XOR operation based on the dynamic authentication key. The random number and the dynamic authentication key can prevent forward security attack.

6) Denial of service (Dos). The attacker overloads the reader by transmitting interference signals. The reader cannot respond to the request for the legitimate tag. In the protocol, when receiving the information, the reader first verifies the correctness of r_1. Since r_1 is a random number, it is different in each session. The reader can quickly determine whether the signal comes from a legitimate tag. The protocol can effectively resist denial of service attack.

6.3 Security Comparisons

The security comparison between the proposed protocol and the existing protocols is shown in Table 2. It is obvious that the proposed protocol has the best security performance compared with the existing protocols.

7 Complexity Performance Evaluation

Due to the strong computing power and large storage space of the database and the reader, the performance advantages of the protocol are mainly reflected in the storage complexity and computational complexity of the tag.

7.1 Storage Complexity

The storage complexity of the protocol is mainly reflected by storage performance of the tag. Considering the limited storage space of the tag, the tag storage overhead should be reduced when designing the protocol. Generally, the storage space is divided into basic storage space and temporary storage space. The basic storage space is set by the manufacturer when the tag is delivered. The temporary storage space is the additional space that the tag needs to temporarily allocate according to its own calculation.

We make the following assumptions, L_{ID} is the length of the tag identity, L_K is the length of the private key, L_F is the length of the encryption function, L_N is the length of the number, and L_{bit} is the length of the bitwise operation. Generally, the key and the number have the same length. They are also operation objects of bitwise operation. That is $L_N = L_K = L_{bit}$. The tag storage space comparison is shown in Table 3.

In Table 3, we find that the basic storage space of the tag in the proposed protocol is equivalent to that of Reference [20]. But with the authentication processing development, the temporary auxiliary storage space is significantly reduced. We observe that the tag total storage space of the proposed protocol is the smaller than other protocols listed in Table 3.

7.2 Computational Complexity

The database and mobile reader have strong computing power in mobile RFID system. The primary factor affecting the computational complexity of the protocol is the efficiency of tag operation. The paper evaluates the computational complexity of the protocol based on experiment of authenticating the legitimacy of tag identity. The experiment is done on the real scene.

Hardware and software environment configuration used in the experiment are as follows.

Upper computer configuration: Intel Core i7-11800H CPU @ 4.2GHZ, 512G Memory, Win10 OS, Visual Studio 2022 as a development environment, MYSQL database.

Hardware of the reader and the tag: Magic RF M100 reader, nRF24LE tag.

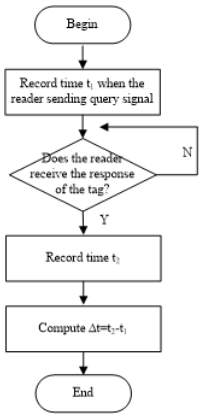


Figure 5: Design flow chart

The efficiency of tag operation is evaluated by the tag computing time. The length of tag identity is generally within 512 bits in EPC and ISO/IEC standard RFID system [10, 16]. Figure 5 shows the design flow chart of

Table 2: Comparison of security features

Protocol	Brute force attack	Impersonation attack	Replay attack	Asynchronous attack	Forward security	Denial of service
Reference [22]	N	Y	Y	N	N	Y
Reference [18]	Y	N	N	Y	Y	Y
Reference [12]	Y	N	Y	N	Y	Y
Reference [20]	N	Y	N	Y	N	N
Reference [8]	Y	Y	N	Y	Y	N
Proposed protocol	Y	Y	Y	Y	Y	Y

$Y: yes, N: no$

Table 3: Comparison of the tag storage space

Protocol	Basic storage space	Temporary storage space
Reference [22]	$2L_{ID}+L_K$	$L_F+5L_N+L_K$
Reference [18]	$L_{ID}+2L_K$	$2L_F+5L_N+L_K+L_{bit}$
Reference [12]	$L_{ID}+2L_K$	$2L_F+6L_{bit}$
Reference [20]	$L_{ID}+L_K$	$2L_F+L_N+4L_{bit}$
Reference [8]	$L_{ID}+L_K$	$2L_F+5L_N$
Proposed Protocol	$L_{ID}+L_K$	$L_F+2L_N+2L_{bit}$

obtaining the tag computing time. Figure 6 shows the experimental scene of tag authentication.

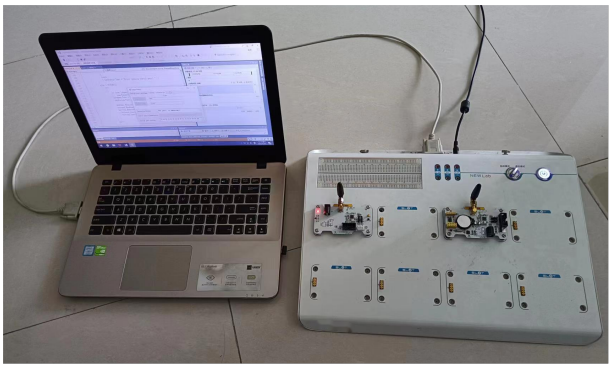


Figure 6: Experimental scene

In the upper computer, the application program is designed by C # language, which can record and display the computing time of the tag. It is shown in Figure 7 and Figure 8.

In References [22] and [8], the tag needs to perform hash function or symmetric encryption function with high complexity for many times. In References [12, 18, 20], the tag performs bitwise operation and bit operation function for many times. However, the proposed protocol only needs to perform one permutation and combination operation, as well as less bitwise operation and arithmetic operation.

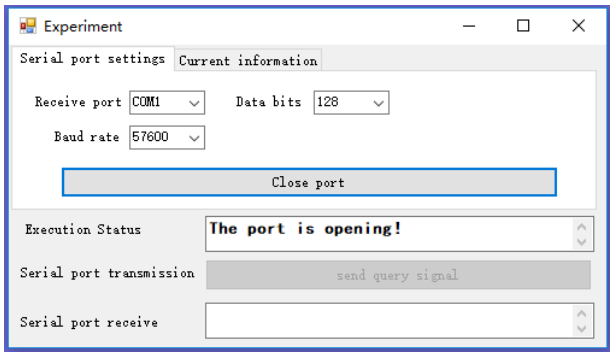


Figure 7: Serial port settings

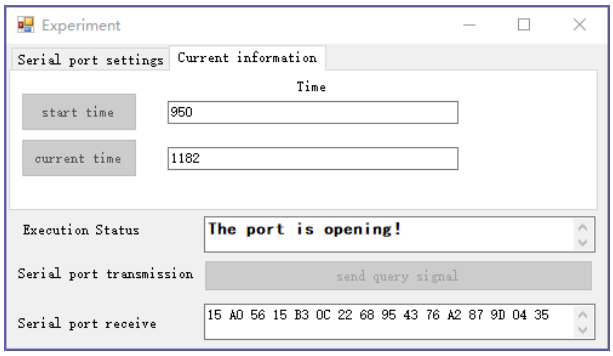


Figure 8: Current information

We assume that the results of all functions in each protocol have same length. Figure 9 shows a comparison of the tag computing time between the proposed protocol and other protocols. As the length of tag identity increases, the computing time of tag of the proposed protocol is significantly reduced.

Although the mobile reader has strong computing power, the low complexity operation of the reader has great value for mobile scenario applications of the protocol. For example, in the electronic toll collection (ETC) system, the low complexity operation of the reader can not only improve the detection efficiency of vehicles, but also prevent car collisions caused by slow detection.

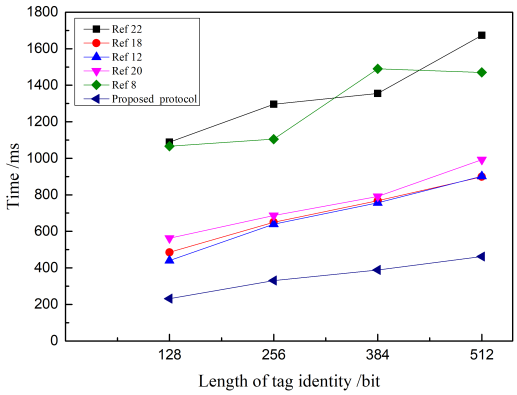


Figure 9: Comparison of tag computing time

In the experiment, we can record time t_0 when the authentication process begins. Record time t_1 when the reader sending query signal. Record time t_2 when the reader receiving the data from the tag. Record time t_3 when the reader sending the data to the database. Record time t_4 when the reader receiving the data from the database. Record time t_5 when the reader sending the data to the tag. Clearly, we can simply to calculate the result, $\Delta t_0 = t_1 - t_0$,$\Delta t_1 = t_3 - t_2$, $\Delta t_2 = t_5 - t_4$. The computing time of the reader is $\Delta t_0 + \Delta t_1 + \Delta t_2$.

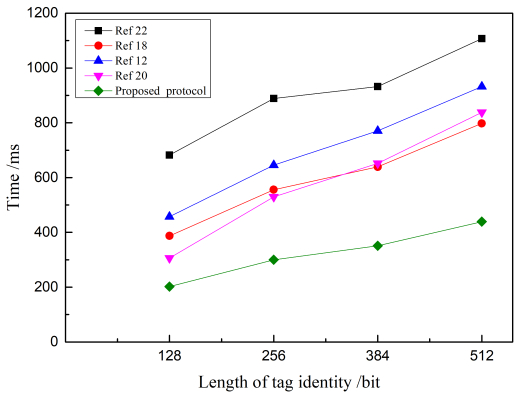


Figure 10: Comparison of reader computing time

References [8] doesn't participate in the comparative experiment, because the reader only performs forwarding operations. In References [22], the reader needs to perform hash function several times. In References [12, 18, 20], the reader performs bitwise operation and bit operation function for many times. In the proposed protocol, the reader uses XOR operation to transfer privacy data, which can reduce the computational complexity. Figure 10 shows a comparison of the reader computing time. As the length of tag identity increases, the computing time of reader of the proposed protocol is reduced significantly.

In summary, the computational complexity of the protocol has obvious advantages. The protocol is suitable for mobile RFID system.

8 Conclusion

In this paper, we have presented a lightweight security authentication protocol for mobile RFID. The tag performs the operation of arrangement and combination of column vectors based on column pseudonym to encrypt its identity. The protocol uses XOR operation to transfer privacy data based on the dynamic authentication keys. Meanwhile, it requires the receiver to verify the random number in time after receiving the information. Formal proof and analysis results show that the proposed protocol has good security and can resist various attacks. Furthermore, the proposed protocol has the low complexity, and it can be well used in the field of production and life.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (61972438), Anhui Natural Science Foundation (2108085MF219), the Key Program of Universities Natural Science Research of the Anhui Provincial Department of Education (KJ2020A1112), Special Project of Science and Technology Development Center of the Ministry of Education of china (2021ALA04004).

References

[1] A. Abuzneid, S. A. Mellouki, Z. Siraj, et al., "Low-cost rfid authentication protocol based on elliptic curve algorithm," *International Journal of Interdisciplinary Telecommunications and Networking*, vol. 13, no. 2, pp. 1–11, 2021.

[2] M. B. Ahmad and F. A. Nababa, "The need of using a radio frequency identification system," *International Journal of New Computer Architectures and their Applications*, vol. 11, no. 2, pp. 22–29, 2021.

[3] H. L. Alaoui, A. E. Ghazi, M. Zbakh, et al., "A highly efficient ecc-based authentication protocol for rfid," *Journal of Sensors*, vol. 2021, no. 4, pp. 1–16, 2021.

[4] U. Ali, M. Y. I. B. Idris, M. N. B. Ayub, et al., "Rfid authentication scheme based on hyperelliptic curve signcryption," *IEEE Access*, vol. 9, pp. 49942–49959, 2021.

[5] S. Anandhi, R. Anitha, and V. Sureshkumar, "An authentication protocol to track an object with multiple rfid tags using cloud computing environment," *Wireless Personal Communications*, vol. 113, no. 2, pp. 2339–2361, 2020.

[6] A. Arslan, S. A. Colak, and S. Erturk, "A secure and privacy friendly ecc based rfid authentication

protocol for practical applications," *Wireless Personal Communications*, vol. 120, no. 4, pp. 2653–2691, 2021.

[7] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems*, vol. 8, no. 1, pp. 18–36, 1990.

[8] V. Chegeni, H. Javadi, M. Goudarzi, et al., "Providing a hybrid cryptography algorithm for lightweight authentication protocol in rfid with urban traffic usage case," *The ISC International Journal of Information Security*, vol. 13, no. 1, pp. 73–85, 2021.

[9] N. Dinarvand and H. Barati, "An efficient and secure rfid authentication protocol using elliptic curve cryptography," *Wireless Networks*, vol. 25, no. 1, pp. 415–428, 2019.

[10] B. Fatemeh and C. K. Nemai, "Hybrid chipless rfid tags-a pathway to epc global standard," *IEEE Access*, vol. 6, pp. 67415–67426, 2018.

[11] T. F. Lee, K. W. Lin, Y. P. Hsieh, et al., "Lightweight cloud computing-based rfid authentication protocols using puf for e-healthcare systems," *IEEE Sensors Journal*, vol. 23, no. 6, pp. 6338–6349, 2023.

[12] D. W. Liu, S. H. Xu, and W. T. Zuo, "A mobile rfid authentication protocol based on self-assembling cross-bit algorithm," *International Journal of Network Security*, vol. 24, no. 5, pp. 975–983, 2022.

[13] M. Mehrabani and S. Sadegha, "Security analysis and improvement of wei-chi ku and yi-han chen's rfid protocol," *International Journal of Innovation in Engineering*, vol. 1, no. 2, pp. 73–83, 2021.

[14] M. Naeem, S. A. Chaudhry, K. Mahmood, et al., "A scalable and secure rfid mutual authentication protocol using ecc for internet of things," *International Journal of Communication Systems*, vol. 33, no. 7, pp. 1–13, 2019.

[15] I. Sarah, B. Mustapha, and D. Karim, "An enhanced scalable and secure rfid authentication protocol for wban within an iot environment," *Journal of information security and applications*, vol. 58, no. 86, pp. 1–15, 2021.

[16] G. Saxl, M. Ferdik, M. Fischer, et al., "Uhf rfid prototyping platform for iso 29167 decryption based on an sdr," *Sensors*, vol. 19, no. 10, pp. 1–12, 2019.

[17] M. Shariq, K. Singh, M. Y. Bajuri, et al., "A secure and reliable rfid authentication protocol using digital schnorr cryptosystem for iot-enabled healthcare in covid-19 scenario," *Sustainable Cities Society*, vol. 75, pp. 1–13, 2021.

[18] G. F. Shen, S. M. Gu, and D. W. Liu, "An anti-counterfeit complete rfid tag grouping proof generation protocol," *International Journal of Network Security*, vol. 21, no. 6, pp. 889–896, 2019.

[19] J. Su, Z. Sheng, and A. X. Liu, "Capture-aware identification of mobile rfid tags with unreliable channels," *IEEE Transactions on Mobile Computing*, vol. 14, no. 8, pp. 1182–1195, 2020.

[20] A. Tewari and B. B. Gupta, "Secure timestamp-based mutual authentication protocol for iot devices using rfid tags," *International Journal on Semantic Web and Information Systems*, vol. 16, no. 3, pp. 20–34, 2020.

[21] G. H. Wei, Y. L. Qin, and W. Fu, "An improved security authentication protocol for lightweight rfid based on ecc," *Journal of Sensors*, vol. 2022, pp. 1–6, 2022.

[22] Y. Xu and J. S. Yuan, "Design and analysis of an id-updated mutual authentication protocol for mobile rfid system," *Photonic Network Communications*, vol. 37, no. 2, pp. 204–211, 2019.

[23] Z. G. Zhao, "A secure rfid authentication protocol for healthcare environments using elliptic curve cryptosystem," *Journal of Medical Systems*, vol. 38, no. 5, pp. 46–47, 2014.

Biography

Tao Pan was born in 1986. He is a lecturer at Anhui Technical College of Mechanical and Electrical Engineering. His major research interests include RFID technology and information security.

Kai-Zhong Zuo was born in 1974. He received his Ph.D. from Shanghai University. He is currently a professor and a supervisor of Master's student at Anhui Normal University. His major research interests include data security and privacy preservation.

Tao-Chun Wang was born in 1979. He received his Ph.D. from Nanjing University of Aeronautics. He is currently a professor and doctoral tutor at Anhui Normal University. His major research interests include sensor technology and crowd sensing.

Chun-Hong Deng was born in 1970. He is currently a professor at Anhui Technical College of Mechanical and Electrical Engineering. His major research interests include internet of things.

Research on the Protection of Personal Sensitive Information and Privacy Data on the Internet Under Legal Regulations

Xiaodan Li

(Corresponding author: Xiaodan Li)

Law Teaching and Research Department, Qingdao Party School of CPC
Qingdao, Shandong 266071, China
Email: lixdxd@hotmail.com

(Received Dec. 15, 2022; Revised and Accepted Dec. 11, 2023; First Online Feb. 23, 2024)

Abstract

The current legal framework falls short in adequately addressing the protection needs of personal sensitive information and privacy data on the Internet, demanding more effective safeguarding through reliable algorithms. This paper commences with a concise overview of the existing legal system. Subsequently, focusing on the data classification task, the differential privacy algorithm was integrated with the XGBoost algorithm to create the differential privacy-extreme gradient boosting (DP-XGBoost) algorithm. The method's performance was then analyzed using a dataset. The results revealed that the XGBoost algorithm outperformed the C4.5 algorithm in classification accuracy. Compared with DiffP-C4.5 and DP-random forest (RF), the DP-XGBoost algorithm exhibited superior accuracy under various privacy budgets. Furthermore, when compared with the XGBoost algorithm at different maximum tree depths, the DP-XGBoost algorithm experienced an accuracy loss of within 5%. These findings demonstrate that the DP-XGBoost algorithm can deliver privacy protection while ensuring robust classification performance, making it applicable for safeguarding real personal sensitive information and privacy data.

Keywords: Cybersecurity; Legal System; Privacy Data; Sensitive Information; XGBoost

1 Introduction

In the era of widespread Internet usage, various industries are increasingly relying on the Internet, leading to the accumulation of vast amounts of information data [20]. Information data such as user preferences recorded on shopping websites, patient information stored in online hospitals, and other valuable knowledge are crucial for decision-making in areas such as personalized recommendation, disease prediction, and opportunity identification [12]. However, the surge in personal sensitive information and privacy data leaks has become a serious concern [17]. For instance, in personalized recommendation research, there is a risk of leaking user identity information, and disease prediction studies may inadvertently expose patients' medical information. Balancing the utilization of data with the imperative to protect privacy is paramount [14]. While legal systems have enacted legislation to safeguard personal privacy, the rapid evolution of the Internet necessitates more than legal frameworks alone to address the growing demand for privacy protection in the current big data environment. Consequently, researchers are increasingly exploring different algorithms to protect information data without compromising usability [2].

Huang *et al.* [8] integrated differential privacy (DP) into various stages of principal component analysis-support vector machine (PCA-SVM), resulting in DPPCA-SVM and PCADP-SVM. The theoretical and experimental analysis demonstrated the effectiveness of these methods concerning noise expectation and classification accuracy. Zhang *et al.* [21] proposed a local DP K-modes clustering data privacy-preserving method, achieving protection of user privacy without third-party during clustering. Handa *et al.* [7] tackled the data utilization challenge posed by encryption through a searchable encryption method, allowing end-users to retrieve relevant documents from the cloud. However, the balance between search power and efficiency remains an area of investigation. Pasupuleti *et al.* [15] designed a lightweight attribute-based encryption scheme to provide privacy and access control for cloud data. This paper provides an overview of the current legal system regarding personal privacy protection. Addressing the limitations of the legal system, this paper proposes a protection method that combines DP and extreme gradient boosting (XGBoost) to safeguard personal sensitive information and privacy data. Experimental results verified the method's efficacy, offering a novel approach to reinforce privacy protection

and enhance information security. Furthermore, it contributes theoretical foundations for effectively combining DP with classification algorithms.

2 Current Status of Internet Information Data Protection Under Legal Regulations

In the era of rapid Internet development, the incidence of sensitive personal information and privacy data leakage and misuse has been on the rise. There are some notable incidents.

In 2013-2014, Yahoo Inc. experienced a massive hack, resulting in the theft of account information for approximately 3 billion users, including names, passwords, and other sensitive details. In 2018, Cambridge Analytica unlawfully accessed the personal data of millions of Facebook users. In 2019, Baidu App faced accusations of collecting sensitive information, such as geolocation and search history, in the background without users' explicit consent.

The escalating issue of privacy breaches has prompted the development of regulations and legislations worldwide to govern methods related to personal information data [11]. For instance, the European Union has introduced the General Data Protection Regulation (GDPR) [6], which sets guidelines for gathering and handling personal data. Similarly, California Consumer Privacy Act (CCPA) mandates that companies afford consumers a certain level of control over their data. Comparable regulations are also in place in Canada and Japan.

China's Personal Information Protection Law incorporates provisions to safeguard sensitive personal information and privacy data, including:

1) The purpose and manner of handling personal information must be clearly defined;
2) Personal information unrelated to service provision should not be collected;
3) Individuals have the right to access, correct, and delete their personal information;
4) Relevant authorities are tasked with strengthening the supervision and management of personal information.

However, the existing legal framework faces challenges in meeting the current demands of personal privacy data protection. Emerging technologies and regulatory challenges have rendered the current regulations somewhat inadequate in addressing contemporary privacy issues. To enhance the protection of sensitive personal information and private data, various technologies are being applied, categorized into three types.

1) Data anonymization: This involves fuzzy processing of data through the deletion and hiding of sensitive information, i.e., cutting off the association between the user's identity and personal data. Common techniques include k-anonymity and l-diversity [10].
2) Data encryption: Techniques like secure multi-party computation and homomorphic encryption encode plaintext data into ciphertext, ensuring the security of personal information during release or transmission [1].
3) DP: This method protects privacy data by introducing noise perturbations to the original information, making it challenging for attackers to infer the original data through perturbed data [3].

Each technique has unique characteristics. Anonymization algorithms are easy to implement but may perform poorly under complex privacy attacks. Encryption algorithms provides high data availability but comes with substantial computational costs. DP excels in privacy protection but requires reasonable control of the privacy budget. Given the broad applications of personal sensitive information and privacy data, such as in personalized recommendations and trend predictions, this paper proposes a classification algorithm designed to effectively protect this information, incorporating the principles of DP.

3 XGBoost Algorithm Based on Differential Privacy

3.1 Differential Privacy

Given a randomized algorithm A, if there are neighboring datasets D_1 and D_2 ($|(D_1-D_2)\cup(D_2-D_1)|=1$), function Q is queried. If the range of query results $r \subseteq Range(Q)$ satisfies:

$$Pr[A_Q(D_1)=r] \le e^{\epsilon} \times Pr[A_Q(D_2)=r],$$

then the algorithm is said to satisfy ϵ-DP, probability $Pr[]$ is controlled by the randomness of the algorithm. ϵ is the privacy budget. The smaller the value of ϵ, the higher the privacy protection, but meanwhile the lower the availability of the data.

For any function $f: D \to R^d$, its input is D, and its output is a d-dimensional vector called R^d. If

$$\Delta f = \max_{D_1,D_2} ||f(D_1)-f(D_2)||_p$$

then, Δf is called the global sensitivity of f. p is used to measure the L_p distance used by Δf, usually L_1, i.e., 1-oder norm distance.

The implementation of DP requires corresponding noise mechanisms, of which two are commonly used.

1) Laplace mechanism [13]: For numeric data, Laplace noise $Lap(\Delta f/\epsilon)$ is added to query result $f(D)$. Algorithm A is said to satisfy ϵ-DP if and only if the output of the algorithm satisfies:

$$A(D) = f(D) + Lap(\Delta f/\epsilon).$$

2) Indexing mechanism: It is applicable to non-numerical data. Evaluation function q with a low sensitivity level is selected, and its sensitivity level is defined as:

$$S(q) = \max_{D_1, D_2, r} ||q(D_1, r) - q(D_2, r)||$$

For dataset D, if algorithm A satisfies the requirement that the probability that the output is r has a proportional relationship with $\exp[\frac{\epsilon q(D,r)}{2S(q)}]$, then algorithm A is said to satisfy ϵ-DP.

3.2 XGBoost Algorithm

Among classification algorithms, the XGBoost algorithm is a Boosting algorithm [9], which trains multiple decision trees as weak classifiers and accumulates them to obtain the final model, thus achieving good performance. The objective function of the XGBoost algorithm can be written as:

$$obj(\theta) = \sum_{i=1}^{N} l(y_i, \hat{y_l}) + \sum_{j=1}^{t} \Omega(f_j),$$

where y_i and $\hat{y_l}$ are the real data and target data, and f_j refers to the j-th weak classifier. There are totally t weak classifiers. There is a constraint function:

$$\Omega(f_t) = \gamma T + \frac{\lambda}{2} \sum_{j=1}^{T} w_j^2$$

where T and w represent the number of leaf nodes and the output fraction, γ and λ are constants. Leaf node number and the corresponding fraction are unified, then:

$$f_t(x) = w_h(x),$$

where $h(x)$ refers to the leaf node mapped by sample x and $w_h(x)$ is the calculated leaf node fraction. After Taylor expansion, the objective function of the XGBoost algorithm is obtained:

$$obj^{(t)} = \gamma T + \frac{1}{2} \sum_{i=1}^{T} (\frac{G_j^2}{H_j + \lambda})$$

where G_j and H_j are the first and second order derivative values of the sample.

3.3 XGBoost Based on DP

In this paper, DP is combined with the XGBoost algorithm to design a DP-XGBoost algorithm with the aim that no third-party attacker can utilize the algorithm to infer personal sensitive information and privacy data. The decision tree for the XGBoost algorithm is constructed using the classification and regression tree (CART) algorithm [16], which uses Laplace noise perturbation for each leaf node during internal node splitting. For the j-th leaf node, its sensitivity level is defined as:

$$\Delta V_{X,j} \leq \frac{g_l^*}{1+\lambda}$$
$$g_l^* = \max_{i \in D} || \frac{\vartheta(y_i, \hat{y_l})}{\vartheta \hat{y_l}} || = \max ||g_i||,$$

where g_l^* is the maximum value of the absolute value of the first-order derivative (also called the gradient value).

When adding noise, if the maximum sensitivity level is set for each leaf node, it will affect the accuracy of the model. In order to reduce the sensitivity of the posterior iteration tree, during the leaf node computation process, the sample gradient is cropped, i.e., for the t-th tree, sample gradient $\widetilde{g_i}$ needs to satisfy $|\widetilde{g_i}| \leq g_l^*(1-\delta)^{t-1}$, where δ is the shrinkage rate, which is the ratio of the output results of all samples on the first decision tree to the real data. At this time, the sensitivity level of the j-th leaf node on the t-th tree satisfy:

$$\Delta \widetilde{V_{X,j}} \leq \frac{g_l^*}{1+\lambda}(1-\delta)^{t-1}.$$

When calculating each leaf node, the original gradient value is first compared to $g_l^*(1-\delta)^{t-1}$. If the original gradient value is greater, $g_l^*(1-\delta)^{t-1}$ is used to replace the original gradient value, thus realizing that the leaf node sensitivity level is reduced in form of $(1-\delta)^{t-1}$.

Privacy budget ϵ allocation can cause certain effects on the classification accuracy of the XGBoost algorithm, the DP-XGBoost algorithm realizes the allocation of ϵ based on shrinkage rate δ. For dataset D, the number of samples allocated to the t-th tree is $\frac{|D|\delta(1-\delta)^{t-1}}{1-(1-\delta)^T}$. By this way, sample waste can be avoided and every sample can be selected.

The DP-XGBoost algorithm is applied to data classification tasks, and its procedure is as follows.

1) The dataset is divided into a training set and a test set. $\frac{|D|\delta(1-\delta)^{t-1}}{1-(1-\delta)^T}$ samples are extracted from the training set and assigned to the t-th tree. Extraction is repeated T times.

2) The value of ϵ is initialized to obtain a decision tree that satisfies DP protection.

3) The training set assigned to the current tree is assigned to the root node, followed by step-by-step split to build a decision tree. The leaf node number is computed, and then a Laplace noise perturbation is added. The perturbed value is saved.

4) The training of all decision trees is completed to get the XGBoost algorithm that satisfies DP.

5) The test set is classified using the trained DP-XGBoost model.

4 Experimental Analysis

4.1 Experimental Setup

The experiments were executed on a 64-bit Windows 10 operating system powered by an Intel Core i5-9400F CPU, which is clocked at 2.90 GHz and equipped with 32 GB of memory. All algorithms were implemented using the Python programming language. The experimental dataset was sourced from the UCI database [19], as depicted in Table 1. Ten-fold cross-test was used, and the ultimate results were averaged.

Table 1: Experimental dataset

Dataset	Tuple	Number of Attributes	Number of Categories
Heart	270	13	2
Nursery	12960	8	5
Adult	32561	15	2

The mentioned datasets serve distinct purposes: the Heart dataset aims to ascertain whether a patient has a heart condition, the Nursery dataset aims to rank applications for childcare centers, and the Adult dataset is designed to predict whether an individual's annual salary exceeds 50K. All these datasets contain sensitive and private personal information that requires safeguarding.

In the DP-XGBoost algorithm, the maximum depth of the tree was taken as 5, regularization parameter λ was taken as 1, and γ was taken as 0. To avoid too many samples being filtered, g_l^* was taken as 1, and δ was set as 0.1 when the first tree was sampled.

In the experiments, the C4.5 classification algorithm in decision tree [18] and the XGBoost algorithm without the addition of DP were employed as the baseline models to evaluate the accuracy loss of the DP-XGBoost algorithm. To assess the efficacy of the DP-XGBoost algorithm in striking a balance between privacy preservation and classification accuracy, it was compared with the following two methods:

1) DiffP-C4.5 [5]: It reduces waste of privacy budget by utilizing the exponential mechanism, while building upon C4.5;

2) DP-random forest (RF) [4]: This method perturbs node class statistics to ensure DP protection.

4.2 Results Analysis

First of all, the accuracy of different algorithms for different datasets under different ϵ values is shown in Figures 1 $\sim$ 3.

According to Figures 1 $\sim$ 3, the classification accuracies of both C4.5 and XGBoost algorithms exhibited some degradation on large datasets, with the highest accuracies observed on the Heart dataset and the lowest on

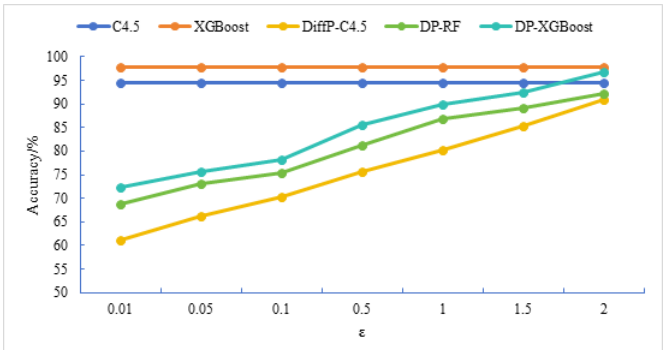


Figure 1: Accuracy for the Heart dataset under different ϵ values

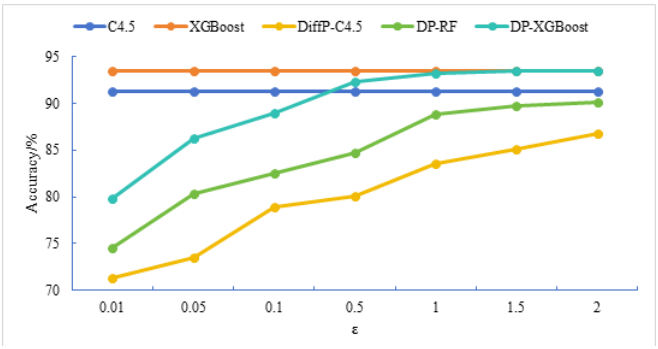


Figure 2: Accuracy for the Nursery dataset under different ϵ values

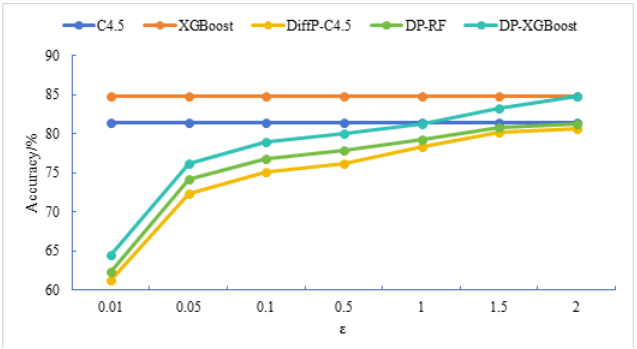


Figure 3: Accuracy for the Adult dataset under different ϵ values

the Adult dataset. This result suggested that the performance of data classification could be influenced by the size of the dataset.

Upon comparing the classification algorithms, it is evident that the XGBoost algorithm had a higher classification accuracy than the C4.5 algorithmm suggesting that it outperformed the C4.5 algorithm in terms of data classification. After the introduction of privacy budget, the accuracy of the algorithm increased as the ϵ value became larger. This is attributed to the fact that when the ϵ value was small, the protection of sensitive personal information and privacy data was robust, resulting in decreased data availability and subsequently lower accuracy in categorization.

In comparison to the DiffP-C4.5 and DP-RF algorithms, the DP-XGBoost algorithm consistently exhibited higher accuracy at equivalent ϵ values. When the ϵ value was small, the introduction of substantial noise caused a decline in accuracy. However, as the ϵ value increased, the results of the algorithm gradually approached those of both C4.5 and XGBoost algorithms. This outcome suggested that, compared to the other methods, the DP-XGBoost algorithm performed better in balancing privacy protection and classification accuracy. It effectively safeguarded personal sensitive information and privacy data in the dataset while ensuring the algorithm's accuracy in accomplishing classification tasks, thereby better addressing practical needs.

When the ϵ value was fixed at 1, the Adult dataset was used as a case to examine the effect of the maximum depth of the tree on the DP-XGBoost algorithm and to compare the accuracy loss of the DP-XGBoost algorithm with respect to the XGBoost algorithm. Table 2 presents the specific results.

Table 2: Effect of maximum depth of tree on accuracy (unit: %)

	XGBoost	DP-XGBoost	Accuracy loss
1	75.64	75.32	0.32
3	82.33	79.64	2.69
5	84.87	81.27	3.60
7	85.62	82.16	3.73
9	82.17	78.33	3.84
11	79.62	75.33	4.29

According to Table 2, when the maximum depth of the tree was set to 7, the XGBoost achieved a maximum accuracy of 85.62%, and the DP-XGBoost algorithm reached 82.16%. As the maximum depth of the tree increased to 11, the accuracies of the XGBoost and DP-XGBoost algorithms decreased to 79.62% and 75.33%, respectively. This may be because a tree with a shallow maximum depth would result in insufficient training, while a tree with an excessively large maximum depth would introduce excessive noise and lead to overfitting.

Comparing the XGBoost algorithm with the DP-XGBoost algorithm, it was found that as the maximum depth of the tree increased, the accuracy loss due to adding DP also increased, and the impact of noise interference on data accuracy became more significant. However, the overall accuracy loss caused by the addition of DP remained below 5%. This result demonstrated the reliability of the DP-XGBoost algorithm, making it suitable for practical applications in protecting personal sensitive information and privacy data, thereby addressing the limitations of the existing legal system.

5 Conclusion

This paper introduces the DP-XGBoost algorithm as a solution for safeguarding personal sensitive information and privacy data on the Internet, addressing gaps in the current legal system. The proposed algorithm not only performs data classification tasks but also employs DP to protect personal sensitive information and privacy data. Experimental results on the datasets demonstrate the reliability of the method, with an accuracy loss of within 5%. Moreover, the algorithm achieves high classification accuracy under different privacy budgets, making it a promising candidate for practical applications.

References

[1] C. Boura, N. Gama, M. Georgieva, D. Jetchev, "CHIMERA: Combining ring-LWE-based fully homomorphic encryption schemes," *Journal of Mathematical Cryptology*, vol. 14, no. 1, pp. 316-338, 2020.

[2] B. A. Dawood, F. Al-Turjman, A. A. Hussain, B. D. Deebak, "Chapter 9-Data protection and privacy preservation mechanisms for applications of IoT in smart grids using AI," *Sustainable Networks in Smart Grid*, pp. 207-231, 2022.

[3] B. Fabian, "Differential privacy and noisy confidentiality concepts for european population statistics," *Journal of Survey Statistics and Methodology*, vol. 10, no. 3, pp. 642-687, 2021.

[4] S. Fletcher, M. Z. Islam, "A differentially private random decision forest using reliable signal-to-noise ratios," in *Australasian Joint Conference on Artificial Intelligence*, pp. 192-203, 2015.

[5] A. Friedman, A. Schuster, "Data mining with differential privacy," in *Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 493-502, 2010.

[6] G. Georgiadis, G. Poels, "Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review," *Computer Law & Security Review: the International Journal of Technology Law and Practice*, vol. 44, no. 11, pp. 105640, 2022.

[7] R. Handa, C. R. Krishna, N. Aggarwal, "Searchable encryption: A survey on privacy-preserving search schemes on encrypted outsourced data," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 17, pp. e5201.1-e5201.49, 2019.

[8] Y. Huang, G. Yang, Y. Xu, H. Zhou, "Differential privacy principal component analysis for support vector machines," *Security and Communication Networks*, vol. 2021, pp. 5542283:1-5542283:12, 2021.

[9] S. T. Ikram, A. K. Cherukuri, B. Poorva, P. S. Ushasree, Y. Zhang, X. Liu, G. Li, "Anomaly detection using XGBoost ensemble of deep neural network models," *Cybernetics and Information Technologies: CIT*, vol. 21, no. 3, pp. 175-188, 2021.

[10] K. Kita, Y. Koizumi, T. Hasegawa, "Private retrieval of location-related content using K -anonymity and application to ICN," *Computer Networks*, vol. 209, no. 2, pp. 108908-, 2022.

[11] D. J. Kornbeck, "Data protection around the world: Privacy laws in action," *Journal of Data Protection & Privacy*, vol. 5, no. 1, pp. 97-99, 2021.

[12] S. Krishnan, P. Magalingam, R. Ibrahim, "Hybrid deep learning model using recurrent neural network and gated recurrent unit for heart disease prediction," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 6, pp. 5467-5476, 2021.

[13] X. Li, H. Li, H. Zhu, M. Huang, "The optimal upper bound of the number of queries for Laplace mechanism under differential privacy," *Information Sciences*, vol. 503, pp. 219-237, 2019.

[14] N. Martindale, S. L. Stewart, N. A. McGirl, M. B. Adams, G. Westphal, J. R. Garner, "Enabling computation on sensitive data in international safeguards with privacy-preserving encryption techniques," *Journal of Nuclear Materials Management*, vol. 49, no. 2, pp. 16-25, 2021.

[15] S. K. Pasupuleti, D. Varma, "Chapter 5-Lightweight ciphertext-policy attribute-based encryption scheme for data privacy and security in cloud-assisted IoT," *Real-Time Data Analytics for Large Scale Sensor Data*, Academic Press, pp. 97-114, 2020.

[16] E. F. Ramadhani, A. A. R. Fernandes, N. W. S. Wardhani, "Comparison of discriminant analysis and adaptive boosting classification and regression trees on data with unbalanced class," *WSEAS Transactions on Mathematics*, vol. 20, pp. 650-656, 2021.

[17] C. Regueiro, I. Seco, S. de Diego, O. Lage, L. Etxebarria, "Privacy-enhancing distributed protocol for data aggregation based on blockchain and homomorphic encryption," *Information Processing & Management*, vol. 58, no. 6, pp. 1-17, 2021.

[18] V. Sandeep, S. Kondappan, A. A. Jone, B. S. Raj, "Anomaly intrusion detection using SVM and C4.5 classification with an improved particle swarm optimization (I-PSO)," *International Journal of Information Security and Privacy*, vol. 15, no. 2, pp. 113-130, 2021.

[19] UC Irvine Machine Learning Repository, *Browse Datasets*, Feb. 21, 2024. (`http://archive.ics.uci.edu/datasets`)

[20] D. Vashi, H. B. Bhadka, K. Patel, S. Garg, "An efficient hybrid approach of attribute based encryption for privacy preserving through horizontally partitioned data," *Procedia Computer Science*, vol. 167, pp. 2437-2444, 2020.

[21] S. B. Zhang, L. J. Yuan, X. J. Mao, G. M. Zhu, "Privacy protection method for K-modes clustering data with local differential privacy," *Acta Electronica Sinica*, vol. 50, no. 9, pp. 2181-2188, 2022.

Biography

Xiaodan Li is a teacher working on the Law Teaching and Research Department of the Qingdao Party School of CPC, China. She graduated from China University of Political Science and Law with a doctorate in Criminal Law. Her research interests include criminal law and criminal psychology.

An Erasure Code with Low Repair-Cost Based on A Combined-stripe Encoding Structure

Minjun Sun[1,2], Dan Tang[1,2], Yue Li[1,2], Xie Wang[1,3], Hongliang Cai[1,2], and Qiong Zeng[1,2]
(Corresponding author: Dan Tang)

School of Software Engineering, Chengdu University of Information Technology[1]
Sichuan Province Engineering Technology Research Center of Support Software of Informatization Application[2]
Key Laboratory of Sichuan University for Aviation Manufacturing and Ground Command Software[3]
Chengdu 610225, China
Email: tangdan@foxmail.com

(Received July 27, 2023; Revised and Accepted Jan. 11, 2024; First Online Feb. 23, 2024)

Abstract

As a commonly used data redundancy strategy, erasure codes can effectively improve storage efficiency. However, the more network bandwidth consumed during repair, the more it limits its practical application in distributed storage systems. To solve the problem of high repair costs of erasure codes, this paper proposes an erasure code-named combined-stripe local reconstruction codes (CSLRC). CSLRC generates local parity blocks for redundancy protection by adding appropriate redundancy and using combined-stripe coding. CSLRC can flexibly configure coding parameters to balance storage overhead and repair costs better. Experimental results show that CSLRC can significantly reduce the amount of data to be read and transmitted during the repair process while maintaining high fault tolerance, saving network bandwidth and I/O resources, and effectively shortening repair time compared with other erasure codes.

Keywords: Distributed Storage System; Erasure Codes; Local Reconstruction Code; Low Repair-cost; Node Repair

1 Introduction

In order to meet the demand for reliable storage of huge amounts of data, distributed storage systems usually perform data redundancy to prevent data loss or data unavailability in case of node failure. A simple data redundancy strategy is replication, i.e., multiple copies of data are placed on different nodes, and data availability can be ensured as long as one copy is available. However, when the system size is large, replication will consume a lot of additional storage resources. Therefore, enterprises and researchers are gradually focusing on erasure codes [23].

Among all the erasure codes, the most representative one is Reed-Solomon (RS) codes [3]. RS codes are maximum distance separable (MDS) codes [21], whose minimum code distance reaches Singleton bounds. This optimally balances fault tolerance and storage overhead and is favored by many storage systems [9]. However, RS codes are far more expensive to repair than multicopy techniques. Repairing a failed block of (n, k)RS code requires reading and transmitting k blocks from the surviving nodes, which consumes a lot of network bandwidth and I/O resources. A recent study of the Facebook data warehouse cluster [14] showed that RS codes need to consume 180 TB of network bandwidth per day for recovering data from 50 failed machines. Although erasure codes can effectively improve storage efficiency, excessive repair cost has become one of the key issues that hinders its practical application in storage systems.

To address the repair performance bottleneck of erasure codes, some scholars constructed block codes [18] by adding appropriate storage overhead to optimize repair performance. LRC (local reconstruction codes) [6] deployed in Microsoft's WAS storage system is a typical scheme in block codes. LRC divides the original data block into multiple groups, and the groups are internally protected by generating local parity blocks for fault tolerance. The increased local parity blocks are utilized to reduce the repair cost of single node failures. In addition, LRCs proposed by Sathiamoorthy *et al.* [16], UFP-LRC (the unequal failure protection based local reconstruction code) proposed by Hu *et al.* [4], and RGRC (rotation group repairable codes) proposed by Zhang *et al.* [22] are suitable for single node failures. However, these erasure codes generally suffer from the same repair problem as MDS codes when they fail at multiple nodes. In real storage systems, concurrent failures cannot be avoided, and multi-node failure repair is not uncommon [10]. Pyramid codes proposed by Huang *et al.* [5] are applicable to the case of multi-node failure, and with more levels of grouping, the cost of repairing multi-node failure can be further reduced. However, it will increase more storage overhead,

so Pyramid codes cannot effectively balance storage overhead and repair cost. The GRC (group repairable codes) proposed by Lin *et al.* [10] adds redundancy protection for global parity blocks based on the coding structure idea of Basic-Pyramid codes. This can reduce the high repair overhead caused by the failure of a single global parity block. However, when a data node fails, its repair performance is not improved compared to Pyramid codes. In addition, Meng *et al.* [12] proposed DLRC (dynamic local reconstruction code) based on the idea of block codes. DLRC solves the problem of poor dynamic adjustment ability of the parameters of erasure codes. However, to meet multi-node fault tolerance, the cost of repairing a single node is too large.

In summary, the existing proposed erasure codes have some deficiencies in trade-off between storage overhead and repair cost and cannot satisfy users' demand for fast repair of failed nodes while optimizing repair performance in both single-node and multi-node failure cases. Most of the existing research work only focuses on reducing the repair cost of single-node failure but is not ideal for optimizing repair performance of multi-node failure, and the repair cost of multi-node failure is still too high. To address this problem, this paper proposes combined-stripe local reconstruction codes (CSLRC), which adopts combined-stripe coding to generate local parity blocks for redundancy protection. CSLRC has high repair performance in both single-node and multi-node failure cases and can flexibly configure each coding parameter while maintaining high fault tolerance. This can effectively trade-off storage overhead and repair cost. CSLRC reduces the amount of data required in the repair process, thus reducing network bandwidth and disk I/O resource consumption. It better meets data reliability requirements of distributed storage systems.

2 Related Work

Erasure codes are favored by distributed storage systems as an alternative fault-tolerance scheme to multicopy technology [1]. However, the more expensive repair cost in turn limits its application in storage systems. To reduce the repair cost of erasure codes, some scholars have improved the scheme by designing erasure codes with novel coding structures.

One of the classes is Regenerating Codes (RGC), which is designed based on the idea of network coding. RGC reduces the total amount of data downloaded during repair by preprocessing the data in the surviving nodes. However, the repair often needs to read a large amount of data, which can consume I/O resources greatly. Dimakis *et al.* [2] used information flow graph to compute the minimum cut-off boundary to obtain a lower bound curve for the repair bandwidth of a failed node. From the two extreme points on this curve, the researchers designed minimum storage regenerating (MSR) codes [15] and minimum storage regenerating (MBR) codes [11]. For the problem of large amount of read data during RGC repair, Rashmi *et al.* [13] proposed product-matrix-MSR (PM-MSR) codes to minimize I/O overhead. However, this scheme requires more than twice the storage overhead to optimize. Besides, some researchers have combined the coding methods of RGC and LRC to construct novel erasure codes to improve repair performance, such as Availability Zones Codes (AZ-Codes) [19] and Hybrid Regenerating Codes (Hybrid-RC) [20]. Although RGC can effectively reduce the amount of data transferred during repair, it fails to save I/O cost. Excessive I/O operations will affect overall I/O performance of the storage system. The vast majority of existing RGCs have high compilation code complexity and low code rate, so they are rarely implemented in real storage systems. The other type is block code [18], which is constructed by increasing redundancy to optimize repair performance, and its structure is simple, easier to implement, and more flexible. Block code usually groups the data blocks and utilizes the local parity blocks generated within the group for fault tolerance protection. This reduces the repair cost of node failures. However, the existing proposed block code [4, 6, 16, 22] cannot simultaneously satisfy the repair performance optimization problem in the case of single node failure and multi-node failure. Most current research focuses on reducing the repair cost of single-node failures [10], and there are fewer studies on optimizing the repair performance of multi-node failures.

Except for designing low repair cost erasure codes with novel coding structure from the erasure code itself, some improvement schemes predict disk failure or node failure through machine learning models and migrate and repair the blocks that will fail in advance to improve data reliability. Zhang *et al.* [24] proposed proactive LRC (pLRC), which utilizes node prediction techniques to distinguish the failure probability of different data blocks. This dynamically adjusts the group size of failed blocks in LRC to reduce the repair bandwidth of these blocks that will fail. Li *et al.* [8] proposed fast proactive repair (FastPR), which combines migration and repair, parallelizes the repair operation of the storage system, and effectively re-duces repair time. Song *et al.* [17] proposed local EC proactive recovery (LEC-PR). LEC-PR reduces inter-node traffic transmission by refining the failure level to the disk level based on FastPR and utilizing the bandwidth of each node for parallel recovery. Moreover, some researchers have proposed schemes to optimize the repair process to reduce the restoration time of unavailable data. Partial Parallel Repair (PPR), a partially parallel repair scheme proposed in literature [7], reduces network stress by splitting the repair process of a single block into multiple partial operations that can be performed in parallel. It schedules them to recover unavailable data blocks on multiple nodes that are already involved in data reconstruction. Literature [9] introduces the concept of repair pipelining by scheduling the repair of failed data in a finegrained manner on storage nodes in a pipelined fashion. This further improves the parallelism of repair and reduces the repair time of a

single failed block.

3 Important Concepts of Erasure Codecs

The data organization structure of (n, k) erasure code in distributed storage system is shown in Figure 1. The (n, k) erasure code divides the original data into k data blocks, i.e., D_1, D_2, ..., D_k, which are computed by the erasure code algorithm to produce n coded blocks, i.e., C_1, C_2, ..., C_n, which are stored on n different nodes. The set of all these n coded blocks independently associated with an erasure coding algorithm constitutes a stripe.

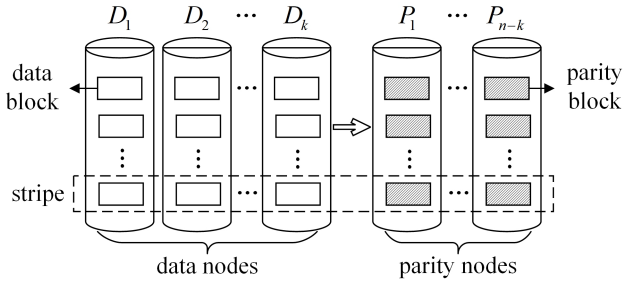


Figure 1: Data organization of (n, k) erasure code

The erasure code shown in Figure 1 is also called a systematic erasure code, which satisfies $D_i=C_i(0<i\leq k)$, and the rest of the coded blocks except the data block are called parity blocks, denoted as $P_i(1\leq i\leq n\text{-}k)$, $P_i=C_{k+i}(0<i\leq n\text{-}k)$. Unless otherwise specified, the erasure codes discussed in this paper refer to systematic erasure codes. When repairing a failed node, the process by which the erasure code obtains data from the available nodes to compute the failed coding blocks is called decoding or repairing. In order to facilitate the understanding, based on the literature [22], the concepts related to the data repair problem are given as follows:

- Fault Tolerance. The maximum number of arbitrary block failures that an erasure code can tolerate. Assuming that the fault tolerance of a erasure code is t, there exists a case where t+1 blocks fail, making the failed data unrepairable. Conversely, data is repairable when any number of blocks less than or equal to t fail.
- Global parity blocks. A parity block encoded from all data blocks in the stripe is a global parity block.
- Local parity block. The parity block generated by the computation of some of the encoded blocks (including data blocks and parity blocks) in the stripe is a local parity block.
- Storage overhead. The ratio of the amount of all coded data stored to the amount of original data. The storage overhead reflects the utilization of storage resources by the erasure code.
- Repair Cost. The amount of data that needs to be read to repair the failed data in a broken node. In a distributed storage system, repairing a failed node usually occupies network bandwidth and disk I/O resources, and the amount of data read and transmitted during the repair process will determine the performance of the storage system.
- Repair rate. For a given number of node failures, the ratio of all the failures that can be repaired to all the failures is the repair rate of the erasure code for a given number of node failures.

4 Encoding of CSLRC

The CSLRC proposed in this paper is a local reconstruction code constructed based on the systematic MDS code by using combined stripe encoding. The encoding structure of CSLRC is shown in Figure 2. The (10, 2, 3, 1) CSLRC divides the data block into several independent strips, and each stripe encodes the 10 data blocks D_1, D_2, ..., D_{10} according to the encoding algorithm of the (14, 10) MDS code to generate 4 global parity blocks P_1, P_2, ..., P_4. Then these 10 data blocks are equally divided into 2 groups, each group contains 5 data blocks, and at the same time each group is subdivided into front and back segments, the front segment contains 2 data blocks and the back segment contains 3 data blocks.

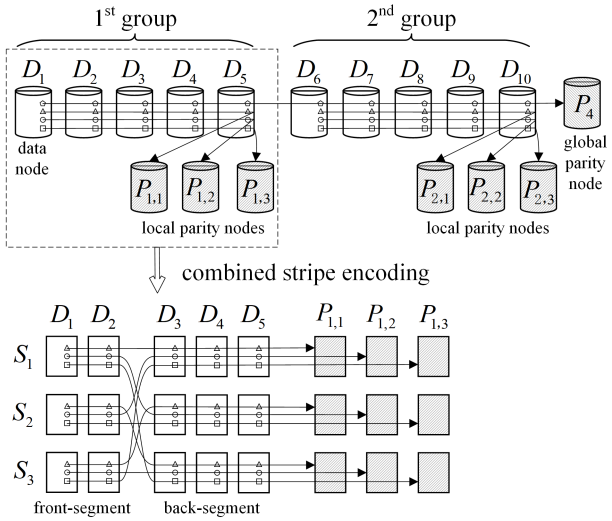


Figure 2: Combined-stripe encoding structure of (10,2,3,1) CSLRC

Keeping the last global parity block of the (14, 10) MDS code unchanged, 3 local parity blocks are computed for each group. The local parity blocks are $P_{1,1}$, $P_{1,2}$, $P_{1,3}$ in the first group and $P_{2,1}$, $P_{2,2}$, $P_{2,3}$ in the second

group. The 3 strips are then sequentially formed into a combined-stripe set, denoted S, S={$S_a|a$=1,2,3}. The j-th local parity block in the i-th ($0<i\leq l$) group of stripe $S_a(0<a\leq 3)$ in the stripe set S is encoded by the 3 data blocks in the back segment of the i-th group in stripe S_a and the 2 data blocks in the front segment of the i-th group in stripe $S_b(0<b\leq 3)$, which is encoded in the same way as the global parity block P_i of the (14, 10) MDS code, and the only thing needed is to set the other data blocks to zero, where j satisfies j=1+(x-1+y-1)mod3.

$$D\times G = D\times \begin{bmatrix} g_1 & g_2 & \cdots & g_n \end{bmatrix} = \begin{bmatrix} D_1 \\ D_2 \\ \cdots \\ D_k \end{bmatrix}^T \begin{bmatrix} g_{1,1} & \cdots & g_{1,1} \\ g_{2,1} & \cdots & g_{2,n} \\ \cdots & \cdots & \cdots \\ g_{k,1} & \cdots & g_{k,n} \end{bmatrix} = \begin{bmatrix} C_1 \\ C_2 \\ \cdots \\ C_n \end{bmatrix}^T \quad (1)$$

A formal description of CSLRC is given by the encoding structure of CSLRC. In general, CSLRC can be denoted by (k, l, m, r). Where k denotes the number of data blocks in the stripe, l denotes the number of groups in each stripe, m denotes the number of local parity blocks in each group as well as the number of strips in the combined-stripe coding, and r denotes the number of global parity blocks in the stripe. The specific coding procedure of CSLRC is as follows:

1) Given an (n, k) systematic MDS code which divides the original data into k fixed-size blocks as D_1, D_2, ..., D_k, the encoding generates q global parity blocks, where q=n-k, and each global parity block is linearly combined from these k data blocks. Specifically, as shown in Equation (1), the data matrix D=[D_1 ... D_k] corresponding to the data blocks is multiplied with the generating matrix G of the MDS code in the finite field $GF(2^w)$, and the encoding yields n coded blocks, i.e., C_1, C_2, ..., C_n. There are q global parity blocks in these n coded blocks, denoted as $P_i(0<i\leq q)$. Where $g_{i,j}(0<i\leq$k,$0<j\leq n)$ is an element in the finite field $GF(2^w)$ and D_i=$C_i(0<i\leq k)$, P_i=$C_{k+i}(0<i\leq q)$, the coding parameter n of the (n, k)MDS code satisfies $n\leq 2^w$+1.

2) Divide the data blocks in the stripe into l groups, denoted as $U_i(0<i\leq l)$, each containing e=k/l data blocks, and compute m local parity blocks for U_i. Constituting m strips into a combined-stripe set as S, S={$S_a|(0<a\leq m$}. Keep the encoding of the global parity block $P_z^a(m<z\leq q)$ in stripe $S_a(0<a\leq m)$ unchanged. The group in stripe S_a is denoted by $U_i^a(0<i\leq l)$, and the data blocks in group U_i^a are denoted as $D_x^a((i$-1)$e<x\leq ie)$. The data blocks in group U_i^a are subdivided into front and back segments, with the front segment containing f=$\lfloor e/2\rfloor$ data blocks and the back segment containing h=e-f data blocks. There are m local parity blocks in group $U_i^a(0<i\leq l)$, and each local parity block is encoded by h data blocks in the back segment of group U_i^a and f data blocks in the front segment of group U_i^b, denoted as $P_{i,z}^a(z$=1+(a-1+b-1)mod$m)$. $P_{i,z}^a$ is calculated in the same way as P_z^a, except that the other data blocks are set to zero.

The encoding formula for the parity block of the (k, l, m, r) CSLRC is obtained as:

$$P_z^a = \sum_{i=1}^{k} g_{i,k+z} D_i, 0<a\leq m, m<z\leq q. \quad (2)$$

$$P_{i,z}^a = \sum_{i=(i-1)\times e+1}^{(i-1)\times e+f} g_{x,k+j} D_x^b + \sum_{i=(i-1)\times e+f+1}^{i\times e} g_{y,k+j} D_y^a, \quad (3)$$
$$0<i\leq l, 0<a,b\leq m,$$
$$z=1+(a+b-2) \bmod m.$$

5 Decoding of CSLRC

When a node fails, (k, l, m, r) CSLRC cannot directly determine whether it is repairable by the number of failed blocks like (n, k) MDS codes. (k, l, m, r) CSLRC is repairable in some cases where more than n-k nodes fail, and in some cases it is not. Taking (10, 2, 3, 1) CSLRC with 5 missing data blocks within the stripe as an example, CSLRC can repair the failure situation shown in Figure 3, but cannot repair the failure situation shown in Figure 4. The shaded areas in Figures Figure 3 and Figure 4 represent the failed data nodes.

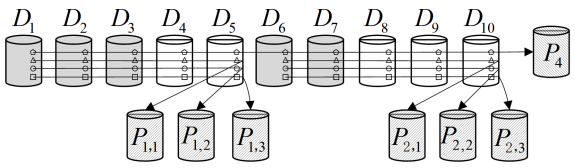


Figure 3: Repairable situation when (10,2,3,1) CSLRC fails 5 nodes

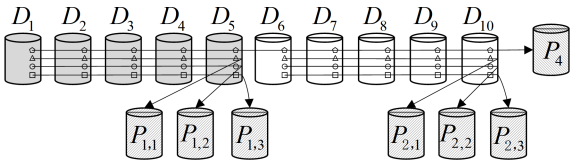


Figure 4: Unrepairable situation when (10,2,3,1) CSLRC fails 5 nodes

For the repairable failure case shown in Figure 3, the number of intra-group failed blocks of groups U_1 and U_2 does not exceed their intra-group fault tolerance, and CSLRC can recover the failed blocks by intra-group decoding. In the failure case shown in Figure 3, the number

of failed blocks in the group U_1 exceeds its fault tolerance. It should be repaired by decoding at the global level, however, the failure exceeds the fault tolerance of (14, 10) MDS codes, so it cannot be repaired.

Algorithm 1 Decoding algorithm of CSLRC

Input: $failure\_loc[]$: Array of locations of failed blocks in the stripe, $read\_loc[]$: Array of locations of blocks to be read in the stripe, $read\_buf[]$: Cache array of data to be read.

Output: $repair\_buf[]$: Cache array of repaired data.

```
Begin
Initialize failure_loc[], read_loc[], read_buf[].
if failure_loc[].length > 0 then
    Update gps_failureLoc[][]; //Update the location of the failed blocks in each group.
    for i = 0 to l do
        gp_failureNum=gps_failureLoc[i].length; //Get the number of failed blocks in the i-th group.
        if gp_failureNum == 0 then
            continue;
        end if
        if gp_failureNum > 0 and gp_failureNum < m+1 then
            cs_groupDecode(); //Intra-group decoding of combined stripe set.
            Result stored in repair_buf[];
            Update failure_loc[];
            continue;
        end if
        //Global decoding of combined stripe set.
        if gp_failureNum > m and cs_globalDecode() == TRUE then
            Result stored in repair_buf[];
            Update failure_loc[];
            continue;
        end if
        break;
    end for
end if
if failure_loc[].length == 0 then
    return TRUE;
end if
if i == l and cs_globalDecode() == TRUE then
    Result stored in repair_buf[];
    return TRUE;
end if
return FALSE;
End
```

There are different failure modes for node failure, for different failure modes this paper proposes a CSLRC decoding algorithm based on greedy strategy. The CSLRC decoding algorithm is mainly divided into two parts (See Algorithm 1: intra-group decoding of combined-stripe set and global decoding of combined-stripe set, the details are as follows:

1) Intra-group decoding of combined-stripe set. For each group in $S=\{S_a|a=1,2,...,m\}$, assume that the number of intra-group failed blocks in group $U_i^a(0 < i \leq l)$ is F. When F≤m, i.e., the number of intra-group failed blocks is not more than the number of intra-group local parity blocks, it is judged to be repairable intra-group. If all the F failed blocks in the strip S_a are front segment data blocks, they are repaired by the calculation of the set of parity equations corresponding to $\{P_{i,z}^a|0<b\leq F, z=1+(b+a\text{-}2)\bmod m\}$ and if they are all back segment data blocks, they are repaired by the calculation of the set of parity equations corresponding to $\{P_{i,z}^b|0<a\leq F, z=1+(a+b\text{-}2)\bmod m\}$, and the above decoding process is repeated until all the failed blocks in S are repaired. For all other cases, the $F\times m$ failed blocks in S are repaired by the calculation of the set of parity equations corresponding to $\{P_{i,z}^a|0<z\leq F, 0<a\leq m\}$.

2) Global decoding of combined-stripe set. Given $i(0<a\leq l)$, if all intra-group local parity blocks $P_{i,z}$ in the stripe are available, the corresponding global parity block P_z is marked as available. At the global level, the judgment is repairable if the number of failed blocks is not greater than the number of global parity blocks, i.e., $F\leq m+r$. Then the $F\times m$ failed blocks in S are recovered by calculating the corresponding set of parity equations from $\{P_z^a|0<z\leq F, 0<a\leq m\}$, where P_z^a denotes the global parity block in the stripe S_a.

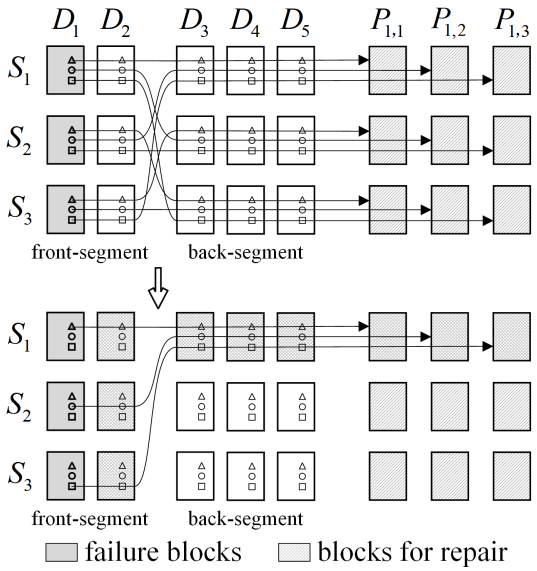


Figure 5: Decoding of single-node failure for (10,2,3,1) CSLRC

Next, the decoding process of (10,2,3,1) CSLRC is demonstrated by taking the failure of a single node as an example, as shown in Figure 5, where the shaded part

Table 1: Comparison of the performance of various erasure codes

Metrics	(n,k)RS code	(k,l,r)LRC	(n,k)Basic-Pyramid	(k,l,m,r)CSLRC
Average Repair Cost	k	$\frac{k^2/l+(r+1)k}{k+l+r}$	$\frac{k^2/l+(r+m)k}{k+ml+r}$	$\frac{k^2/l+(2/m-2)lhf+(m+r)k}{k+ml+r}$
Minimal repair cost	k	$\frac{k}{l}$	$\frac{k}{l}$	$\frac{k+(m-1)lf}{ml}$
Storage Overhead	$\frac{n}{k}$	$\frac{k+l+r}{k}$	$\frac{n}{k}$	$\frac{k+ml+r}{k}$
Fault Tolerance	n-k	$r+1$	$m+r$	$m+r$
Maximal Fault Tolerance	n-k	$r+l$	$ml+r$	$ml+r$

indicates the failed node D_1 and the failed data blocks in it. The (10,2,3,1) CSLRC is decoded in terms of the combined-stripe set S=$\{S_1,S_2,S_3\}$, and the failed block is the data block in the front segment of group $U_i^y(0<y\leq 3)$. The corresponding set of parity equations is constructed as:

$$E_1 = \begin{cases} g_{1,13}D_1^1 + \sum_{a=2}^{3} g_{a,13}D_a^1 + \sum_{b=4}^{6} g_{b,13}D_b^1 = P_{1,1}^1 \\ g_{1,14}D_1^2 + \sum_{a=2}^{3} g_{a,14}D_a^2 + \sum_{b=4}^{6} g_{b,14}D_b^1 = P_{1,2}^1 \\ g_{1,15}D_1^3 + \sum_{a=2}^{3} g_{a,15}D_a^3 + \sum_{b=4}^{6} g_{b,15}D_b^1 = P_{1,3}^1 \end{cases}$$

From the set of parity equations E_1, repairing the failed data block D_1^1 in stripe S_1 needs to read 5 coded blocks, i.e., $D_2^1, D_3^1, D_4^1, D_5^1, P_{1,1}^1$. And repairing the failed data block D_1^2 in stripe S_2 and the failed data block D_1^3 in stripe S_3 with repairing the data block D_1^1 duplicates the reading of data block D_3^1, D_4^1, D_5^1. And the duplicated data blocks need to be read only once, so repairing the failed data blocks D_1^2 and D_1^3 only need to read the 4 coded blocks $D_2^2, P_{1,2}^1, D_2^3, P_{1,3}^1$ again. Compared with the (14, 10) MDS code which needs to read 30 blocks to repair the failed data block D_1 in 3 strips, CSLRC only needs to read 9 blocks, which reduces the repair cost by 70%.

6 Theoretical Analysis

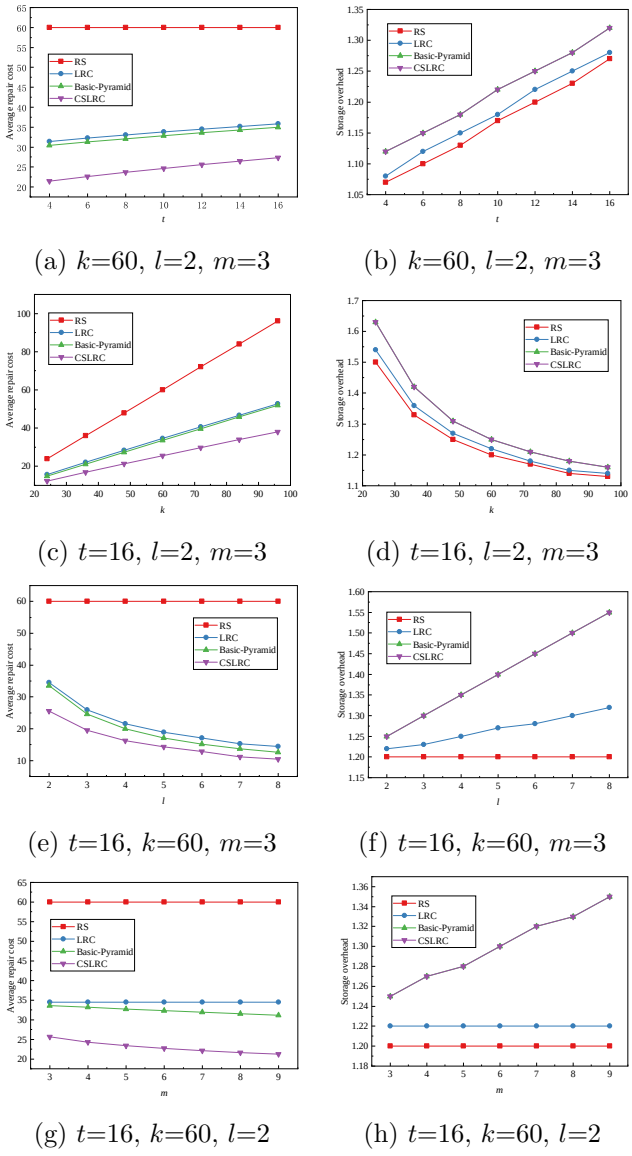
In this paper, we summarize the performance characteristics of CSLRC by quantitatively comparing it with RS codes [3], LRC [6], and Basic-Pyramid codes [5], based on the requirements of distributed storage systems on the three aspects of the erasure codes: fault tolerance, storage overhead, and repair cost. The performance metrics of these erasure codes are listed in Table 1. Where ARC represents the average repair cost of erasure codes, which is defined as the average number of blocks required to repair a single failed block under the assumption that all nodes or disks have the same probability of being repaired due to failure. In addition, MRC is defined as the minimal repair cost (MRC) of repairing a data block, i.e., the minimum number of blocks that need to be read to repair a data block.

From Table 1, it can be seen that under the premise of the same fault tolerance capability, CSLRC has the maximum fault tolerance number and therefore has better fault tolerance performance. In addition, CSLRC has all the advantages of Basic-Pyramid codes and has the lowest repair cost compared to RS codes, LRC, and Basic-Pyramid codes, thus it has better reliability and repair performance. In this paper, we verify the reliability and repair performance of CSLRC by analyzing the repair cost and storage overhead comparison of RS code, LRC, Basic-Pyramid codes and CSLRC under 4 different parameters, namely, fault tolerance t, number of data blocks k, number of groups l, and number of intra-group parity blocks m. The results of the comparison are shown in Figure 6.

Theoretically, CSLRC has the lowest ARC with different fault tolerance, while the storage overhead increases by a maximum of only 4.5%, as shown in Figure 6(a) and Figure 6(b). The ARCs of CSLRC, LRC, and Basic-Pyramid codes gradually increase with the increase of fault tolerance, while RS codes remain unchanged. Figure 6(d) shows that increasing the number of data blocks decreases the storage overhead of each erasure code. The maximum storage overhead increased by CSLRC compared to RS codes, LRC, and Basic-Pyramid codes decreases from 7.98% to 2.59%. The relative ARC then increases, where the ARC growth rate of CSLRC is smaller and remains lowest, as shown in Figure 6(c). Figure 6(e) and Figure 6(f) shows that CSLRC has the optimal repair performance given different numbers of groups, except for RS code. Increasing the number of groups can significantly reduce the ARC of each erasure code. However, it is at the cost of increasing more storage overhead, and the trend of decreasing the ARC of each erasure code decreases. Therefore, we cannot just increase the number of groups to reduce the cost of erasure code repair. As can be seen from Figure 6(g) and Figure 6(h), CSLRC with different numbers of intra-group parity blocks still has the lowest ARC, while the storage overhead increases by 11.1% at most. Increasing the number of intra-group parity blocks can effectively reduce the ARC of CSLRC.

In summary, given the same fault tolerance, CSLRC with different numbers of data blocks, numbers of groups, and numbers of parity blocks has the best repair performance and keeps lower storage overhead when compared to RS codes, LRC codes, and Basic-Pyramid codes. While

maintaining high fault tolerance performance, CSLRC can flexibly configure each coding parameter to better balance storage overhead and repair cost. Therefore, CSLRC can better meet the reliability requirements of distributed storage systems.



(a) k=60, l=2, m=3 (b) k=60, l=2, m=3

(c) t=16, l=2, m=3 (d) t=16, l=2, m=3

(e) t=16, k=60, m=3 (f) t=16, k=60, m=3

(g) t=16, k=60, l=2 (h) t=16, k=60, l=2

Figure 6: Comparison of repair cost and storage overhead of various erasure codes

7 Experiment and Discussion

The author conducted experiments on the erasure code test platform based on the distributed storage system Ceph in this section. The repair performance of CSLRC in the distributed storage system was evaluated by testing CSLRC in many aspects and comparing and analyzing it with common erasure codes.

7.1 Experimental Environment and Parameters

The erasure code test platform used in the experiment uses Ceph v13.2.3 to build a distributed storage system, and the test platform contains 25 nodes. Except for one client and three monitor nodes, the remaining nodes are used as OSD (Object Storage Device) storage nodes. The architecture of erasure code test platform is shown in Figure 7. The platform implements RS code [3], LRC [6], Basic-Pyramid code [5], UFP-LRC [4], DLRC [12], and CSLRC through Java SE 8 and integrates them as plug-ins in the platform system. Each node was configured with an Intel Core i7 processor, 8 GB of RAM, and 500 GB of disk, and a CentOS 7 system and JDK1.8.0_301 were installed for all nodes.

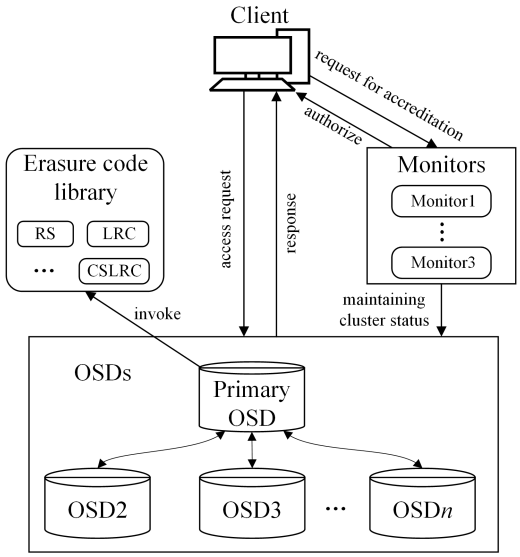


Figure 7: Overview of erasure code test platform architecture

Experimental comparison of (10, 2, 3, 1) CSLRC, (14, 10) RS code, (16, 10) Basic-Pyramid code, (10, 2, 3) LRC, (4+6, 2, 3) UFP-LRC and (10, 2, 6, 4) DLRC with fault tolerance equal to 4. The coding parameters of each erasure code are shown in Table 2, where l denotes the number of groups, m denotes the number of intra-group parity blocks, and r denotes the number of global parity blocks. The number of data blocks in the 2 groups of (4+6, 2, 3) UFP-LRC is not balanced, the 1st group contains 4 data blocks and the 2nd group contains 6 data blocks. (10, 2, 6, 4) DLRC initially divides the original data blocks into two groups, puts a global parity block at the end of each initial group, and then divides these 12 coded blocks into 4 groups overlapping each other, each group containing 6 coded blocks.

Table 2: The values of various encoding parameters for the erasure code used in the test

Coding scheme	l	m	r
(10, 2, 3)LRC	2	1	3
(16, 10)Basic-Pyramid	2	2	2
(4+6, 2, 3)UFP-LRC	2	1	3
(10, 2, 6, 4)DLRC	4	1	2
(10, 2, 3, 1)CSLRC	2	3	1

7.2 Experimental Comparison Index

The experiment will use the repair rate, repair cost, repair time, and storage utilization as comparison indices. The repair rate is one of the most important indicators to measure the performance of erasure codes. The repair rate at different numbers of failed nodes comprehensively reflects the fault tolerance performance of erasure codes. Repair cost is the amount of data read during the repair process, and it reflects the occupation of network bandwidth and disk I/O resources by the repair operation of erasure codes. Repair time measures the real-time capability of erasure codes repairing failed data, and the speed of the repair process will affect the access performance of the system. Storage utilization is the ratio of the original data volume to the volume of all coded data stored, and it reflects the occupation of storage resources by erasure codes. Based on these comparison indices and according to two cases of single-node repair and multi-node repair, we will conduct our experiment.

7.3 Result and Discussion

7.3.1 Repair Rate

The repair rate comparison experiment is designed to randomly generate x failed nodes multiple times and record the repair rate when each erasure code fails x nodes. The repair rate comparison of each erasure code is given in Figure 8.

All erasure codes can completely repair the failed data when the number of failed nodes does not exceed 4. When the number of failed nodes reaches 5, the data of (14, 10) RS code is lost. When the number of failed nodes reaches 6, the data of (10, 2, 3) LRC is lost. When the number of failed nodes reaches 7, the data of (10, 2, 6, 4) DLRC is lost. Only the data of (10, 2, 3, 1) CSLRC tolerates 7 node failures at higher probability. CSLRC consumes almost the same amount of storage space compared to Basic-Pyramid codes and DLRC but has better fault tolerance performance than both. Taken together, given the same fault tolerance, (10, 2, 3, 1) CSLRC tolerates more node failures than (14, 10) RS code, (16, 10) Basic-Pyramid code, (10, 2, 3) LRC, (4+6, 2, 3) UFP-LRC and (10, 2, 6, 4) DLRC and has higher fault-tolerant performance.

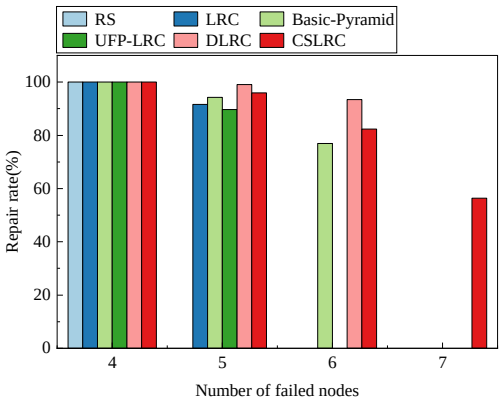


Figure 8: Comparison of repair rate

7.3.2 Single-node Repair Performance

Upload test files with sizes ranging from 15MB to 120MB in increasing order to the erasure codes test platform. The default block size is 64KB. A single failed node is randomly generated to simulate a single node failure in the storage system, and the erasure codes test platform records the amount of data read and the repair time when each erasure codes repairs a single failed node.

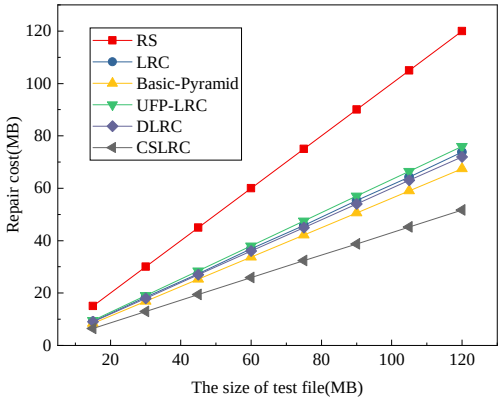


Figure 9: Comparison of average repair cost of various erasure codes with single-node failure

Figure 9 shows the comparison of the average repair cost of each erasure code at single node failure. As can be seen from Figure 9, the repair cost of (10, 2, 3, 1)CSLRC is reduced by about 56.9% compared to (16, 10)RS code, about 23.4% compared to (16, 10)Basic-Pyramid, about 29.3% compared to (10, 2, 3)LRC, about 31.9% compared to (4+6, 2, 3)UFP-LRC, and about 28.2% compared to (10, 2, 6, 4)DLRC, when a single node fails. CSLRC uses intra-group decoding of combined-stripe set, which can effectively reduce the repair cost of a single failed data node.

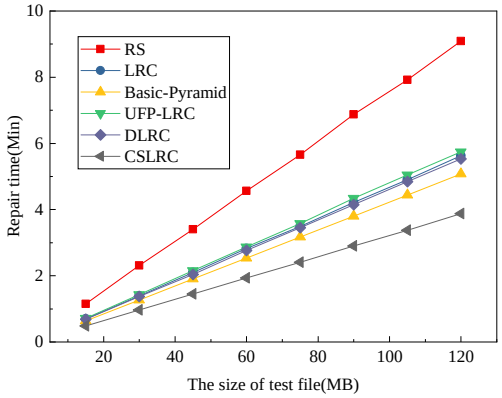


Figure 10: Comparison of average repair time of various erasure codes with single-node failure

Figure 10 shows the comparison of the average repair time of each erasure code at single node failure. From Figure 10, it can be seen that the repair time of (10, 2, 3, 1) CSLRC is shortened by about 57.6% compared to (14, 10) RS code, about 24.3% compared to (16, 10) Basic-Pyramid, about 30.9% compared to (10, 2, 3) LRC, about 32.8% compared to (4+6, 2, 3) UFP-LRC, and about 29.4% compared to (10, 2, 6, 4) DLRC, when a single node fails. CSLRC is decoded in units of combined-stripe sets, which can further reduce the repair time for single node failures.

From the experimental comparison results, it can be concluded that CSLRC has lower repair cost, saves more network bandwidth and disk I/O resources, has shorter repair duration, avoids high repair latency, and effectively improves data availability and storage system reliability compared to other erasure codes in case of single node failure.

7.3.3 Multi-node Repair Performance

The experiment is designed to simulate the case of multiple node failures in a storage system by randomly generating x failed nodes with x increasing in order. The amount of data read and the repair time when x failed nodes are repaired by each erasure code is recorded according to the erasure code test platform. The test file size is 60MB and the block size is 64KB by default. The maximum number of failed nodes in the experimental design is 4. In this section, multi-node failure refers to the failure of 2 4 nodes.

Figure 11 represents the comparison of the average repair cost of each erasure code at multi-node failure. From Figure 11, it is observed that the repair cost of (10, 2, 3, 1) CSLRC is decreased by 8.6%-38.9% compared to (14, 10) RS code, by 8.6%-26.7% compared to (16, 10) Basic-Pyramid, by 8.6%-38.9% compared to (10, 2, 3) LRC, by 8.6%-38.9% compared to (4+6, 2, 3) UFP-LRC, by 16.9%-35.7% compared to (10, 2, 6, 4) DLRC. LRC and UFP-LRC can only be repaired by repairing at the global level when multiple nodes fail within a group, and thus have a higher repair cost. CSLRC prioritizes the use of intra-group decoding in the complex stripe set when the number of failed blocks within a group does not exceed the fault-tolerance capacity, which ensures that the amount of data to be read for repairing a failed block in the combined-stripe set is minimized, and thus has a lower repair cost.

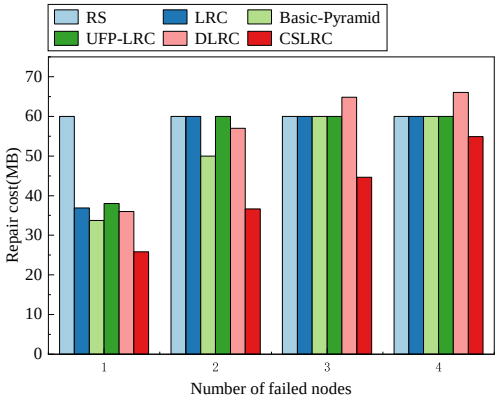


Figure 11: Comparison of average repair cost of various erasure codes with multi-node failure

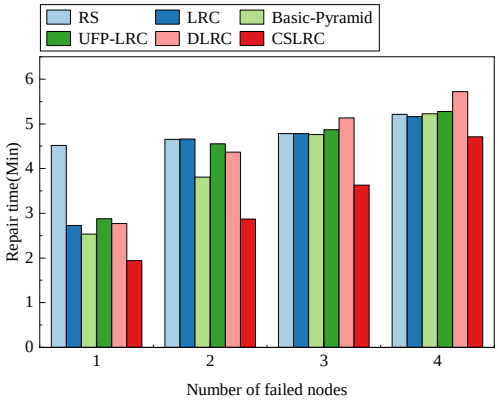


Figure 12: Comparison of average repair time of various erasure codes with multi-node failure

The average repair time comparison of each erasure code in case of multi-node failure is shown in Figure 12. According to Figure 12, the repair time of (10, 2, 3, 1) CSLRC is shortened by 9.7%-38.3% compared to (14, 10) RS code, by 9.8%-24.7% compared to (16, 10) Basic-Pyramid, by 8.8%-38.4% compared to (10, 2, 3) LRC, by 10.6%-37% compared to (4+6, 2, 3) UFP-LRC, by 17.6%-34.2% compared to (10, 2, 6, 4) DLRC. CSLRC prioritizes the use of intra-group decoding of combined-stripe set, which makes it possible to read and transmit

less data when repairing the failed data, effectively shortening the repair time.

The experimental results indicate that CSLRC also has better repair performance in the case of multi-node failure, with the increase of the number of failed nodes, the repair cost of each erasure code is gradually increasing, and the low repair cost advantage of CSLRC in the single-node repair is gradually weakened, but compared with other corrective censoring codes, it still has a lower repair cost, and the corresponding repair time is also shorter.

7.3.4 Storage Utilization

The storage utilization comparison experiment is designed to upload the test file of size 60MB to the erasure codes test platform, and record the actual storage space occupied by the coded file stored by each erasure codes, and finally calculate the storage utilization of each erasure code according to the result data, and the comparison results are shown in Figure 13. It is clear from Figure 13 that the storage efficiency of (10, 2, 3, 1) CSLRC is reduced by about 17.7% compared to (14, 10) RS code, about 11.8% compared to (10, 2, 3) LRC and (4+6, 2, 3) UFP-LRC, about 5.9% compared to (19, 12) Basic-Pyramid and (10, 2, 6, 4) DLRC. Although the storage utilization of CSLRC is reduced compared to other erasure codes, it is still within an acceptable range compared to its reduced repair cost and repair time.

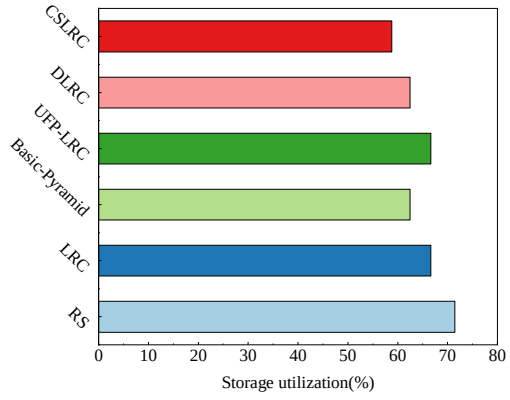


Figure 13: Comparison of storage utilization

8 Conclusions

This paper proposes CSLRC to address the problem of erasure codes needing to read and transmit a large amount of data when repairing. CSLRC groups the strips, constitutes multiple strips into a combined-stripe set, and generates local parity blocks for redundancy protection by employing combined-stripe coding for each group in the stripe set. This provides better repair performance in case of node failure. The experimental results demonstrate that compared with RS code, Basic-Pyramid code, LRC, UFP-LRC, and DLRC, CSLRC decreases the single-node repair cost by 23.4% to 56.9% and the repair time by 24.3% to 57.6%. It also decreases the multi-node repair cost by 8.6% to 38.9% and the repair time by 8.8% to 38.4%. In addition, CSLRC has high fault tolerance performance and can flexibly configure each encoding parameter to better balance storage overhead and repair cost. Therefore, CSLRC has more advantages in meeting the data reliability requirements of distributed storage systems.

Acknowledgments

This work is partially supported by Key R & D projects of Si-chuan Science and Technology Department (2022YFG0037).

References

[1] H. Dau, I. M. Duursma, H. M. Kiah, and O. Milenkovic, "Repairing reed-solomon codes with multiple erasures," *IEEE TRANSACTIONS ON INFORMATION THEORY*, vol. 64, no. 10, pp. 6567–6582, 2018.

[2] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4539–4551, 2010.

[3] Y. Hu, L. Cheng, Q. Yao, P. P. Lee, W. Wang, and W. Chen, "Exploiting combined locality for wide-stripe erasure coding in distributed storage," in *Proceedings of the 19th USENIX Conference on File and Storage Technologies, FAST 2021*, Virtual, Online, pp. 233–248, 2021.

[4] Y. Hu, Y. Liu, W. Li, K. Li, K. Li, N. Xiao, and Z. Qin, "Unequal failure protection coding technique for distributed cloud storage systems," *IEEE Transactions on Cloud Computing*, vol. 9, no. 1, pp. 386–400, 2021.

[5] C. Huang, M. Chen, and J. Li, "Pyramid codes: Flexible schemes to trade space for access efficiency in reliable data storage systems," *ACM Transactions on Storage*, vol. 9, no. 1, pp. 1–28, 2013.

[6] C. Huang, H. Simitci, Y. Xu, A. Ogus, B. Calder, P. Gopalan, J. Li, and S. Yekhanin, "Erasure coding in windows azure storage," in *Proceedings of the 2012 USENIX Annual Technical Conference, USENIX ATC 2012*, Boston, MA, United states, pp. 15–26, 2012.

[7] R. Li, X. Li, P. P. Lee, and Q. Huang, "Repair pipelining for erasure-coded storage," in *Proceedings of the 2017 USENIX Annual Technical Conference, USENIX ATC 2017*, Santa Clara, CA, United states, pp. 567–579, 2019.

[8] X. Li, K. Cheng, Z. Shen, and P. P. C. Lee, "Fast proactive repair in erasure-coded storage: Analysis,

design, and implementation," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 12, pp. 3400 –3414, 2022.

[9] X. Li, Z. Yang, J. Li, R. Li, P. P. C. Lee, Q. Huang, and Y. Hu, "Repair pipelining for erasure-coded storage: Algorithms and evaluation," *ACM Transactions on Storage*, vol. 17, no. 2, JUN 2021.

[10] X. Lin, Y. Wang, X. Pei, and F. Xu, "Grc: A high fault-tolerance and low recovery-overhead erasure code for multiple losses," *Journal of Computer Research and Development*, vol. 51, no. 2, pp. 172–181, 2014.

[11] K. Mahdaviani, S. Mohajer, and A. Khisti, "Product matrix minimum storage regenerating codes with flexible number of helpers," in *IEEE International Symposium on Information Theory - Proceedings*, vol. 2018-January, Kaohsiung, Taiwan, pp. 41–45, 2017.

[12] Y. Meng, L. Zhang, D. Xu, Z. Guan, and L. Ren, "A dynamic erasure code based on block code," in *Proceedings of the 2019 International Conference on Embedded Wireless Systems and Networks, EWSN 2019, Beijing, China, February 25-27, 2019*, pp. 379–383, 2019.

[13] K. Rashmi, P. Nakkiran, J. Wang, N. B. Shah, and K. Ramchandran, "Having your cake and eating it too: Jointly optimal erasure codes for i/o, storage and network-bandwidth," in *Proceedings of the 13th USENIX Conference on File and Storage Technologies, FAST 2015*, Santa Clara, CA, United states, pp. 81–94, 2015.

[14] K. V. Rashmi, N. B. Shah, D. Gu, H. Kuang, D. Borthakur, and K. Ramchandran, "A "hitchhiker's" guide to fast and efficient data reconstruction in erasure-coded data centers," *ACM SIGCOMM COMPUTER COMMUNICATION REVIEW*, vol. 44, no. 4, pp. 331–342, 2014.

[15] K. V. Rashmi, N. B. Shah, and P. V. Kumar, "Optimal exact-regenerating codes for distributed storage at the msr and mbr points via a product-matrix construction," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 5227–5239, 2011.

[16] M. Sathiamoorthy, M. Asteris, D. Papailiopoulos, A. G. Dimakis, R. Vadali, S. Chen, and D. Borthakur, "Xoring elephants: Novel erasure codes for big data," *Proceedings of the VLDB Endowment*, vol. 6, no. 5, pp. 325–336, 2013.

[17] Y. Song, M. Yang, and B. Wang, "Lec-pr: Proactive recovery method in erasure-coded storage," in *Proceedings of IPDRM 2022: 5th Annual Workshop on Emerging Parallel and Distributed Runtime Systems and Middleware, Held in conjunction with SC 2022: The International Conference for High Performance Computing, Networking, Storage and Analysis*, Dallas, TX, United states, pp. 9–16, 2022.

[18] Y.-J. Wang, F.-L. Xu, and X.-Q. Pei, "Research on erasure code-based fault-tolerant technology for distributed storage," *Jisuanji Xuebao/Chinese Journal of Computers*, vol. 40, no. 1, pp. 236–255, 2017.

[19] X. Xie, C. Wu, J. Gu, H. Qiu, J. Li, M. Guo, X. He, Y. Dong, and Y. Zhao, "Az-code: An efficient availability zone level erasure code to provide high fault tolerance in cloud storage systems," in *IEEE Symposium on Mass Storage Systems and Technologies*, vol. 2019-May, Santa Clara, CA, United states, pp. 230–243, 2019.

[20] L. Ye, D. Feng, Y. Hu, and X. Wei, "Hybrid codes: Flexible erasure codes with optimized recovery performance," *ACM TRANSACTIONS ON STORAGE*, vol. 16, no. 4, pp. 1–26, 2020.

[21] Q. Yu, L. Wang, Y. Hu, Y. Xu, D. Feng, J. Fu, X. Zhu, Z. Yao, and W. Wei, "Boosting multi-block repair in cloud storage systems with wide-stripe erasure coding," in *IEEE International Parallel and Distributed Processing Symposium, IPDPS 2023, St. Petersburg, FL, USA, May 15-19, 2023*. IEEE, pp. 279–289, 2023.

[22] H. Zhang, S. Liu, D. Tang, and H. Cai, "Erasure code with low recovery-overhead in distributed storage systems," *Journal of Computer Applications*, vol. 40, no. 10, pp. 2942–2950, 2020.

[23] X. Zhang, N. Liang, Y. Liu, C. Zhang, and Y. Li, "Sa-rsr: a read-optimal data recovery strategy for xor-coded distributed storage systems," *Frontiers of Information Technology and Electronic Engineering*, vol. 23, no. 6, pp. 858–875, 2022.

[24] X. Zhang, J. Xu, and Y. Hu, "Proactive locally repairable codes for cloud storage systems," *Jisuanji Yanjiu yu Fazhan/Computer Research and Development*, vol. 56, no. 9, pp. 1988–2000, 2019.

Biography

Minjun Sun, born in 1998, M. S., candidate. His research interests include coding theory and distributed storage systems.

Dan Tang, born in 1982, Ph. D., professor. His research interests include coding theory and distributed storage systems.

Yue Li, born in 1997, M. S., candidate. Her research interests include Information hiding and digital watermarking.

Xie Wang, born in 1970, M. S., Associate professor. His research interests include Computer software and theory, big data analysis.

Hongliang Cai, born in 1983, Ph. D., Associate professor. His research inter-ests include coding theory and visual cryptography.

Qiong Zeng, born in 1976, M. S., Lecturer. Her research interests include data mining and systems development.

Network Security Situational Awareness of Enterprise Control Systems under Machine Learning

Hui You

(Corresponding author: Hui You)

Network Security Defense Department, Beijing Police College
Nanjian Road, Changping District, Beijing 102202, China
Email: yhui1984@outlook.com

(Received Dec. 29, 2022; Revised and Accepted Dec. 26, 2023; First Online Feb. 23, 2024)

Abstract

In the process of operation, enterprise control system networks face complex network attacks and require enhanced protection. This study investigated the method of network security situational awareness (NSSA) for enterprise control systems. XGBoost was used to implement situational assessment, and an improved bat algorithm (IBA) was designed to optimize the parameters of XGBoost to obtain the IBA-XGBoost situational assessment method. Bidirectional long short-term memory (BiLSTM) was applied for situational prediction, and an IBA was also used to optimize parameters to achieve the IBA-BiLSTM situational prediction method. Tests were conducted using the NSL-KDD dataset. It was observed that the IBA-XGBoost method outperformed other machine learning methods, such as the KNN algorithm, in situational assessment. The obtained situation values closely aligned with actual values, demonstrating root-mean-square error (RMSE) and mean absolute error (MAE) values as low as 0.051 and 0.016, respectively. Additionally, IBA-BiLSTM outperformed the other algorithms in situation prediction, achieving an RMSE of 0.028 and an MAE of 0.021. These results validate the effectiveness of the proposed situation evaluation and prediction methods, showcasing their applicability in real-world enterprise control systems.

Keywords: Enterprise Control Network; Machine Learning; Network Security Situational Awareness; XGBoost

1 Introduction

The enterprise control system enables the automated control of various equipment and software involved in the production processes of enterprises, widely utilized in industries such as aviation and electric energy. With the continuous advancement of intelligent technology, an increasing number of sensors and devices are integrated into enterprise control systems, making the system network more susceptible to threats such as viruses and hackers. Traditional protection methods for enterprise control system networks include firewalls [11], intrusion detection [1], etc. However, faced with the growing complexity and frequency of external attacks, these conventional approaches struggle to comprehensively control the system's security status.

In contrast to traditional methods, network security situational awareness (NSSA) [9] technology can extract effective features from vast amounts of data, providing a timely and effective reflection of the system's security status. This enhances the network defense capability of enterprise control systems. Machine learning methods find extensive applications in NSSA [21]. Yao *et al.* [20] designed a framework that combines multivariate heterogeneous data based on the attack behavior model and proved its feasibility through experiments. He *et al.* [8] designed a situation prediction method using the dual-feedback Elman model and found through experiments that only four samples did not match the actual outcomes. Pavol *et al.* [12] compared statistical and neural network models in NSSA, concluding that the neural network method was more accurate than the traditional statistical model.

Tao *et al.* [16] reduced data dimensions through a stacked auto-coding network and used the output low-dimensional data as the input for a back-propagation neural network (BPNN) to assess situation. To further enhance NSSA effectiveness, this paper introduces a situation assessment and prediction method based on machine learning. Experiments were conducted on the designed method to evaluate its performance in addressing NSSA challenges. This work offers a novel security method for enterprise control systems, contributing to the safe operation of network systems.

2 Network Security Situation Awareness Methods

2.1 XGBoost-Based Situational Assessment Method

As industrialization and informationization continue to integrate, the interconnection between the enterprise control system and the Internet deepens. This integration aims to simultaneously enhance production efficiency and elevate management standards within enterprises. However, a surge in security threats emanating from the network also appears. Attacks on the control system network of enterprises often have a direct impact on their production and operational efficiency. In 2012, Saudi Arabia's National Petroleum Company experienced a cyberattack that paralyzed its internal network. In 2014, a Norwegian offshore oil platform fell victim to a network attack, resulting in production interruptions. Additionally, in 2015, the Ukrainian power system faced a large-scale cyberattack, leading to a prolonged power outage [18]. As technology continues to advance, the network security threats confronting enterprise control systems are becoming increasingly complex and diverse. This evolution necessitates heightened standards for network security protection.

NSSA can realize effective monitoring and analysis of the enterprise control system network, enabling early detection of potential attacks and reducing the extent of damage. NSSA includes situation assessment and situation prediction. The first one pertains to evaluating the present state of security, while the second one relates to forecasting the forthcoming status of network security. First of all, in terms of situation assessment, it is necessary to quantify the security situation according to certain indicators. This paper is based on the characteristics of the enterprise control system network and quantifies the security situation based on the attacks on the network. The details are shown below.

1) Attack probability P: The percentage of attack data out of the total amount of network data over a period of time.

2) Impact degree of attack Y: According to the common vulnerability scoring system (CVSS) [6], the impact on the network is categorized into three categories: confidentiality, integrity, and availability, and the weights are taken as 0.3, 0.1, and 0.6 respectively. The impact degree of the i-th kind of attack can be written as:

$$Y_i = round_2[\log_2(\frac{0.3 \times 2^{C_i} + 0.1 \times 2^{I_i} + 0.6 \times 2^{A_i}}{3})],$$

where $round_2$ means reserving two decimal places, C_i, I_i, and A_i corresponds to the impact value of confidentiality, integrity, and availability of the i-th kind of attack. The impact value is set as 0/0.2/0.6 corresponding to no (N), low (L), and high (H) impact.

Ultimately, the quantization yields a situation value of:

$$V = \frac{P \times \sum_{i=1}^{n} Y_i \times N_i}{N_A}$$

where N_i stands for the number of the i-th kind of attack and N_A stands for the count of attacks on the network.

Referring to the National Internet Emergency Center, the situation values are divided into four levels (Table 1).

Table 1: Classification of situation levels

Situation value	Security level
0-0.2	Excellent
0.2-0.4	Good
0.4-0.75	Medium
0.75-0.9	Poor
0.9-0.1	Dangerous

For the classification of attacks on the network, this paper chooses the XGBoost algorithm [10], a machine learning method, whose objective function can be written as:

$$obj = \sum_{i=1}^{n} l(y_i, \hat{y_i}) + \sum_{k=1}^{K} \Omega(f_k),$$

where $\sum_(i = 1)^n l(y_i, \hat{y_i})$ is the error between the actual and predicted values, and $\sum_{k=1}^{K} \Omega(f_k)$ is the regularity term, which is employed for managing the intricacy of the model. Performing a Taylor second-order expansion on the above equation, at the t-th iteration, the objective function can be rewritten as:

$$obj^{(t)} = \sum_{i=1}^{n} [g_i f_t(x_i) + \frac{1}{2} h_i f_t^2(x_i)] + \Omega(f_t),$$

where g_i is the first-order derivative and h_i is the second-order derivative. After sorting, there is:

$$obj^{(t)} = -\frac{1}{2} \sum_{j=1}^{T} (\frac{G_j^2}{H_j + \lambda}) + \gamma T,$$

where T is the count of leaf nodes, γ and λ are penalty factors.

The formula for the iterative decision tree can be written as: *** please add a formula. ***

where η is the learning rate of the iterative decision tree, which is used to control the iteration speed (0-1, 0.1 by default). In addition, the values of maximum depth of the tree and the number of weak classifiers, i.e., m and n, will also affect the accuracy of the algorithm for the classification of cyber-attacks. In order to obtain better performance, appropriate parameter adjustment is needed [15]. Therefore, this paper uses an improved bat

algorithm (IBA) to realize the optimization of η, m, and n in the XGBoost algorithm.

The bat algorithm (BA) is a swarm intelligence algorithm [7] and finds extensive usage in various optimization problems [19]. Assume that a bat flies at position h_i with a velocity of v_i, the frequency range of sound wave is $[f_{\min}, f_{\max}]$, the loudness range is $[A_{\min}, A_0]$, and the wavelength is λ, then the equation for updating the position and velocity of the bat can be written as:

$$\begin{aligned} v_i^t &= v_i^{t-1} + (x_i^{t-1} - x_g) f_i \\ x_i^t &= x_i^{t-1} + v_i^t, \end{aligned}$$

where x_g is the current global optimal position of the bat and f_i is the frequency of adjusting the bat's velocity, whose calculation formula is:

$$f_i = f_{\min} + \beta \times (f_{\max} - f_{\min}),$$

where β is a random number obeying a normal distribution in [0,1]. The local search process for the bat can be written as:

$$x_{new} = x_{old} + \alpha A_{avg}^t$$

where x_{new} is the new solution, x_{old} is the selected optimal old solution, $\alpha \in [-1, 1]$, and A_{avg}^t is the average loudness of the bat's sound waves at moment t. When a bat finds a prey, it raises the frequency of the sound wave and decreases the loudness of the sound wave to move towards the prey. The process can be written as:

$$\begin{aligned} A_i^{t+1} &= \alpha A_i^t, \\ r_i^{t+1} &= r_i^0 [1 - \exp(-\delta t)], \end{aligned}$$

where r_i^0 is the initial pulse emissivity, α and δ are constants.

In order to further improve the BA's optimization searching effect, the initialization of bat populations is implemented based on Tent chaotic mapping [4], and the process is as follows:

1) Initial value x_0 is randomly generated within the range of (0,1).

2) A sequence of Tent chaotic mappings is generated based on the following equation:

$$x_{k+1} = \begin{cases} 2x_k + rand(u\frac{n-k}{n}), & 0 \le x_k \le 0.5 \\ 2(1 - x_k) + rand(u\frac{n-k}{n}), & 0.5 < x_k \le 1 \end{cases}$$

where x_k denotes the value after k times of Tent chaotic mapping, n denotes the total number of calculations to be performed, u stands for the disturbance coefficient, and rand denotes a random number between 0 and 1.

3) The sequence is intercepted to obtain a number of numerical sequences, which are the initialized bat population.

The specific procedure of the IBA-XGBoost algorithm-based situation assessment method is as follows.

1) The parameters of the XGBoost algorithm are initialized, and bat individuals are encoded according to the parameters that need to be optimized.

2) The bat population is initialized using Tent chaotic mapping, and the optimal bat individual, i.e., the optimal parameter of the XGBoost algorithm, is calculated by IBA using the mean square error (MSE) as the objective function.

3) The optimal parameters obtained are used to build a situation assessment model, and a test set is input for model evaluation.

2.2 Bidirectional Long Short-Term Memory-Based Situation Prediction

There is a certain temporal pattern in network attacks on enterprise control systems. To address situation prediction, this paper selects bidirectional long short-term memory (BiLSTM), renowned for its effectiveness in temporal prediction, as the model. BiLSTM [14] addresses the limitations of traditional unidirectional long short-term memory (LSTM), which can only capture information from one direction. The BiLSTM architecture is depicted in Figure 1.

LSTM obtains the output through the calculation of three gates. Suppose the state of the hidden layer at the previous moment is h_{t-1}, the input at the current moment is x_t, then the output of the forgetting gate is f_t:

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f).$$

The input gate is used to update important information, and its output is i_t:

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i).$$

Cell state C_t at the current moment can be written as:

$$C_t = f_t \times C_{t-1} + i_t \times \tilde{C}_t,$$

where $\tilde{C}_t$ is the interim cell state: $\tilde{C}_t = \tanh(W_c \cdot [h_{t-1}, x_t] + b_c)$. Finally, the calculation formulas of output gate o_t and hidden layer state h_t at the current moment are:

$$\begin{aligned} o_t &= \sigma(W_o \cdot [h_{t-1}, x_t] + b_o), \\ h_t &= o_t \times \tanh(C_t). \end{aligned}$$

There are also parameters in BiLSTM that can affect the effectiveness of the situation prediction, and IBA is also used for optimization. The specific procedure of the IBA-BiLSTM-based situation prediction approach based on is presented below.

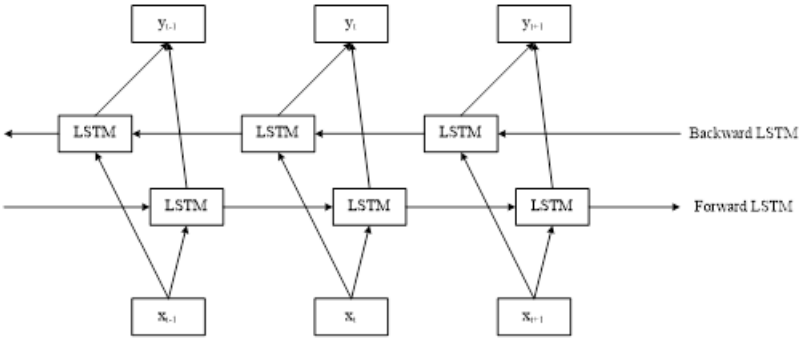


Figure 1: BiLSTM structure

1) The structure of BiLSTM is initialized. The optimization targets include the quantity of iterations, the Dropout ratio, and the count of units in hidden layers. Individual bats are encoded.

2) The parameters of BiLSTM are optimized using IBA.

3) The optimal parameters of BiLSTM are obtained to establish a situation prediction model. The model is utilized to generate prediction outcomes by inputting the test set.

3 Experiments and Analysis

3.1 Experimental Setup

Experiments were performed on a computer system that operated on Windows 10. This sytem was equipped with an Intel(R)Core(TM) i7-5500U processor and had a memory capacity of 8 GB. Python 3.9 programming language was used. The dataset used for the experiments was from NSL-KDD [17]. Each sample contained 41-dimensional features and one-dimensional labels, and the attacks are distributed as presented in Table 2.

Table 2: Distribution of cyber-attacks in the NSL-KDD dataset

	KDD Train+	KDD Test+
Normal	67343	9711
DoS	45927	7458
Probe	11656	2421
U2R	52	200
R2L	995	2654
Total	125973	22544

The situation values obtained using the IBA-XGBoost model were used as the data for the situation prediction, and the inputs and outputs of the IBA-BiLSTM model were determined using a sliding window with a value of 6. The situation values of the first five moments were taken as the inputs, which were used to predict the situation values of the latter moments. The performance of both the situation assessment and prediction methods was evaluated using the following two indicators.

Assuming that the actual value is y_i and the output value of the model is $\hat{y}_i$.

1) Root-mean-square error (RMSE): A quantification of the disparity between the observed value and the estimated value:

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2};$$

2) Mean absolute error (MAE): The actual situation of the error of the estimated value:

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|y_i - \hat{y}_i|.$$

3.2 Results Analysis

Ten samples were randomly selected to compare the IBA-XGBoost model with other machine learning methods:

1) K-nearest neighbor (KNN) [5];

2) Support vector machine (SVM) [3];

3) Decision tree (DT) [13].

The findings are presented in Table 3.

Table 3 reveals that the KNN method exhibited two sample evaluation errors. Specifically, the evaluation result for sample 4 was medium, while the actual level was poor. Similarly, the evaluation result for sample 7 was medium, while the actual level was poor. The SVM method demonstrated two sample evaluation errors. Sample 4 received a medium evaluation, but it was poor actually; sample 8 was rated as poor, but its actual level was dangerous. The DT method obtained a sample evaluation error. Its assessment for sample 4 was medium, but it was actually poor. Both the XGBoost and IBA-XGBoost methods accurately evaluated all the ten samples, highlighting the superior performance of the XGBoost-based

Table 3: Results of security situation assessment

	KNN	SVM	DT	XGBoost	IBA-XGBoost	Actual value
1	0.155/excellent	0.107/excellent	0.145/excellent	0.133/excellent	0.125/excellent	0.12/excellent
2	0.268/good	0.213/good	0.262/good	0.251/good	0.244/good	0.24/good
3	0.584/medium	0.589/medium	0.579/medium	0.546/medium	0.551/medium	0.55/medium
4	0.721/medium	0.732/medium	0.748/medium	0.761/poor	0.782/poor	0.77/poor
5	0.264/good	0.256/good	0.212/good	0.225/good	0.232/good	0.23/good
6	0.397/good	0.391/good	0.384/good	0.357/good	0.367/good	0.36/good
7	0.734/medium	0.752/poor	0.801/poor	0.771/poor	0.785/poor	0.78/poor
8	0.951/dangerous	0.889/poor	0.935/dangerous	0.927/dangerous	0.912/dangerous	0.91/dangerous
9	0.289/good	0.221/good	0.231/good	0.247/good	0.255/good	0.25/good
10	0.961/dangerous	0.959/dangerous	0.907/dangerous	0.945/dangerous	0.934/dangerous	0.93/dangerous

Note: Bolding indicates that the output situation level does not match the reality.

assessment method. To further understand the performance of different assessment methods, RMSE and MAE were compared, as depicted in Figure 2.

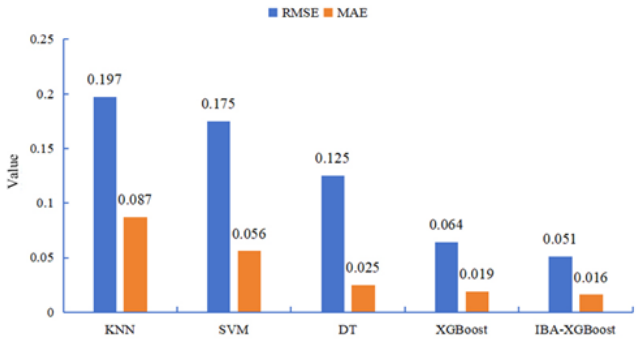


Figure 2: Comparative results of RMSE and MAE on the situational assessment

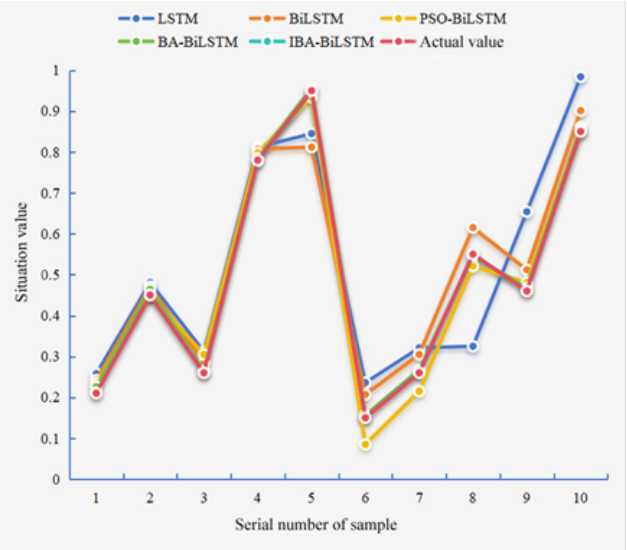


Figure 3: Security situation prediction results

Observing Figure 2, it becomes evident that the KNN method exhibited the poorest performance in assessing the cybersecurity situation of enterprise control systems, with an RMSE and MAE of 0.197 and 0.087 respectively. The SVM and DT methods had an RMSE value greater than 0.1. In comparison, the RMSE and MAE of the XGBoost method was 0.064 and 0.019, respectively, both markedly lower than the values of the KNN, SVM, and DT methods. Subsequently, after parameter optimization by IBA, the RMSE of the IBA-XGBoost approach was 0.051, reflecting a 20.31% reduction compared to the XGBoost method, and the MAE was 0.016, demonstrating a 15.79% reduction compared to the XGBoost method. This result demonstrated the efficacy of IBA in enhancing the performance of the XGBoost method. Again with ten samples, the IBA-XGBoost method was compared with the following methods: LSTM, BiLSTM, BiLSTM optimized by particle swarm algorithm (PSO) [2]: PSO-BiLSTM, BA-BiLSTM, and IBA-BiLSTM. The comparative results are presented in Figure 3.

In Figure 3, it is evident that the predicted values obtained by the LSTM method exhibited a large gap from the real values, accompanied by considerable fluctuations, notably in the prediction for sample 8 where the disparity was pronounced. Subsequently, the prediction results of the BiLSTM and PSO-BiLSTM methods slightly outperformed the LSTM method, yet there remained a discernible gap from the real values. In contrast, the predicted values of the BA-BiLSTM and IBA-BiLSTM methods aligned closely with the real values, indicating their superior prediction capabilities. The calculated RMSE and MAE results were compared in Figure 4.

The findings illustrated in Figure 4 suggest that, among the compared methods, the LSTM method exhibited a poor performance in situation prediction. In contrast, the BiLSTM method outperformed the LSTM method with a lower RMSE of 0.107 and MAE of 0.061, indicating that the BiLSTM approach was more adept at capturing temporal information in situation values over time, leading to superior results compared to the LSTM

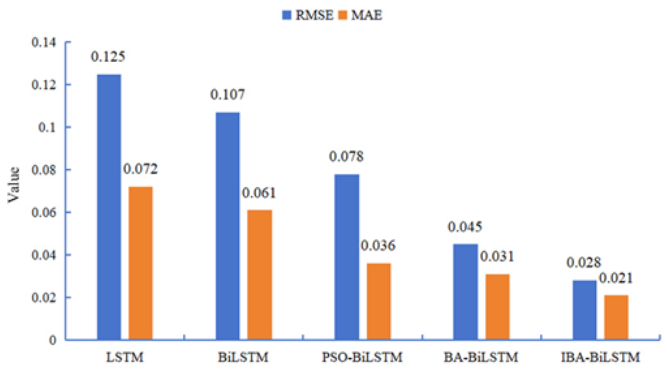


Figure 4: Comparative results of RMSE and MAE

method. The RMSE of the BA-BiLSTM method was 0.045, representing a 42.31% reduction compared to the PSO-BiLSTM method, while the MAE was 0.031, signifying a 13.89% reduction compared to the PSO-BiLSTM method. This result demonstrated that, in comparison to PSO, BA yielded superior parameter optimization effects for BiLSTM. Finally, the RMSE of the IBA-BiLSTM approach was 0.028, demonstrating a 37.78% reduction compared to the BA-BiLSTM approach, and its MAE was 0.021, indicating a 32.26% reduction compared to the BA-BiLSTM approach. This result confirmed that the IBA was more effective in enhancing prediction performance.

4 Conclusion

This paper studied the NSSA challenges faced by enterprise control systems based on machine learning. The IBA-XGBoost method and the IBA-BiLSTM method were designed for situation evaluation and prediction respectively. Through experimentation on the NSL-KDD dataset, it was observed that the two approaches exhibited superior performance in both situation assessment and prediction. They are effective in obtaining more accurate situation values for determining security levels and making reliable predictions for future situation values. The two methods hold promising potential for practical applications in real-world enterprise control systems.

References

[1] A. Alamleh, O. S. Albahri, A. A. Zaidan, A. H. Alamoodi, A. S. Albahri, B. B. Zaidan, S. Qahtan, "Multi-attribute decision-making for intrusion detection systems: A systematic review," *International Journal of Information Technology & Decision Making*, vol. 22, no. 01, pp. 589-636, 2023.

[2] A. Amiri, A. Salmasnia, M. Zarifi, M. R. Maleki, "Adaptive Shewhart control charts under fuzzy parameters with tuned particle swarm optimization algorithm," *Journal of Industrial Integration and Management*, vol. 8, no. 2, pp. 241-276, 2023.

[3] F. Camastra, V. Capone, A. Ciaramella, A. Riccio, A. Staiano, "Prediction of environmental missing data time series by support vector machine regression and correlation dimension estimation," *Environmental Modelling & Software*, vol. 150, pp. 1-7, 2022.

[4] S. Chen, S. Wang, "An optimization method for an integrated energy system scheduling process based on NSGA-II improved by tent mapping chaotic algorithms," *Processes*, vol. 8, no. 4, pp. 1-11, 2020.

[5] P. Chumnanpuen, "K-nearest neighbor and random forest-based prediction of putative tyrosinase inhibitory peptides of abalone haliotis diversicolor," *Molecules*, vol. 26, no. 12, pp. 1-10, 2021.

[6] K. Gencer, F. Baifti, "The fuzzy common vulnerability scoring system (F-CVSS) based on a least squares approach with fuzzy logistic regression," *Egyptian Informatics Journal*, vol. 22, no. 2, pp. 145-153, 2020.

[7] Y. Guo, J. Chen, "An anomaly feature mining method for software test data based on bat algorithm," *International Journal of Data Mining and Bioinformatics*, vol. 27, pp. 58-72, 2022.

[8] J. He, J. Yang, "Network security situational level prediction based on a double-feedback elman model," *Informatica: An International Journal of Computing and Informatics*, vol. 46, no. 1, pp. 87-93, 2022.

[9] M. Husák, L. Sadlek, S. Špaček, M. Laštovička, M. Javorník, J. Komárková, "CRUSOE: A toolset for cyber situational awareness and decision support in incident handling," *Computers & Security*, vol. 115, pp. 1-5, 2022.

[10] S. T. Ikram, A. K. Cherukuri, B. Poorva, P. S. Ushasree, Y. S. Zhang, X. Liu, G. Li, "Anomaly detection using xgboost ensemble of deep neural network models," *Cybernetics and Information Technologies*, vol. 21, no. 3, pp. 175-188, 2021.

[11] S. H. Mohammed, A. D. Jasim, "Evaluation of firewall and load balance in fat-tree topology based on floodlight controller," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, pp. 1157-1164, 2020.

[12] S. Pavol, Staňa Richard, G. Andrej, et al., "Network security situation awareness forecasting based on statistical approach and neural networks," *Logic Journal of the IGPL*, vol. 31, no. 2, pp. 352–374, 2023.

[13] A. Pradeepika, R. Sabitha, "Examination of diabetes mellitus for early forecast using decision tree classifier and an innovative dependent feature vector based naive bayes classifier," *ECS Transactions*, vol. 107, no. 1, 2022.

[14] A. Shaikh, M. Bhargavi, C. P. Kumar, "An optimised Darknet traffic detection system using modified locally connected CNN - BiLSTM network," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 43, pp. 87-96, 2023.

[15] P. Srinivas, R. Katarya, "hyOPTXg: OPTUNA hyper-parameter optimization framework for predicting cardiovascular disease using XGBoost,"

Biomedical Signal Processing and Control, vol. 73, pp. 1-10, 2022.

[16] X. Tao, K. Kong, F. Zhao, S. Cheng, S. Wang, "An efficient method for network security situation assessment," *International Journal of Distributed Sensor Networks*, vol. 16, no. 11, pp. 1-13, 2020.

[17] M. Tavallaee, E. Bagheri, W. Lu, A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA'09)*, pp. 53-58, 2009.

[18] J. Weiss, "Industrial control system cyber security and the critical infrastructures," *OR Insight*, vol. 19, no. 4, pp. 33-36, 2016.

[19] C. Yang, L. L. Sun, H. Guo, Y. S. Wang, Y. Shao, "A fast 3D-MUSIC method for near-field sound source localization based on the bat algorithm," *International Journal of Aeroacoustics*, vol. 21, no. 3/4, pp. 98-114, 2022.

[20] Y. Yao, Y. Sun, Z. Liu, X. Meng, Z. Liu, "A data fusion framework of multi-source heterogeneous network security situational awareness based on attack pattern," *Journal of Physics: Conference Series*, vol. 1550, no. 6, pp. 1-12, 2020.

[21] B. Zhu, Y. Chen, Y. Cai, "Three kinds of network security situation awareness model based on big data," *International Journal of Network Security*, vol. 21, no. 1, pp. 115-121, 2019.

Biography

Hui You, born in June 1984, has received the doctor's degree from Beijing Normal University in 2020. She is an associate professor and is working in Beijing Police College. She is interested in mathematical modeling, network security, and big data.

Transform Sequential Data to Image for Detecting Covert Timing Channel

Xuwen Huang[1], Yonghong Chen[2], Xiaolong Zhuang[1], and Yuwei Lin[1]
(Corresponding author: Yonghong Chen)

School of Computer Science and Technology, Huaqiao University[1]
Xiamen Key Laboratory of Data Security and Blockchain Technology, Huaqiao University[2]
Xiamen, Fujian 361000, China
Email: djandcyh@163.com

(Received Aug. 30, 2023; Revised and Accepted Jan. 23, 2024; First Online Feb. 14, 2024)

Abstract

The network covert timing channel utilizes inter-packet delay to encode binary data to achieve information leakage and other purposes. In recent years, Covert Timing Channels (CTCs) have been demonstrated to be applicable across various protocols and networks, posing a significant threat to network security. Simultaneously, new CTCs have challenged the efficacy of CTC detection schemes. The recent ϵ-κlibur and ϵ-κlibur-O channels exhibit structural and characteristic similarities to legitimate channels, rendering ML-based detection methods like GAS and Snap ineffective. In this paper, we investigate an approach based on Gramian Angular Field (GAF), Markov Transition Field (MTF), and Recurrence Plot (RP) image processing. We further employ the knowledge-distilled and compressed image classification model MobileVit for detection. Our approach achieves a detection rate 98.24% for seven different channels within a sampling window of 64 IPDs. Experimental results demonstrate our proposed scheme's generality, sensitivity, and effectiveness.

Keywords: Covert Time Channel; Image Classification Network; Knowledge Distillation; MobileViT

1 Introduction

The network covert timing channel (CTC) is a technique that achieves information hiding through the manipulation of inter-packet delays based on constructed rules. In the past decade, numerous studies have utilized various protocols to implement CTCs. For instance, CTCs have been established through VoLTE traffic [46] and the MQTT protocol in the Internet of Things [27]. Moreover, CTCs have been implemented in diverse scenarios and networks, such as Vehicle Ad-Hoc Networks (VANETs) [38] and CAN bus communication in vehicular networks [12].

The characteristics of CTC make it have both positive and negative effects. CTCs are concealed, private and they possess low active drop rates. Malicious software employs CTCs to obfuscate its presence, making it challenging to detect [25]. On the other hand, CTCs can serve legitimate purposes, such as enabling reliable covert communications within MTS systems [20] or evading censorship [4]. They can also be applied in automotive control networks to enhance robustness and ensure stable communication [41].

Current detection methods for network covert timing channels predominantly rely on statistical and deep learning approaches. Statistical solutions extract statistical features, effectively detecting specific CTCs but lacking generality and sensitivity, particularly with larger sampling windows [17]. With hardware advancements, deep learning-based CTC detection schemes have emerged, demonstrating substantial effectiveness [10], although cost reduction remains an ongoing concern. Recently, Sebastian *et al.* [47] proposed ϵ-κlibur and ϵ-κlibur-O channels, imitating the distribution structure of normal Inter-Arrival Times (IATs and IPDs are the same) to undermine CTC detection performance. ML-based methods like Snap and GAS fail to effectively detect these channels. While enhanced ϵ-similarity has been proposed to improve ϵ-κlibur detection performance without significantly compromising original CTC detection. But it lacks generality, yielding AUC values between 0.80 and 0.88 for TRCTC. Therefore, new CTC detection solutions must simultaneously address both sensitivity and generality.

Inter-packet delay (IPD) represents univariate sequential data and CTC detection aims to classify it. This paper proposes leveraging IPD characteristics by transforming sequential data into images for classification. Inspired by significant achievements in computer vision, Wang *et al.* [43] introduced the encoding of time series data into various image types, such as GAF and MTF. By converting 12 standard datasets into combined GAF-MTF images, they demonstrated that the tiled CNN-based image classification model outperformed concurrent state-of-

the-art methods. GAF retains time dependencies between consecutive IPDs, MTF captures IPD probability transition patterns and Recursive Plot (RP) preserves non-stationarity and inherent similarity of IPDs. In previous work, our team applied GAF, MTF and RP image processing techniques for CTC detection. The combination of GAF-MTF-RP images yielded the best classification results [15]. Our approach achieved effective detection on publicly available and locally collected datasets, utilizing the MobileVit network as the optimal model and a sampling window of 64 IPDs. Building upon this prior research, this paper conducts detection for ϵ-κlibur and ϵ-κlibur-O. We also use knowledge distillation to compress the MobileVit model. In summary, the key contributions of this paper can be summarized as follows:

- We introduce detection methods for ϵ-κlibur and ϵ-κlibur-O, leveraging GAF, MTF and RP to extract feature matrices from sequential data IPD. These three matrices are combined into a three-channel image for classification.
- We employ knowledge distillation on the MobileVit network. Compared to a teacher network, using three teacher networks to train MobileVit network yields the best results. Distilled models offer advantages in terms of scale and speed, facilitating faster detection and reduced deployment costs.
- We conduct a series of comparative experiments, training the distilled network with optimal parameters, achieving the highest accuracy in classifying seven different channels. Furthermore, our distilled network outperforms popular distillation networks like Deit [40] and FasterNet [8] for this specific classification task.

The remaining sections of this paper are organized as follows: Section 2 discusses related work. In Section 3, we provide a detailed presentation of the detection approach, including its conceptual framework and intricate details. Section 4 outlines the configuration of our proposed scheme, including parameter settings and presents the results of our experimental analysis, which are subsequently showcased and analyzed. Finally, Section 5 concludes our work, summarizing the key findings and contributions.

2 Related Work

Research on the distribution patterns of normal traffic's inter-packet delay has shown that it does not adhere to a normal distribution. Early studies proposed that IPD follows distributions such as Pareto [31] and gamma distributions [29]. Recently Weibull distribution has been considered for studying anomalous IPD for Intrusion Detection Systems (IDS) [35]. We use the traffic data from GAS [17]. It has two datasets. Both datasets follow long-tailed distributions, while Backbone traffic has larger deviation than Lab, indicating more disperse IPDs and more fluctuant timing behavior [17]. It is sourced from CAIDA and some similar datasets have demonstrated adherence to the Weibull distribution such as MAWI, NUST [35]. Additionally, other laws like Benford's Law [30] and Zipf's Law [39] have also been employed to model normal traffic IPD characteristics. Some IDS systems construct models for binary classification based on the distribution patterns of normal IPD, without studying the IPD of CTCs. However, CTCs possess different IPD characteristics from normal traffic, allowing them to easily bypass IDS. In the aforementioned studies, variations in IPD distribution structure are observed due to different paths, periods and environments of the collected datasets. This variation may lead to differing findings. Similar challenges exist in current CTC detection research and CTC detection schemes which need to be validated across different datasets. Therefore, for CTC research, we advocate for the release of more publicly available datasets.

In recent literature on CTC classification research, CTCs are mainly categorized into Fixed-IPD Channels, Dynamic-IPD Channels, Combinatorial-IPD Channels and Delayed-IPD Channels [17]. These are represented by IPCTC [6], Jitterbug [34], LNCTC [33] and TRCTC [5], respectively, which are commonly studied as the primary detection targets.

2.1 Channel Classification

This paper primarily investigates and introduces six types of covert timing channels, including four typical CTCs and two recent CTCs.

2.1.1 IPCTC

Cabuk *et al.* [6] proposed IP Covert Timing Channel (IPCTC), where the sender and the receiver select parameter ω as the time interval for sending packets. For sending a bit 1, the sender sends a packet within ω time. For sending a bit 0, the sender remains silent for ω time.

2.1.2 Jitterbug

Shah *et al.* [34] proposed the passive CTC JitterBug. The sender and the receiver choose parameter ω. For sending a bit 1, the sender increases the time interval to a multiple of ω. For sending a bit 0, the sender increases the delay to a multiple of $\omega/2$, while avoiding multiples of ω.

2.1.3 LNCTC

Sellke *et al.* [33] proposed the LNCTC, using parameters L-bit and N consecutive IPDs. L-bits are embedded into N consecutive IPDs. The consecutive IPDs are of the set T. $T = \{D,\ D + 2^0 * d,\ \cdots,\ D + 2^L * d\}$. The sender and the receiver negotiate to determine the value of D and d.

2.1.4 TRCTC

Cabuk *et al.* [5] proposed a time-replay covert timing channel (TRCTC), which uses a legal traffic IPD set S. S is divided into two equal parts, S_0 and S_1. When the sender needs to send a bit 0, an IPD is randomly selected from S_0 to introduce a delay before sending bit 0. Similarly, when sending a bit 1, an IPD is selected from S_1.

2.1.5 ϵ-κlibur

Sebastian *et al.* [47] proposed ϵ-κlibur, modifying delays without compromising transmission bandwidth or reliability. Given an IPD list D, $D = \{d_1,\ d_2, \cdots,\ d_i\}$, modified delays are obtained as $D = \left\{d_1^{'},\ d_2^{'}, \cdots,\ d_i^{'}\right\}$. A threshold t is set. If $d_i \leq t$ and $d_i > t$, or $d_i > t$ and $d_i^{'} \leq t$. The count of errors increases. The impact score $I = E/D$, where smaller I is acceptable. Modifications are applied according to certain rules, with τ and 2τ as examples for CTC IPD lists. If d_i is not greater than t, $d_i^{'}$ is drawn from a normal distribution $N\,(0,\ (threshold/7))$ and takes positive values. If $d_i^{'}$ at this point exceeds t, $d_i^{'}$ is set to t. If the original d_i is greater than t, $d_i^{'}$ is drawn from $(1.5\tau,\ 2.4\tau)$ with a step size of 0.001. The author maintains I at 0.

2.1.6 ϵ-κlibur-O

Building upon ϵ-κlibur, an additional outlier value of 10τ is introduced to extend the distribution of time. This step makes the IPD distribution of ϵ-κlibur-O more similar to that of normal channels, as real-world conditions often involve fluctuations, causing delays to occasionally stand out.

Senders and receivers agree upon parameter modifications that still allow distinguishing between sending 1 and 0 using a threshold t. However, detection schemes are unaware of t and the IPD distribution of ϵ-κlibur and ϵ-κlibur-O closely resembles that of normal channels. As a result, detection performance is reduced.

2.2 CTC Detection Scheme Classification

CTC detection methods vary based on their distinctive features. This paper categorizes them as five parts.

2.2.1 Regularity, ϵ-similarity and Entropy-based Detection

ϵ-similarity [6] detection and compressibility [7] were proposed very early for CTC detection. Wendzel *et al.* [44] used compressibility score, ϵ-similarity and regularity for changing countermeasures in CTC detection. Gianvecchio *et al.* [11] proposed entropy-based CTC detection and Conditional Entropy Estimation (CEE) for detection. These are classical detection methods, they are often effective for one or two channels and require a large detection window.

2.2.2 Non-parametric Detection Methods

Mou *et al.* [28] proposed a sliding serial port detection scheme based on wavelet transform and Support Vector Machines (SVM). Liu *et al.* [21] proposed a detection approach utilizing Discrete Wavelet Multi-Resolution Transformation (DWMT). Rezaei *et al.* [32] detected CTCs by three non-parametric statistical tests, Spearman Rho, Wilcoxon Signed-Rank and Mann-Whitney-Wilcoxon rank sum test.

2.2.3 Machine Learning Based Detection Methods

Shrestha *et al.* [36] proposed a SVM classifier training fingerprinting CTC flows for detection. iglesias *et al.* [16] utilized decision trees to classify traffic. Li *et al.* [18] collected eight statistical features of IPD as communication fingerprints for classification by a Random Forest classifier.

Darwish *et al.* [9] proposed a deep learning-based hierarchical statistical classification detection method for CTCs. Han *et al.* [9] utilized K-Nearest Neighbors (KNN) for classification based on various statistical indicators. Al-Eidi *et al.* [2] proposed a hybrid model of CNN and LSTM for CTC detection using IPD sequential data. li *et al.* [19] proposed similar model using CNN and Transformer architectures for detection .

2.2.4 Image Processing and Sequential Data Processing-based Detection

Snap is the first CTC solution using image processing [1]. Wu *et al.* [45] proposed an approach based on sequential data, firstly transforming it into symbol time series, computing State Transition Probability Matrices (STPM) and finally classifying based on similarity scores. Sun *et al.* [37] proposed a detection approach for CTCs using GAF images and GAN network(CD-ACGAN). Based on Snap, Al-Eidi *et al.* [3] proposed a CNN image classification model for detection.

2.2.5 Other Detection Methods

Lu *et al.* [24] proposed a multi-dimensional feature detection analyzed from the perspectives of shape, change pattern and data statistics. Wang *et al.* [42] proposed a detection scheme for CTCs based on perceptual hashing.

2.3 Image Classification Networks

Image classification has been an active research trend worldwide, greatly facilitated by the emergence of artificial intelligence. The introduction of deep learning algorithms has brought various innovations in image classification. Each year witnesses the emergence of important networks for image classification. Notable examples include ResNet [13], Swin Transformer [22], Convnext [23] and MobileVit [26] etc.

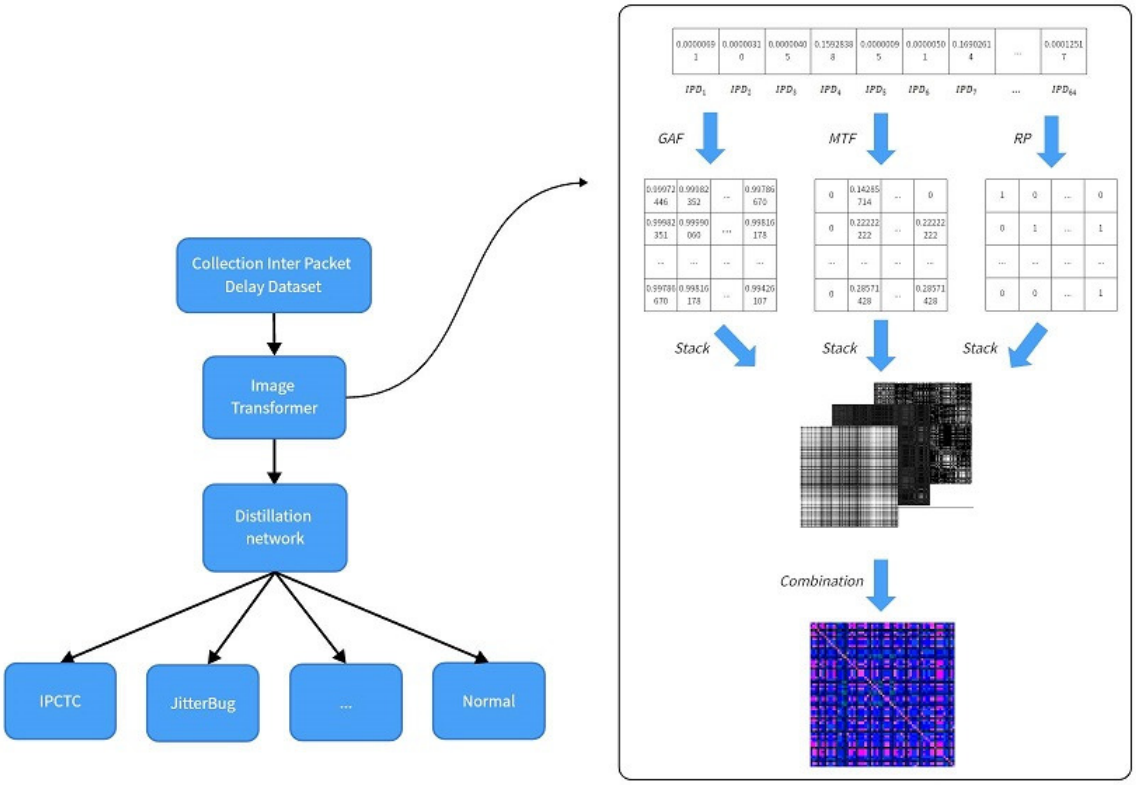


Figure 1: The proposed scheme

2.4 Knowledge Distillation

Knowledge distillation was proposed by Geoffrey Hinton [14], compresses knowledge learned by multiple models into a single model that is easier to deploy. Currently, knowledge distillation has been applied to lightweight networks like Deit and FasterNet in image classification.

3 Approach

This section provides a detailed description of our detection scheme. First, we extract three matrices of IPD, GAF, MTF and RP. These matrices are subsequently normalized and mapped to pixels, forming a three-channel image. Let the sequential data of IPD be represented by $X = \{x_1, x_2 \cdots x_n\}$, with a length of N. The proposed scheme is depicted as Figure 1.

3.0.1 GAF

Mapping X to the range$[-1,\ 1]$:

$$\widetilde{p_i} = \frac{(x_i - max(X) + x_i - min(X))}{max(X) - min(X)}$$

Encoding values as cosine angles and time stamps as radii, thus representing Cartesian coordinates in polar form:

$$\begin{cases} \varnothing_i = arccos\left(\widetilde{p_i}\right), -1 \le \widetilde{p_i} \le 1 \\ r_i = \frac{i}{N}, 1 \le i \le N \end{cases}$$

The GAF matrix is represented by the sum of triangles between each pair of points, preserving their correlation:

$$G = \begin{bmatrix} cos\left(\varnothing_1 + \varnothing_1\right) & cos\left(\varnothing_1 + \varnothing_2\right) & \cdots & cos\left(\varnothing_1 + \varnothing_n\right) \\ cos\left(\varnothing_2 + \varnothing_1\right) & cos\left(\varnothing_2 + \varnothing_2\right) & \cdots & cos\left(\varnothing_2 + \varnothing_1\right) \\ \cdots & \cdots & \cdots & \cdots \\ cos\left(\varnothing_n + \varnothing_1\right) & cos\left(\varnothing_n + \varnothing_2\right) & \cdots & cos\left(\varnothing_n + \varnothing_n\right) \end{bmatrix}$$

3.0.2 MTF

Dividing X into Q quantile units, represented by quantiles $q\left(i, j \in \{1, 2, \ldots, Q\}\right)$, each x_i corresponding to a q_i value in the one-dimensional data sequence. Each x_{i+1} corresponding to a q_j. W_{ij} is used to denote the probability that q_i followed by q_j:

$$W_{ij} = P\left(x_t \in q_i | x_{t+1} \in q_j\right), 1 \le t \le N - 1$$

The Markov transition matrix is constructed by these probabilities:

$$M = \begin{bmatrix} W_{ij}|x_1 \in q_i, x_1 \in q_j & \cdots & W_{ij}|x_1 \in q_i, x_n \in q_j \\ W_{ij}|x_2 \in q_i, x_1 \in q_j & \cdots & W_{ij}|x_2 \in q_i, x_n \in q_j \\ \cdots & \cdots & \cdots \\ W_{ij}|x_n \in q_i, x_1 \in q_j & \cdots & W_{ij}|x_n \in q_i, x_n \in q_j \end{bmatrix}$$

3.0.3 RP

Reconstructing the one-dimensional time series into an m-dimensional phase space. For a time series X, its sampling

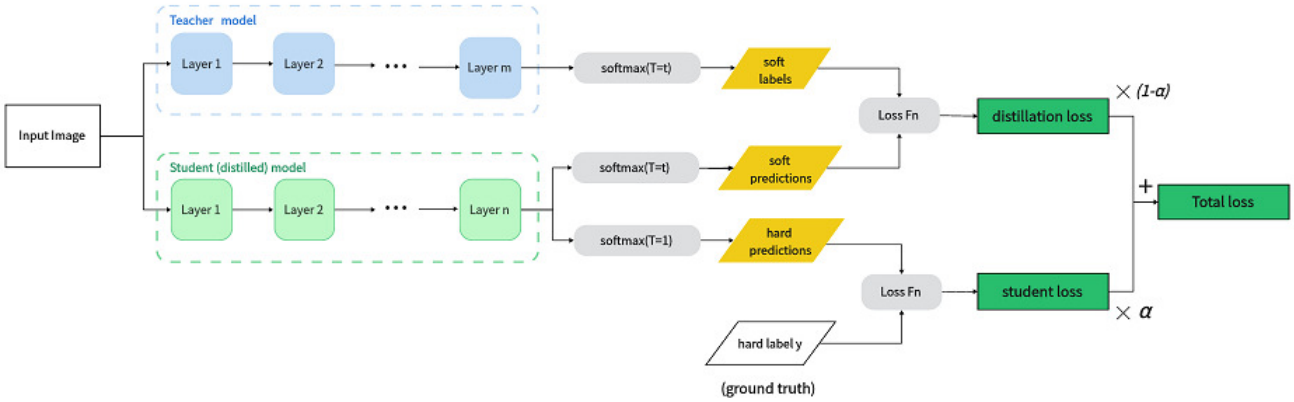


Figure 2: Knowledge distillation process

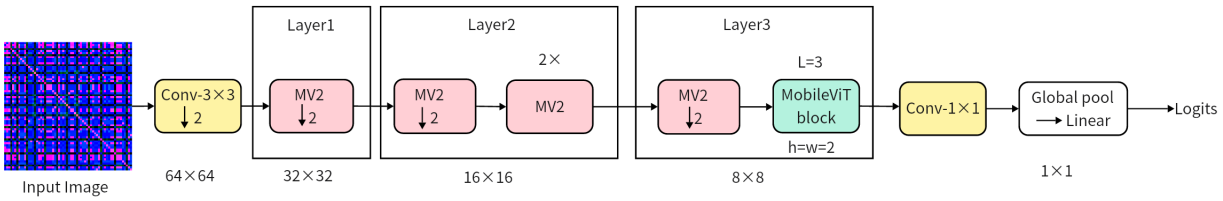


Figure 3: Our modified MobileViT structure

time interval is determined as Δt, along with embedding dimension m and delay time τ, to reconstruct X. The reconstructed dynamic system is defined as:

$$X_i = \left[x_i, x_{i+\tau}, ..., x_{i+(m-1)\tau}\right], i = 1, 2, 3, ..., n-(m-1)\tau$$

Calculating the distance S_{ij} between x_i and x_j in the reconstructed phase space:

$$S_{ij} = \|x_i - x_j\|, \ j = 1, 2, 3, ..., n-(m-1)\tau$$

$\|\bullet\|$ represents the norm. Computing the recursive value:

$$R(i,j) = \Theta(\varepsilon - S_{ij})$$

ε is the threshold. $\Theta(\bullet)$ is the Heaviside function. $\Theta(x \geq 0) = 1, \Theta(x < 0) = 0$, RP is composed of these recursive values.

3.0.4 Knowledge Distillation

For the GAF-MTF-RP images transformed from IPD, multiple models with different weights were trained, including ResNet, Swin-Transformer and ConvNeXt, which generally outperformed lightweight models [15]. However, these heavyweight models showed drawbacks in terms of model size, training time and detection time. In this study, ResNet, Swin-Transformer and ConvNeXt were selected as teacher networks, with MobileVit chosen as the lightweight student network. The experiments employed ResNet50, the tiny version of Swin-Transformer and the small version of ConvNeXt, all following the original paper's structures. Figure 2 shows the knowledge distillation flow chart.

During the experimental process, our student network, MobileVit, was tailored to accommodate 64-pixel images. While ensuring accuracy, we aimed to minimize the number of layers and parameters to meet scalability and speed requirements. Our optimized student network, MobileVit, differs from the xx-small (xxs) model of MobileVit by transitioning from a 5-layer architecture to a 3-layer architecture, resulting in a significant reduction in parameter count. Our modified MobileViT structure is shown in Figure 3. In the 3rd layer, a transformer block is present, with a total of 4 heads in the multi-head self-attention mechanism. The sequence length of intermediate tokens within the Feed-Forward Network (FFN) is set to 128.

After passing through the teacher networks and undergoing softmax, the resulting probability distribution had significant disparities, contributing minimally to the loss function. The concept of "temperature" was introduced to smooth the Logits. The smoothing formula is as follows:

$$q_i = \frac{exp(z_i/T)}{\sum_j exp(z_j/T)}$$

z_i represents the value of the i-th Logit, T is the distillation temperature and q_i is the probability value. Furthermore, the distillation loss is computed and then backpropagation optimizes the student neural network. The distillation loss formula is as follows:

$$L_{dis} = L_{KL}\left(q_i^{teacher}, q_i^{student}\right)$$

$L_{KL}()$ is the KL divergence, $q_i^{teacher}$ is the smoothed value of the i-th teacher network and $q_i^{teacher}$ the smoothed value of

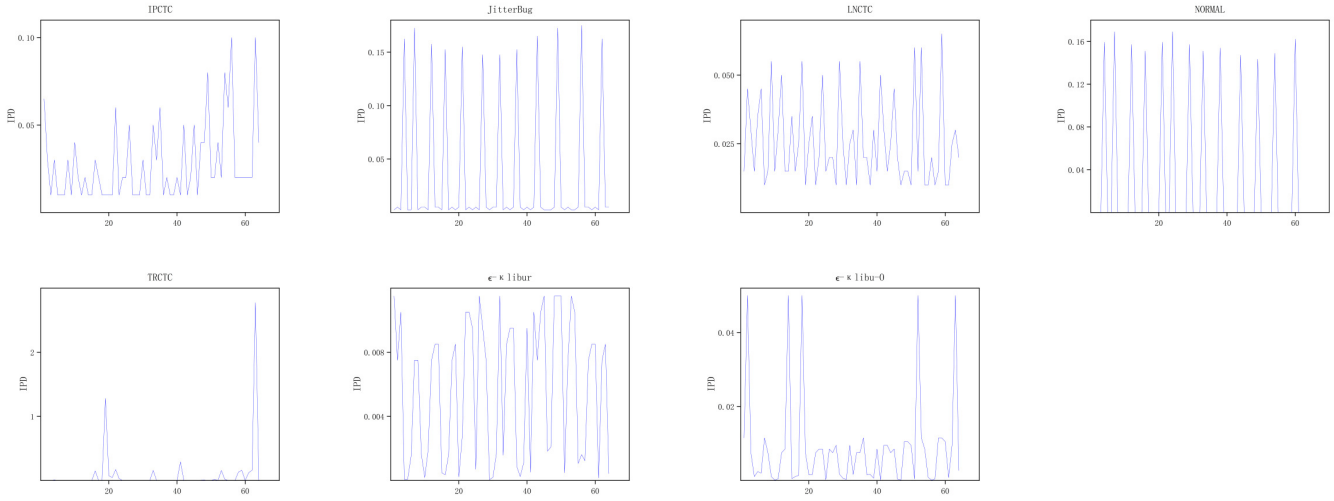


Figure 4: Statistical images of seven channels

the i-th student network. For combining multiple teacher networks, a set of weights w_k is introduced, calculated as follows:

$$w_k = softmax\left(v_k\right) = \frac{exp\ v_k}{\sum_{k=1}^{nt} exp\ v_k}, \sum_{k=1}^{nt} w_k = 1, w_k \in [0,1]$$

where nt represents the number of teacher networks, which is three. The outputs obtained from each teacher network after processing the input data are weighted accordingly:

$$z_i = x_1 \bigotimes w_1 + x_2 \bigotimes w_2 + \cdots + x_{nt} \bigotimes w_{nt}$$

4 Evaluation and Results

4.1 Dataset and Environment

The dataset used in this study is obtained from the GAS method's publicly available dataset [15]. We use the dataset from WAN. Its IPD is more dispersed, more fluctuating and more difficult to detect than the traffic generated by the experiment. The Python version is 3.9, the Torch version is 1.11.0 and the GPU used is the NVIDIA GeForce RTX 3080. The learning rates for ResNet, Swin-T, ConvNeXt and MobileVit are set to 0.0001. The batch size is 64 and the number of epochs is 100.

4.2 Evaluation Metrics

We use the following four metrics to measure the performance of our classification models, TP (True Positive) represents images that are correctly predicted as a CTC by MobileVit. TN (True Negative) represents images that are correctly predicted as legitimate traffic by MobileVit. FP (False Positive) represents images that are incorrectly predicted as a CTC. FN (False Negative) represents images that are incorrectly predicted as legitimate traffic. These metrics were used to calculate the performance indicators of the models:

$$Accuracy = (TP + TN) / (TP + TN + FP + FN)$$

$$Precision\ = TP / (TP + FP)$$

$$Recall\ = TP / (TP + FN)$$

$$F1 - Score = 2 \times Precision\ \times Recall / (Precision\ + Recall)$$

4.3 Image Processing

A dataset created using the backbone traffic from GAS and tools used in ϵ-κlibur and ϵ-κlibur-O was employed to produce ϵ-κlibur and ϵ-κlibur-O flow IPD. The statistical images for the seven data types are as Figure 4.

From the line chart, certain patterns such as relativity, periodicity and stability can be observed. These characteristics serve as the basis for IPD classification. IPCTC exhibits periodic patterns with upward segments, while JitterBug and Normal channels have many sharp sections, indicating significant fluctuations. LNCTC shows less pronounced periodicity, with the distribution primarily in the middle range of 0.012 to 0.06. TRCTC's IPD distribution has significant gaps, as it randomly delays an IPD time to send either 0 or 1, resulting in uneven distribution due to the delay of one small TRCTC segment among the larger Normal segments. For normal flow data and TRCTC, some IPD values are very small, close to 0, making them difficult to observe in the images. In real environments, most data packets are transmitted quickly, resulting in generally lower IPD values. ϵ-κlibur's IPD distribution is coherent, lacking severe fluctuations. ϵ-κlibur-O also exhibits uneven distribution but with more prominent extreme values compared to Normal and fewer than TRCTC. While classification based on the line chart is not accurate, transforming sequential data into images yields seven distinct images as shown in Figure 5.

4.4 Detection Effect of Teacher and Student Networks

Initially, the effects of the three networks without distillation were compared. As seen in the Figure 6, ConvNeXt achieved the highest overall accuracy of 98.43%, followed by Swin-T and ResNet at 98.33% and 98.18% respectively. MobileVit had the lowest accuracy at 97.15%. Compared to heavyweight networks, the lightweight MobileVit had lower accuracy. Additional parameters and layers of heavyweight networks contributed to their stronger learning capability in this image classification task.

Distillation was performed using one-to-one and three-to-

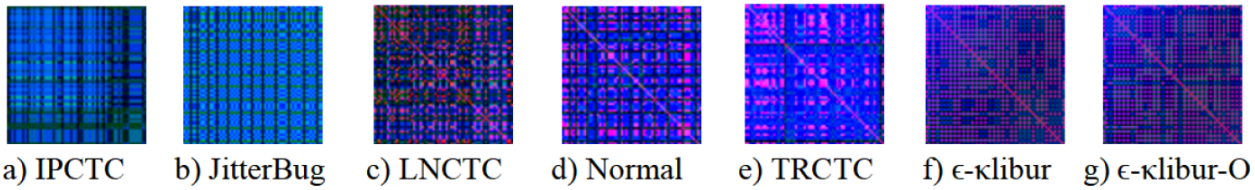


Figure 5: Transformed images of seven channels

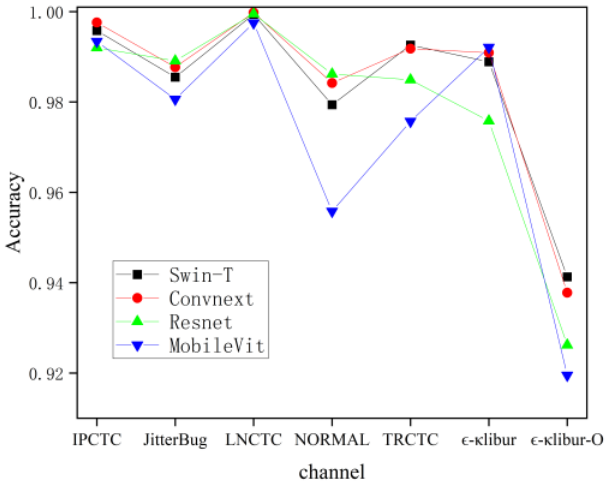


Figure 6: Seven channels accuracy of undistilled networks

one network configurations, as illustrated in Figure 7. In the one-to-one network, the highest accuracy achieved when ResNet trained MobileVit was 98.06%. Swin-T and ConvNeXt both had an accuracy of 98.01%, with little difference. In the three-to-one network, the highest accuracy was 98.24% (with $T = 7, \alpha = 0.3$), surpassing the accuracy of individual teacher networks. Soft labels provided by the three networks played a role in training the student network. Although the accuracy of the distillation network model decreased compared to the individual teacher network for classification, using multiple teacher networks enhanced the accuracy by 1.09% compared to the standalone student network, proving that the distilled MobileVit benefited from the knowledge of the teacher networks.

To find the best distillation network model, T and α were adjusted. The resulet is shown in Figure 8. When $T = 7$, the average accuracy of each channel reached a maximum of 98.24%. The next best accuracy was 98.10% when $T = 10$, followed by $(T = 3) > (T = 5) > (T = 1)$, with accuracies of 98.02%, 97.98% and 97.67% respectively. The comprehensive accuracy of the combined parameters $\alpha = 0.3$ was 98.24%, higher than 98.13% with $\alpha = 0.5$ and 98.01% with $\alpha = 0.7$. According to Figure 8 and Figure 9, the optimal values were T=7 and $\alpha = 0.3$.

4.5 Epoch and Accuracy Curves

In the field of image classification networks, Deit and FasterNet are two popular lightweight image classification networks that achieve good classification results on ImageNet-1K. In this experiment, the distilled MobileVit was compared to Deit and FasterNet. Deit achieved a peak accuracy of 96.27%, while FasterNet reached 98.06%. The code was obtained from the original paper. For this classification task, MobileVit outperformed in terms of classification accuracy. The comparison results are shown in Figure 10.

4.6 Detection Metrics for MobileVit in Different Channels

We collected various evaluation indicators of the scheme under seven channels and the results are shown in Table 1. In terms of various channel metrics, MobileVit achieved detection metrics above 98% for all channels except ϵ-κlibur-O, demonstrating effective detection. Specific attention was given to ϵ-κlibur and ϵ-κlibur-O. For ϵ-κlibur, the model's classification accuracy was close to 99%.

Although the IPD distribution of ϵ-κlibur is close to that of legitimate channel traffic, differences still exist. We believe that the differences in the construction process, where authors modified di smaller than t using a normal distribution, might be improved by using a Weibull distribution. In the case of ϵ-κlibur-O, the detection accuracy was only 93.75%, making it more likely to be classified as TRCTC and normal channels. We attribute this to the same obstacles encountered by the Snap method when detecting ϵ-κlibur-O. The presence of outliers in ϵ-κlibur-O affects the correlations between values, leading to lower classification accuracy.

4.7 Compare with Other CTC Detection Methods

We compared nine CTC detection methods, as shown in Figure 11. Among them, five are classical methods often used for comparison: ϵ-similarity, K-S, Regularity, Entropy and CEE. These five methods have very low average detection accuracy for the seven channels because they typically work effectively for only one or two channels and require a larger IPD sampling window. In this study, all methods sampled 64 IPDs as a window, limiting their detection performance. Compared to Darwish's hierarchical statistics and deep learning methods (referred to as DNN), their detection accuracy is 86%. DNN's accuracy is lower for the detection of ϵ-κlibur and ϵ-κlibur-O channels, leading to an average accuracy that is not very high. SnapCatch, which extracts image features in a relatively simple way and distinguishes images based on eight statistical values, also has lower average detection accuracy compared to our approach. In comparison to Sun's DC-ACGAN method, although there are similarities in the image feature extraction, the difference in the performance of the image classification network leads to our method achieving higher average accu-

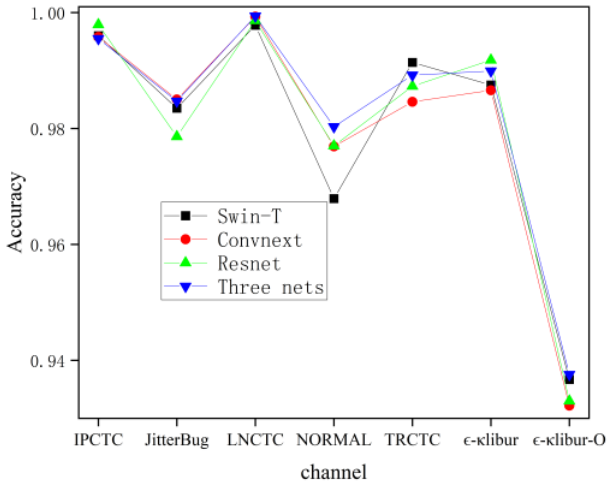


Figure 7: Seven channels accuracy of distilled networks

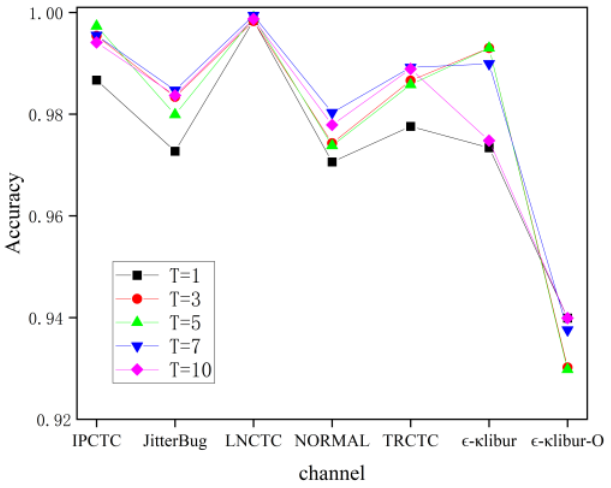


Figure 8: Seven channels accuracy with different T

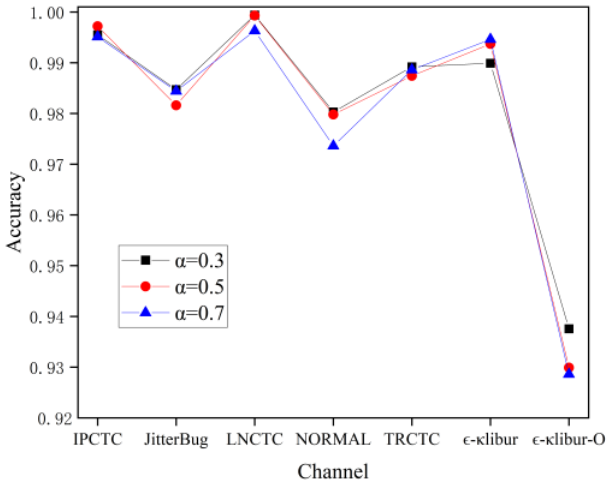


Figure 9: Seven channels accuracy with different α.

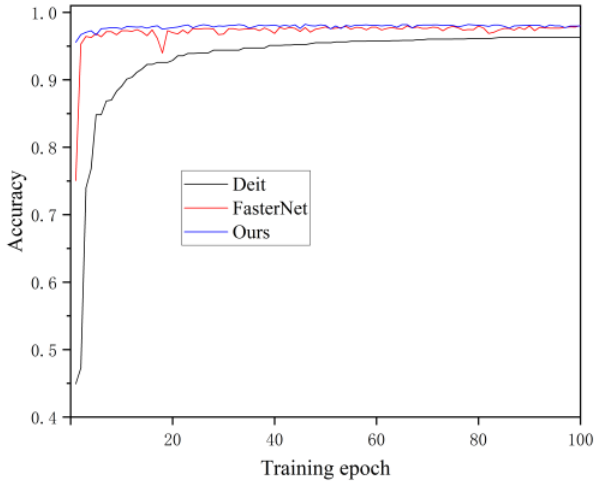


Figure 10: Experimental results compared with Deit and FasterNet

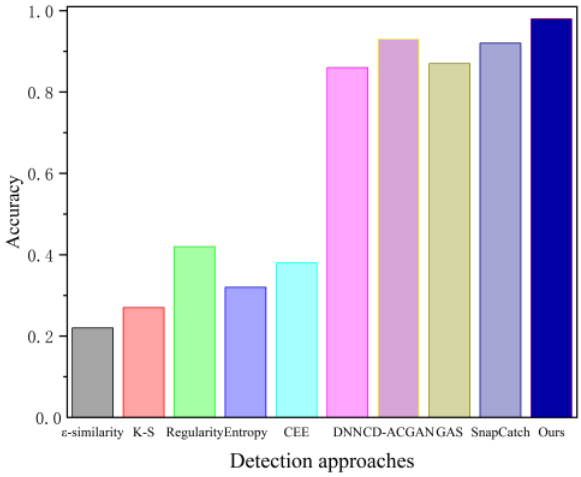


Figure 11: Accuracy of different CTC detection methods

racy. During the restoration phase, GAN network training is unstable, with significant accuracy fluctuations and requiring a longer training period. For the GAS method, because it was originally designed for blind detection, adapting it from binary to multi-class methods resulted in an accuracy of 87%, with lower detection accuracy for ϵ-κlibur and ϵ-κlibur-O channels. In summary, compared to the other eight detection methods, our detection scheme achieves the highest average detection accuracy for each channel.

4.8 Network Params and FLOPs

We employed the thop library in Python to meticulously document the parameters and computational load of the networks utilized in our experiments, as outlined in Table 2. Notably, within the context of this study, the optimized MobieVit model exhibited a significant reduction in parameters, distinguishing itself as the network with the least parameter count and computational load among all the networks investigated.

Table 1: Evaluation indicators of seven channels

Channel Class	Accuracy	Precision	Recall	F1 Score
IPCTC	99.55%	99.49%	99.50%	99.50%
JitterBug	98.47%	99.33%	97.99%	98.66%
LNCTC	99.94%	99.75%	99.90%	99.82%
Normal traffic	98.03%	97.83%	97.08%	97.40%
TRCTC	98.92%	97.25%	99.16%	98.20%
ϵ-κlibur	98.99%	96.08%	98.86%	96.95%
ϵ-κlibur-O	93.75%	98.79%	93.03%	96.46%
Total	98.24%	98.36%	97.93%	98.14%

Table 2: Network Params and FLOPs

Network	Params	FLOPs
Swin-T	27.50	737.61
ConvNext	27.83	364.62
Resnet	21.29	300.27
Deit	5.68	93.06
FasterNet	3.91	29.24
Ours	0.16	14.72

5 Conclusion

In conclusion, this study adopted a novel approach to transforming sequential data into images using GAF-MTF-RP, a three-channel image representation of IPD. The multi-teacher distillation was applied to the MobileVit network for detecting various covert channels. Through parameter tuning, we achieved classification accuracy above 98% for six types of channels, although not as high for ϵ-κlibur-O. However, our approach demonstrates higher generality compared to GAS and Snap, requiring only a detection window size of 64 for high sensitivity. GAS uses 250 IPDs on average to achieve effective detection and Snap uses 256 IPDs. Our distilled MobileVit model outperforms some popular distillation networks in this classification task.

Looking ahead, we aim to enhance the classification performance on ϵ-κlibur-O. Additionally, we plan to investigate the inherent structure of images from normal channels and utilize semi-supervised image classification networks to achieve blind detection capabilities.

References

[1] S. Al-Eidi, O. Darwish, Y. Chen, G. Husari, "Snapcatch: automatic detection of covert timing channels using image processing and machine learning," *IEEE Access*, vol. 9, pp. 177–191, 2020.

[2] S. Al-Eidi, O. Darwish, Y. Chen, M. Maabreh, Y. Tashtoush, "A deep learning approach for detecting covert timing channel attacks using sequential data," *Cluster Computing*, pp. 1–11, 2023.

[3] S. Al-Eidi, O. Darwish, G. Husari, Y. Chen, M. Elkhodr, "Convolutional neural network structure to detect and localize ctc using image processing," in *2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, pp. 1–7. IEEE, 2022.

[4] D. Barradas, N. Santos, L. Rodrigues, V. Nunes, "Poking a hole in the wall: Efficient censorship-resistant internet communications by parasitizing on webrtc," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pp. 35–48, 2020.

[5] Serdar Cabuk. *Network covert channels: Design, analysis, detection, and elimination*. PhD thesis, Purdue University, 2006.

[6] S. Cabuk, C. E. Brodley, C. Shields, "Ip covert timing channels: design and detection," in *Proceedings of the 11th ACM conference on Computer and communications security*, pp. 178–187, 2004.

[7] S. Cabuk, C. E. Brodley, C. Shields, "IP covert channel detection," *ACM Transactions on Information and System Security (TISSEC)*, vol. 12, no. 4, pp. 1–29, 2009.

[8] J. Chen, S. H. Kao, H. He, W. Zhuo, S. Wen, C. H. Lee, and S. H. G. Chan, "Run, don't walk: Chasing higher flops for faster neural networks," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 12021–12031, 2023.

[9] O. Darwish, A. Al-Fuqaha, G. B. Brahim, I. Jenhani, and A. Vasilakos, "Using hierarchical statistical analysis and deep neural networks to detect covert timing channels," *Applied Soft Computing*, vol. 82, p. 105546, 2019.

[10] M. A. Elsadig and A. Gafar, "Covert channel detection: machine learning approaches," *IEEE Access*, vol. 10, pp. 38391–38405, 2022.

[11] S. Gianvecchio and H. Wang, "An entropy-based approach to detecting covert timing channels," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 6, pp. 785–797, 2010.

[12] B. Groza, L. Popa, and P. S. Murvay, "Canto-covert authentication with timing channels over optimized traffic flows for can," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 601–616, 2020.

[13] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 770–778, 2016.

[14] G. Hinton, O. Vinyals, and J. Dean, "Distilling the knowledge in a neural network," *arXiv preprint arXiv:1503.02531*, 2015.

[15] X. Huang, Y. Chen, Z. Li, and T. Zhan, "Detection of network time covert channels based on image processing," in *Proceedings of the 2023 4th International Conference on Computing, Networks and Internet of Things*, pp. 701–707, 2023.

[16] F. Iglesias, V. Bernhardt, R. Annessi, and T. Zseby, "Decision tree rule induction for detecting covert timing channels in tcp/ip traffic," in *Machine Learning and Knowledge Extraction: First IFIP TC 5, WG 8.4, 8.9, 12.9 International Cross-Domain Conference, CD-MAKE 2017, Reggio, Italy, August 29–September 1, 2017, Proceedings 1*, pp. 105–122. Springer, 2017.

[17] H. Li, T. Song, and Y. Yang, "Generic and sensitive anomaly detection of network covert timing channels," *IEEE Transactions on Dependable and Secure Computing*, 2022.

[18] Q. Li, P. Zhang, Z. Chen, and G. Fu, "Covert timing channel detection method based on random forest algorithm," in *2017 IEEE 17th International Conference on Communication Technology (ICCT)*, pp. 165–171. IEEE, 2017.

[19] Z. Li, Y. Chen, Z. Teng, and X. Huang, "Contra: A covert timing channel detection approach for little covert information in a network," in *Proceedings of the 2023 4th International Conference on Computing, Networks and Internet of Things*, pp. 614–620, 2023.

[20] C. Liang, T. Baker, Y. Li, R. Nawaz, and Y. A. Tan, "Building covert timing channel of the iot-enabled mts based on multi-stage verification," *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[21] A. Liu, J. Chen, and H. Wechsler, "Real-time covert timing channel detection in networked virtual environments," in *Advances in Digital Forensics IX: 9th IFIP WG 11.9 International Conference on Digital Forensics, Orlando, FL, USA, January 28-30, 2013, Revised Selected Papers 9*, pp. 273–288. Springer, 2013.

[22] Z. Liu, Y. Lin, Y. Cao, H. Hu, Y. Wei, Z. Zhang, S. Lin, and B. Guo, "Swin transformer: Hierarchical vision transformer using shifted windows," in *Proceedings of the IEEE/CVF international conference on computer vision*, pp. 10012–10022, 2021.

[23] Z. Liu, H. Mao, C. Y. Wu, C. Feichtenhofer, T. Darrell, and S. Xie, "A convnet for the 2020s," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pp. 11976–11986, 2022.

[24] S. Lu, Z. Chen, G. Fu, and Q. Li, "A novel timing-based network covert channel detection method," in *Journal of Physics: Conference Series*, vol. 1325, p. 012050. IOP Publishing, 2019.

[25] W. Mazurczyk and L. Caviglione, "Information hiding as a challenge for malware detection," *arXiv preprint arXiv:1504.04867*, 2015.

[26] S. Mehta and M. Rastegari, "Mobilevit: light-weight, general-purpose, and mobile-friendly vision transformer," *arXiv preprint arXiv:2110.02178*, 2021.

[27] A. Mileva, A. Velinov, L. Hartmann, S. Wendzel, and W. Mazurczyk, "Comprehensive analysis of mqtt 5.0 susceptibility to network covert channels," *Computers & security*, vol. 104, p. 102207, 2021.

[28] S. Mou, Z. Zhao, S. Jiang, Z. Wu, and J. Zhu, "Feature extraction and classification algorithm for detecting complex covert timing channel," *Computers & Security*, vol. 31, no. 1, pp. 70–82, 2012.

[29] A. Mukherjee, "On the dynamics and significance of low frequency components of internet load," 1992.

[30] M. E. Newman, "Power laws, pareto distributions and zipf's law," *Contemporary physics*, vol. 46, no. 5, pp. 323–351, 2005.

[31] V. Paxson and S. Floyd, "Wide area traffic: the failure of poisson modeling," *IEEE/ACM Transactions on networking*, vol. 3, no. 3, pp. 226–244, 1995.

[32] F. Rezaei, M. Hempel, and H. Sharif, "Towards a reliable detection of covert timing channels over real-time network traffic," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 3, pp. 249–264, 2017.

[33] S. H. Sellke, C. C. Wang, S. Bagchi, and N. Shroff, "TCP/IP timing channels: Theory to implementation," in *IEEE INFOCOM 2009*, pp. 2204–2212. IEEE, 2009.

[34] G. Shah, A. Molina, M. Blaze, *et al.*, "Keyboards and covert channels.," in *USENIX Security Symposium*, vol. 15, p. 64, 2006.

[35] R. Sharma, A. Guleria, and R.K. Singla, "An overview of flow-based anomaly detection," *International Journal of Communication Networks and Distributed Systems*, vol. 21, no. 2, pp. 220–240, 2018.

[36] P. L. Shrestha, M. Hempel, F. Rezaei, and H. Sharif, "A support vector machine-based framework for detection of covert timing channels," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 2, pp. 274–283, 2015.

[37] C. Sun, Y. Chen, H. Tian, and S. Wu, "Covert timing channels detection based on auxiliary classifier generative adversarial network," *IEEE Open Journal of the Computer Society*, vol. 2, pp. 407–418, 2021.

[38] S. Taheri, M. Mahdavi, and N. Moghim, "A dynamic timing-storage covert channel in vehicular ad hoc networks," *Telecommunication Systems*, vol. 69, pp. 415–429, 2018.

[39] T. Tao, "Benford's law, zipf's law, and the pareto distribution," *Retrieved from*, 2009.

[40] H. Touvron, M. Cord, M. Douze, F. Massa, A. Sablayrolles, and H. Jégou, "Training data-efficient image transformers & distillation through attention," in *International conference on machine learning*, pp. 10347–10357. PMLR, 2021.

[41] S. Vanderhallen, J. Van Bulck, F. Piessens, and J. T. Mühlberg, "Robust authentication for automotive control networks through covert channels," *Computer Networks*, vol. 193, p. 108079, 2021.

[42] L. Wang and Y. Chen, "A perceptual hash-based approach to detect covert timing channels.," *Int. J. Netw. Secur.*, vol. 22, no. 4, pp. 686–697, 2020.

[43] Z. Wang, T. Oates, *et al.*, "Encoding time series as images for visual inspection and classification using tiled convolutional neural networks," in *Workshops at the twenty-ninth AAAI conference on artificial intelligence*, vol. 1. AAAI Menlo Park, CA, USA, 2015.

[44] S. Wendzel, F. Link, D. Eller, and W. Mazurczyk, "Detection of size modulation covert channels using countermeasure variation.," *J. Univers. Comput. Sci.*, vol. 25, no. 11, pp. 1396–1416, 2019.

[45] S. Wu, Y. Chen, H. Tian, and C. Sun, "Detection of covert timing channel based on time series symbolization," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 2372–2382, 2021.

[46] X. Zhang, L. Zhu, X. Wang, C. Zhang, H. Zhu, and Y. Tan, "A packet-reordering covert channel over volte voice and video traffics," *Journal of Network and Computer Applications*, vol. 126, pp. 29–38, 2019.

[47] S. Zillien and S. Wendzel, "Weaknesses of popular and recent covert channel detection methods and a remedy," *IEEE Transactions on Dependable and Secure Computing*, 2023.

Biography

Xuwen Huang was born in Jiangxi province, China in 1998. Between 2016 and 2020, he majored in software engineer with East China Jiaotong University School of Science and Technology, Nanchagn, China. He reveived the bachelor's degree in engineering. He is currently working toward the M.S degree with Huaqiao University, Xiamen, China. His research interests include: cyber security, machine learning and time series analysis.

Yonghong Chen received his Ph.D. degree in engineering, from the School of Automation of Chongqing University in July 2005. From September 2006 to October 2007, he went to Kyoto University, Japan as an academic visitor for one year. Now he is a professor and master's tutor of Huaqiao University. He is mainly engaged in the research of computer network and information security, mobile Internet technology, Internet of things technology, technology integration of mobile communication and Internet of things, network and information security.

Xiaolong Zhuang was born in Quanzhou, China in 1999. He obtained a Bachelor's degree in Software Engineering from Jinling College, Nanjing University. He is currently pursuing a master's degree at Quanzhou Overseas Chinese University in China. His main research direction is covert channel detection and the use of perceptual hashing.

Yuwei Lin was born in Fujian province, China in 1997. He received his Bachelor's degree in Engineering from Qing Gong College, North China University of Science and Technology. He is currently pursuing a master's degree at Huaqiao University. His main research interests are network security and network covert channel detection.

Transformer-based Image Super-Resolution Defense Against Adversarial Attacks

Zi-Han Liu

(Corresponding author: Zi-Han Liu)

School of Control and Computer Engineering, North China Electric Power University
Beijing 102206, China
Email: 374047390@qq.com

(Received Mar. 28, 2023; Revised and Accepted Nov. 22, 2023; First Online Feb. 23, 2024)

Abstract

The security issue that deep learning models are vulnerable to adversarial example attacks carefully designed by attackers has attracted people's attention. There is a lot of research on adversarial attack defense methods, but the existing defense methods have the problem of poor versatility. They have a good defense against specific attacks but have poor defense effects or even no defense against other attacks. We propose a general Transformer-based super-resolution network defense method. Our method uses Transformer's self-attention mechanism to dynamically add high-frequency information for different regions in the image to improve image quality. To reduce the impact of adversarial perturbation on the image, we remove the perturbation on the image through multi-scale feature fusion. In addition, to reduce weight, our network uses a diversified window division to establish long-distance dependence between each pixel in the image and the entire feature map, effectively reducing the computational cost of the model. Many experiments have proved that in the face of different types of attacks, our method has an average defense success rate of about 90%, exceeding all advanced baseline defense methods, and is better than existing defense methods based on super-resolution.

Keywords: Adversarial Attacks; Deep Learning; Image Super-resolution; Universal Defense

1 Introduction

In recent years, deep learning has been widely used in image classification, speech recognition, target detection and other fields. It shows outstanding performance and plays a vital role in key tasks in industrial production. At the same time, the security of deep neural networks has received more and more attention. Szegedy *et al.* [26] found that deep neural networks are vulnerable to adversarial example attacks. Adversarial examples add perturbation information imperceptible to the human eye to the original image, and the adversarial examples make the neural network misjudgment. The security problems of deep learning technology have hindered its development and application in specific application fields in real life, such as automatic driving [27], face recognition system [25], etc. How to design efficient defense methods to improve the robustness of deep learning models is very important.

There have been a lot of adversarial attack research work. According to the generation principle of adversarial examples, the generation methods can be mainly divided into based on direct optimization, based on gradient optimization, based on decision boundary analysis and based on generative neural networks. Among them, the method based on direct optimization is to use the algorithm to directly optimize the objective function, which generates less adversarial perturbation, such as: Box-constrained L-BFGS [17] attack, C&W [2] attack, etc. The attack method based on gradient optimization is to add perturbation to the input example in the direction of the model loss function to make the model classification error. This kind of method is simple to implement and has a high success rate of white-box attack, such as FGSM(Fast Gradient Sign Method) [9], I-FGSM(Iterative Fast Gradient Sign Method) [13], PGD(Project Gradient Descent) [18], MI-FGSM(Momentum Iterative Fast Gradient Sign Method) [7], etc. The method based on decision boundary analysis is to gradually reduce the distance between the example and the decision boundary of the model to make the model classification error, such as: DeepFool [20] attack, UAPs [19] attack, etc. The attack method based on the generative neural network is to generate adversarial examples by training the neural network in a self-supervised manner. This type of method can efficiently generate a large number of adversarial examples with high transferability capabilities, such as ATN [1], UAN [11].

With the research on adversarial attacks, some effective defense methods have been proposed, which can be roughly divided into two types: adversarial training and data preprocessing. Adversarial training is currently considered to be one of the most effective defense methods.

It was first proposed by Szegedy *et al.* [26], who used adversarial examples as training data for model training, so that the trained model has a certain against attack ability and achieve high robustness. Madry *et al.* [18] converted the form of adversarial training into a process of external minimization and internal maximization, and minimized the loss function by optimizing model parameters. Adversarial training has certain limitations. It is better at defending against known attacks, but poor at defending against unknown attacks or even unable to defend against them. Adversarial training cannot completely eliminate adversarial examples and requires a large investment.

Defense methods based on data preprocessing modify the input of the model, such as JEPG compression [8], denoiser HGD [15], ComDefend image compression [12] and super-resolution network EDSR [16]. Among them, the super-resolution network EDSR defense method first uses wavelet denoising to reduce the perturbation information on the image, and then adds high-frequency information to the image through a single-image super-resolution network EDSR to improve the visual quality. But EDSR suffers from a fundamental problem in convolutional models that the interaction between the image and the convolutional Kernel is content-independent. It uses the same convolution kernel to restore high-frequency information in different image regions, and the convolution cannot make the feature map establish long-distance dependence.

In order to solve the above problems, we propose a general Transformer-based super-resolution network UDSR, which uses the Transformer's self-attention mechanism to perform self-attention [28] calculations between pixels. In this way, high-frequency information can be dynamically restored to different regions of the image. Through different window division methods, each pixel can establish a long-distance dependence with the entire feature map, which can effectively reduce the calculation cost and improve the image quality. Our method can more effectively defend against adversarial attacks. The main contributions of this research method are as follows:

1) Our approach introduces Transformers into the problem of defense against attacks. We designed a super-resolution network architecture UDSR, which makes the network model more lightweight by adopting a variety of window division methods. Our method can effectively add high-frequency information of images and improve the robustness of classification networks.

2) Our method uses multi-scale feature fusion. By fusing three different scale feature maps, it can effectively reduce the impact of perturbation on the image, and effectively improve the defense success rate in the face of different types of attacks.

3) A large number of experiments have proved that compared with other advanced defense methods, our defense method can significantly improve the defense success rate; compared with other super-resolution-based defense methods, our method has the best defense performance.

2 Related Work

The image after the attacker adds carefully calculated perturbations is called adversarial examples, and the attack on CNN is called adversarial attack. Adversarial examples can cause DNN to output wrong classification results with high confidence.

In an image classification task, consider a deep learning model $f(x) = y^{true}, x \in R^m$ as input to the model, $y^{true} \in R$ is the correct output of the model for the current input. The adversarial attack is that the attacker adds carefully calculated perturbation r to the original input image x. In the untargeted attack, the attacker intends to make$f(x+r) \neq y^{true}$. In the targeted attack, the attacker intends to make$f(x+r) = y^t$, y^t is the target class for the attacker, $x+r$ represents an adversarial example. The added perturbation is a small value, which is imperceptible to the human eyes, and is usually limited by l_0, l_1, l_∞. In targeted attacks, the optimization problem for generating adversarial examples is given by the Equation (1):

$$\begin{aligned} \min \quad & \|r\|_2 \\ \text{s.t.} \quad & 1. f(x+r) = y^t \\ & 2. x + r \in R^m \end{aligned} \tag{1}$$

2.1 Adversarial Attack

The adversarial attack is that the attacker adds a carefully calculated perturbation to the original input image. Adversarial attacks can deceive the deep learning model and make the deep learning model misjudgment. Since the deep neural network is in a high-dimensional linear space, even very small disturbances are continuously accumulated through the forward propagation process of the neural network, and finally act on the activation function, which has a greater impact on the classification results. Researchers have proposed a variety of attack methods, and we will introduce the following attack methods.

2.1.1 L-BFGS

Szegedy *et al.* first proposed the L-BFGS [26] algorithm to directly optimize the objective function to generate adversarial examples, and use the Lange relaxation method to transform the constraints of $f(x+r) = y^t$ into $loss_f(x+r, y^t)$ for optimization. The optimization objectives are as follows:

$$Minimize\, ||r||_2 + loss_f(x+r, y^t) s.t. x + r \in [0,1]^m \tag{2}$$

2.1.2 FGSM

The FGSM [9] algorithm generates an adversarial perturbation in the gradient direction of the loss function, and adds the perturbation to the image to achieve the purpose of making the model misclassify. θ represents the network

parameters of the model, $L(x, y^{true}; \theta)$ represents the loss function of the model. x, y^{true} represent the original input image and the ground truth label. The process of FGSM generating adversarial examples is shown in Equation (3), where $\nabla x L(x, y^{true}; \theta)$ represents the direction of the gradient of the model loss function, and ϵ represents the maximum value of the adversarial perturbation. Since FGSM is a single-step attack, the attack success rate is low.

$$x_{t+1}^{adv} = Clip_x^{\epsilon}\{x_t^{adv} + \alpha \cdot sign(\nabla x L(x, y^{true}; \theta)\} \quad (3)$$

2.1.3 I-FGSM

Kurakin *et al.* proposed the iterative FGSM algorithm (Iterative Fast Gradient Sign Method, I-FGSM) [13], which reduces the optimization interval and divides the perturbation into multi-step calculations. The calculation method of I-FGSM is shown by Equation (4) and Equation (5), where the $Clip(\cdot)$ operation clips the image within the legal range. The disadvantage of I-FGSM is that it is easy to fall into local extrema.

$$x_0^{adv} = x \quad (4)$$

$$x_{t+1}^{adv} = Clip_x^{\epsilon}\{x_t^{adv} + \alpha \cdot sign(\nabla x L(x, y^{true}; \theta)\} \quad (5)$$

2.1.4 MI-FGSM

Dong *et al.* proposed the (Momentum Iterative Fast Gradient Sign Method, MI-FGSM) algorithm [7], which introduced momentum technology into the process of generating adversarial samples. This method stabilizes the direction of gradient updating, avoids local extreme value in the direction of loss function gradient. MI-FGSM has great transferability. The MI-FGSM algorithm is shown in Equation (6) and Equation (7), where μ represents the decay factor of the momentum item, and g_{t+1} is the accumulated gradient at iteration t.

$$g_{t+1} = \mu \cdot g_t + \frac{\nabla x L(x_t^{adv}, ytrue; \theta)}{||\nabla x L(x_t^{adv}, ytrue; \theta)||_1} \quad (6)$$

$$x_{t+1}^{adv} = Clip_x^{\epsilon}\{x_t^{adv} + \alpha \cdot sign(g_{t+1})\} \quad (7)$$

2.2 Defending Against Adversarial Samples

Adversarial examples seriously threaten the security of deep learning models, leading people to question the reliability of deep learning models in some specific application fields. With the development of research on adversarial attacks, some effective adversarial attack defense methods have been continuously proposed. The defense methods can be roughly divided into two types: adversarial training and data preprocessing.

2.2.1 Data Preprocessing

The basic idea of data preprocessing is to destroy the added adversarial perturbation by applying transformation to the adversarial examples, so as to eliminate the influence of perturbation and improve the accuracy of the classifier. Dziugaite *et al.* [8] found that JEPG compression of input data can effectively reduce the threat of adversarial perturbation. DNN is a high-dimensional network topology. Even very small differences will be amplified after DNN processing, which will have a huge impact. Therefore, even the residual noise after image denoising processing will have an impact on the classification accuracy of the deep learning model. Liao *et al.* proposed the High Level Representation Guided Denoiser (HGD) [15] defense method to solve the problem of residual noise amplification. Data preprocessing methods can effectively reduce the impact of adversarial perturbation, but cannot completely remove the impact of adversarial perturbation. Compared with the image super-resolution network EDSR proposed by Aamir Mustafa [21] for adversarial attack defense, our Transformer-based image super-resolution network UDSR can better restore the high-frequency information of the image and "purify" adversarial perturbation more effectively. In addition, UDSR does not need to denoise the image in advance, and can generate high-resolution images end-to-end.

2.2.2 Adversarial Training

The basic idea of adversarial training is to add adversarial examples to the training set to improve the accuracy of the model. Adversarial training can be regarded as an optimization problem of internal maximization and external minimization, as shown in Equation (8) and Equation (9).

$$\min_{\theta} \rho(\theta) \quad (8)$$

$$\rho(\theta) = E_{(x,y)\sim D}[\max_{\theta} L(\theta, x + r, y^{true})] \quad (9)$$

The internal max process maximizes the loss function of the model and finds the most suitable perturbation to generate adversarial examples; the external min process is to train the model to find suitable network parameters θ, so that the model has a certain anti-interference ability. The difference between different adversarial training is the way to generate training data, so the model has a problem of data set dependence. We can improve the generalization ability of the model through knowledge transfer technology.

The super-resolution network defense method we proposed can effectively add corresponding high-frequency information to different regions of the image in the face of different adversarial attack methods, improve image quality, and improve the accuracy of image classification. At the same time, our super-resolution network combines the feature maps of three different scales of the picture to extract features, which can reduce the impact of disturbance on the picture from different dimensions. Our method can well remove the perturbation information in the picture even in the face of unknown attacks.

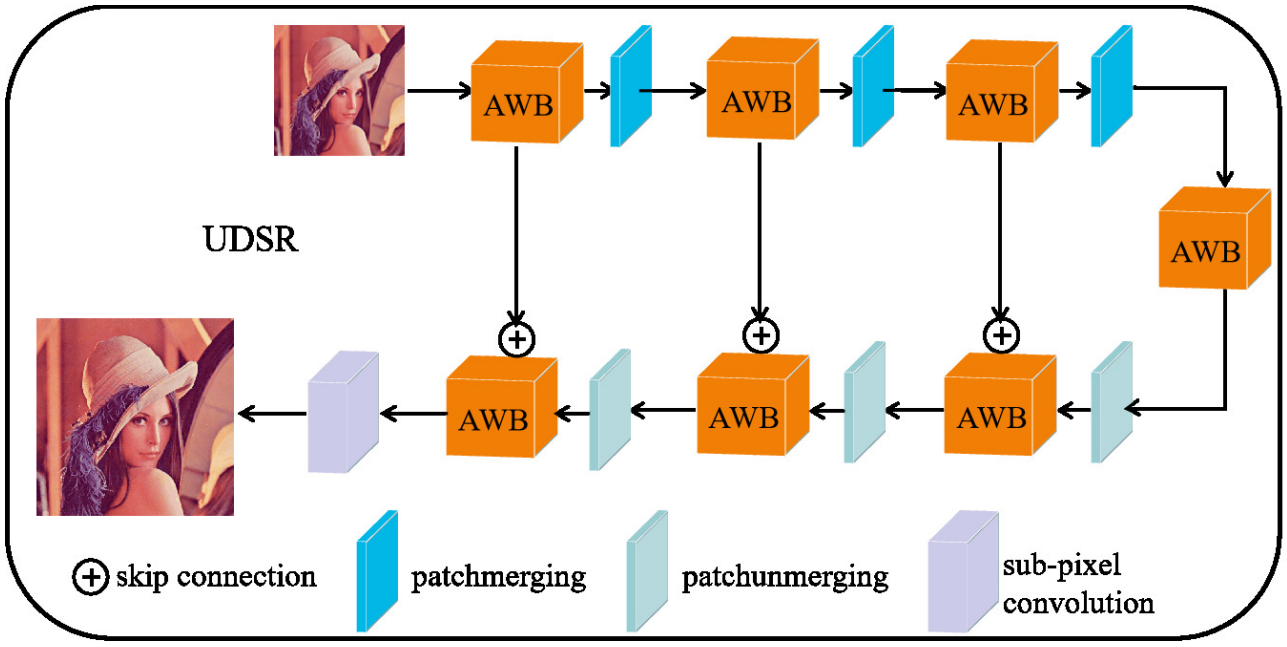


Figure 1: Structure of UDSR

2.3 Image Super-Resolution

Single Image Super-Resolution(SISR) is a classic problem in computer vision and image processing. The goal is to reconstruct a high resolution(HR) image from its low resolution(LR) observation. The process is represented by Equation (10), where f_{SR} is the super-resolution network, $I_{LR} \in R^{H\times W\times 3}$ is the low-resolution image, H and W is the width and height of the low-resolution image, $I_{HR} \in R^{SH\times SW\times 3}$ is the high-resolution image, and S is the image enlargement scale.

$$L_{HR} = f_{SR}(L_{LR}) \tag{10}$$

High-resolution images can improve the accuracy of deep learning model image classification and target detection. It plays a very important role in specific industries, such as high-resolution medical images, high-resolution satellite images, etc.

3 Method

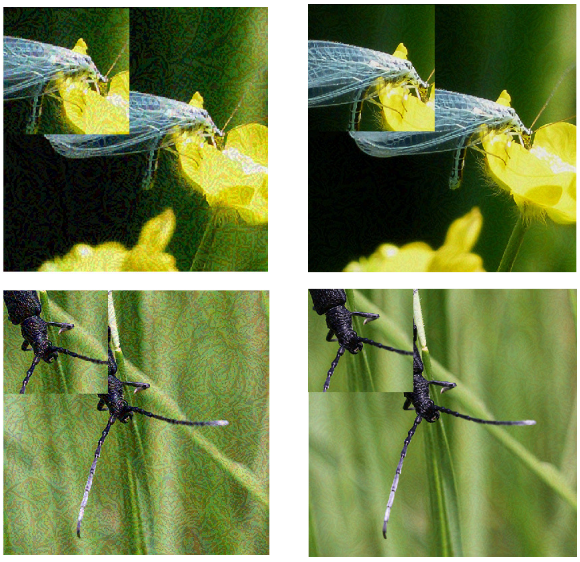
For the perturbation information of different adversarial examples, we designed a general Transformer-based super-resolution network UDSR(UNet Defense Super Resolution), as shown in Figure 1. UDSR uses the UNet architecture for multi-scale feature fusion, in which the encoding and decoding adopt symmetrical Structure. UDSR feature extraction is mainly done by AWB(Axial Window Block). In the encoding part, after merging the feature maps, the scale of the feature maps was reduced to half of the original one, and the number of channels was increased to two times. In the decoding part, after the feature map is expanded, its scale becomes twice as large as the original one, and the number of channels of the image is reduced to half of the original one. Since the calculation amount of Transformer is quadratic with the number of feature map pixels, in order to reduce the calculation amount, Our AWB adopts a diversified window division method, so that the self-attention calculation is only performed inside the window, which can significantly reduce the computational cost. AWB consists of HARL(H Axial Residual Layer), WARL(W Axial Residual Layer) and RB(Residual Block). The self-attention calculation method of HARL and WARL is shown in Figure 4.1(b). The calculation methods of Q, K and V matrices used in the self-attention calculation are shown in Equation (11) - Equation (13), where P_1, P_2 and P_3 are projection matrices sharing weights between different windows, and X is feature maps divided windows.

$$Q = XP_1 \tag{11}$$
$$K = XP_2 \tag{12}$$
$$V = XP_3 \tag{13}$$

The feature map obtained by self-attention calculation inside the window is shown in Equation (14). When our method is performing self-attention calculation, the number of channels of the feature map is divided into d parts on average, and executed d times in parallel Self-attention calculation, which can make different parts of the feature map focus on the details in different channels while reducing the amount of calculation.

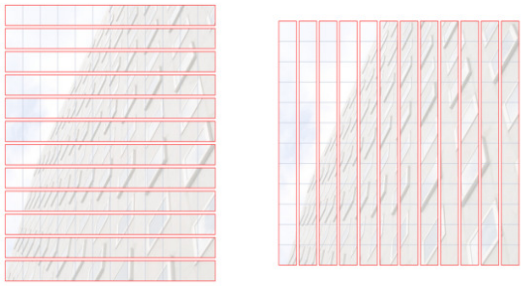
$$Attention(Q, K, V) = Softmax(QK^T\sqrt{d})V \tag{14}$$

As shown in the green area in Figure 4.1(a), RB is composed of a convolution with a convolution kernel of 3 and an activation function(ReLU). Using convolution can effectively extract the adjacent information of each pixel, so that the model has local information processing ability. HARL and WARL in AWB use different window parti-



(a) Adversarial examples (b) SR examples

Figure 2: Super-resolution examples and adversarial examples



(a) HARL (b) WARL

Figure 3: The partition of window

tion methods. HARL and WARL divide the feature map into strip windows in H and W directions, as shown in Figure 4.1(a) and Figure 4.1(b). According to CSWin Transformer [6], after the self-attention calculation of the feature map in the strip window in two directions, each pixel can establish a global dependency with all the information of the entire feature map, which effectively reduces the computational cost of the model. After combining the feature maps of three different scales, our method can well remove the perturbation information in the image and reduce the impact of adversarial attacks on the image. After the feature extraction of AWB, our method can add high-frequency information missing from images in the channel dimension Finally, the image undergoes a sub-pixel convolution [24] to supplement the high-frequency information into the pixel space of the image to complete the super-resolution of the image.

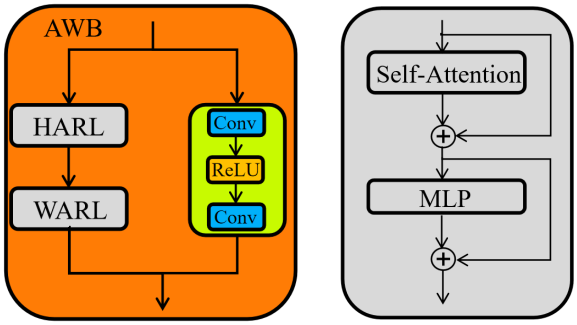
The Transformer-based UDSR method we proposed enables each pixel to perform self-attention calculations inside the window. In this way, high-frequency information can be dynamically added to different regions effectively. After the image is processed by HARL and WARL in AWB, each pixel can establish a long-distance dependence with the entire feature map, making the added high-frequency information clearer and more effective. At the same time, UDSR uses feature map fusion and expansion to extract features of three different scales. After the feature map is down-exampled, the perturbation information of the image can be effectively removed. According to the previous research [21], the perturbation generated by the adversarial attack has a greater impact on the high-frequency information of the image. Our method UDSR improves the image quality by adding high-frequency information and removing disturbance information, which improves the accuracy of the deep learning model.

4 Experiment

4.1 Experiment Setup

Experimental hardware and software platform: Our UDSR network architecture is written in pytorch. The data set is DF2K(DIV2K+Flickr2K), with a total of 3350 training images. The low-resolution images are obtained by bicubic downsampling of high-resolution images, and some of the low-resolution images are countermeasures after adding disturbances. The paired high-resolution images are clean examples with no perturbation added. The GPUs used for model training are 4 GeForce RTX 2080Ti, and the training time is 3 days.

Dataset: The experiment uses 5000 ILSVRC [5] datasets and 1000 NIPS [13] 2017 adversarial attack and defense competition datasets. The ILSVRC dataset selected in the experiment has achieved 100% top-1 accuracy on each model. The NIPS 2017 data set



(a) Axial-Window Block (b) Structure of SA

Figure 4: Structure of AWB and SA(Self-attention)

is collected by Google Brain, where the example size is 299×299, and the classification accuracy rate is 95.9% on the Inc-v3 model.

Model: In the experimental part, the defense success rate is tested in the three classifiers Inception-v3(Inc-v3), ResNet-50(Res-50) and Inception-ResNet-v2(IncRes-v2). The above three models are all Pre-trained models obtained in TensorFlow's GitHub repository: https://github.com/tensorflow/models/tree/master/rese arch/slim.

Attack: To demonstrate the generality of our UDSR defense method against various attacks, FGSM [9], I-FGSM [13], MI-FGSM [7], PGD [18], L-BFGS [17], C&W [2], JSMA [22], DeepFool [20], ZOO [3], DI^{2}FGSM [30], MDI^{2}FGSM [30], a total of eleven attack methods. For FGSM, set and two attack methods, for iterative attack, the maximum perturbation is set to 16. All the above attacks are based on defenseless models to generate adversarial examples.

Defense methods: We selected five defense methods as comparison algorithms in our experiments, namely JPEG compression [4], R&P [29], TVM+ Image Quilting [10], Pixel Deflection [23], Wavelet Denoising+EDSR [21]. Among them, JEPG compression [] of the input data in can effectively reduce the threat of adversarial perturbation; R&P uses a randomized method for adversarial training, including two random operations: random transformation scale size and random filling. R&P can adapt Different network structure models. TVM+Image Quilting achieves the purpose of defense through splicing, variance minimization and other operations. Pixel Deflection sets a denoising module on the high-level feature map of the network to promote the shallow network to better learn "clean" features. Wavelet denoising + EDSR [21] first uses wavelet transform to denoise the image, and then adds high-frequency information to the image through a single image super-resolution network EDSR to improve the visual quality, and defend against adversarial attacks in this way.

4.2 Comparison for Defense Effects of Different Defense Methods

Due to the limited ability of wavelet denoising to reduce image perturbation information, out method considers combining multi-scale features and feature extraction to restore clear images, which will effectively restore image high-frequency information in the face of various perturbations. We conducts experiments on 5000 ILSVRC datasets, and the effects of adversarial examples and super-resolution examples are shown in Figure 3. It can be clearly seen that the UDSR proposed in this paper can effectively remove the perturbation information in the adversarial example, and adding high-frequency details can improve the image quality and help to improve the robustness of the classification network.

Table 1 shows the defense success rate of different defense methods against different attacks. The defense success rate is defined as the classification accuracy of the image processed by the defense model. It can be seen that on the defenseless model, the defense success rate in the face of various attack methods is low. It shows that the classification network is misclassified with a very high confidence in the face of adversarial sample attacks. In the face of different attack methods, the defense success rate of UDSR proposed in this paper is 2.28% higher than that of using wavelet denoising + EDSR in literature . The defense success rate of our method UDSR exceeds all baselines. UDSR can effectively remove perturbation information generated by different attacks. For C&W attacks and DeepFool attacks, TVM+ Image Quilting and Pixel Deflection have achieved similar performance, and successfully resisted about 90% of the attacks. Our UDSR super-resolution defense method has an average defense success rate of 96%. In the face of strong attacks MDI2FGSM, TVM+Image Quilting and JPEG compression have a very low defense success rate of about 1%, while our UDSR has a defense success rate of 39% on IncRes-v2. Experiments have proved that our method UDSR can effectively "purify" the perturbation information in the adversarial examples, effectively reduce the impact of adversarial attacks on image quality, and improve the accuracy of the classification network.

4.3 Impact of Different Defense Methods on Clean Images

This section mainly analyzes the impact of UDSR and other defense methods on the accuracy of clean example identification. The experimental results are shown in Table 2. In order to resist adversarial attacks, various high-performance defense methods have been proposed. The defense method has a good defense effect, but it will sacrifice a certain degree of clean sample classification accuracy. It can be seen from Table 2 that after the clean samples of different data sets are processed by other defense methods, the performance of the classification model has declined, but after the clean samples are processed by

Table 1: Comparison of Defense Effects of Different Defense Methods (%)

Model	Clean Images	FGSM-2	BIM	MI-FGSM	PGD	L-BFGS	C&W	JSMA	DeepFool	ZOO	MDI^{2}FGSM
No Defense											
Inc-v3	100.0	31.7	11.4	1.7	1.1	0.3	0.8	0.8	0.4	1.0	0.6
Res-50	100.0	12.2	3.4	0.4	0.2	0.1	0.1	0.2	1.0	0.8	0.2
IncRes-v2	100.0	59.4	21.6	0.5	0.3	0.1	0.3	0.1	0.1	0.8	0.6
JPEG Compression											
Inc-v3	96.0	62.3	77.5	69.4	68.1	76.5	80.5	78.8	81.2	80.2	1.3
Res-50	92.8	57.6	74.8	70.8	65.3	77.9	81.3	76.3	77.3	76.9	0.4
IncRes-v2	95.5	67.0	81.3	72.8	66.2	79.4	83.1	81.6	83.9	82.9	1.1
R&P											
Inc-v3	97.3	69.2	53.2	89.5	88.5	89.1	89.5	88.2	88.9	87.3	5.8
Res-50	92.5	66.8	88.2	88.0	87.2	86.6	87.5	86.3	90.9	88.9	4.2
IncRes-v2	98.7	70.7	87.5	88.3	86.8	85.1	88.0	85.6	89.7	87.9	5.3
TVM+ Image Quilting											
Inc-v3	91.9	71.1	90.9	90.1	90.0	90.2	90.4	87.9	88.1	87.1	21.9
Res-50	92.7	84.6	91.2	89.6	88.5	89.9	91.7	88.6	90.3	89.9	29.5
IncRes-v2	92.1	78.2	91.3	89.8	89.2	88.4	89.7	86.1	88.9	86.2	24.6
Wavelet Denoising+EDSR											
Inc-v3	97.0	94.2	96.2	95.9	95.1	95.2	96.0	95.1	96.1	95.6	31.7
Res-50	93.9	86.1	92.3	92.0	92.3	92.6	93.1	92.1	91.5	90.1	31.9
IncRes-v2	98.2	95.3	95.8	95.0	94.3	95.6	95.6	94.8	96.0	95.7	35.6
UDSR(ours)											
Inc-v3	99.3	94.5	97.9	97.6	96.3	97.6	96.8	96.8	96.3	95.6	36.4
Res-50	94.6	90.1	95.7	95.8	93.6	95.1	94.6	94.7	94.5	93.6	37.6
IncRes-v2	98.9	96.4	96.6	96.8	96.9	96.7	97.7	95.5	97.1	95.9	42.8

our method UDSR, the average classification error rates of the classification model are only 2.73% and 3.56% on the two datasets, which is lower than all advanced baseline defense methods. This is due to the fact that our method UDSR uses clean samples as part of the training set during training, so that images without disturbance information are added with clearer high-frequency information after UDSR super-resolution. In this way, the classification model has a lower impact on the recognition accuracy of clean samples processed by UDSR.

4.4 Comparison of Defensive Effects with Various Super-resolution Techniques

Image super-resolution maps images from low-resolution space to high-resolution space. Different super-resolution networks have different mapping capabilities. In this paper, we compare UDSR with representative super-resolution networks SR-ResNet [14] and EDSR [16]. For different attack methods, we conducted experiments on the Inc-v3 network. The experimental results are shown in Table 3. It can be found that our method UDSR has a better defense effect than the convolution-based super-resolution network SR-ResNet and EDSR. Our method Transformer-based UDSR can establish a global dependency between each pixel and all the information of the entire feature map, which can effectively restore the global and local high-frequency details of the image. Our method combines feature maps of 3 scales for each image to reduce the influence of perturbation information on the image, so that the classification network can classify more accurately. Compared with literature [21], literature [21] first uses wavelet denoising to preprocess the image for denoising, and then uses EDSR to super-resolution the example, while our method UDSR does not require denoising preprocessing. In addition, the parameter volume of our method UDSR is 26M, which is much smaller than the 43M parameter volume of EDSR. It shows that our method UDSR can save more computing and storage costs.

5 Conclusion

Adversarial attacks will seriously damage the security of deep learning models. Existing defense methods have poor versatility. In order to ensure the generality of defense methods, we propose a general super-resolution network UDSR defense method. Our method uses Transformer's self-attention mechanism dynamically adds high-frequency information to different regions in the image and remove perturbations on images by multi-scale feature fusion, which reduce the impact of anti-perturbation on the image. After UDSR super-resolution processing, the disturbance information of the adversarial samples is significantly reduced, the high-frequency details are significantly increased, and the image quality is significantly improved. In addition, our method uses a diversified window division method to enable the feature map to establish long-distance dependencies while reducing the computational cost of the model. Compared with other advanced defense methods, our defense strategy has

Table 2: The recognition accuracy of clean examples processed by different defense methods(%)

Data Set	Model	No Defense	JPEG	R&P	Image Quilting	Pixel Deflection	EDSR	UDSR
ILSVRC	Inc-v3	100.0	96.0	97.3	96.2	91.9	97.0	99.3
	Res-50	100.0	92.8	92.5	93.1	92.7	93.9	94.6
	IncRes-v2	100.0	95.5	98.7	95.6	92.1	98.2	98.9
NIPS-DEV	Inc-v3	95.9	89.7	92.0	88.8	86.5	90.9	92.6
	Res-50	98.9	86.9	90.6	85.6	87.8	86.9	97.2
	IncRes-v2	99.4	94.5	98.9	87.9	88.9	92.9	99.5

achieved the optimal defense effect for different types of attacks. It has the least impact on the classification accuracy of clean samples. Compared with other defense methods based on super-resolution, our method UDSR network defense effect is more significant.

Table 3: Comparison of various super-resolution techniques(%)

Attack method	No Defense	SR-ResNet	EDSR	UDSR
Clean Imgae	100.0	94.0	96.2	99.3
FGSM-2	31.7	89.5	92.6	94.5
FGSM-10	30.5	69.9	73.3	86.3
I-FGSM	11.4	93.4	95.9	97.9
MI-FGSM	1.7	92.6	95.2	97.6
PGD	1.1	91.5	93.4	96.3
L-BFGS	0.3	92.1	94.4	97.6
C&W	0.8	93.3	95.6	96.8
JSMA	0.8	90.4	93.6	96.8
DeepFool	0.4	93.2	95.5	96.3
ZOO	1.0	90.8	93.5	95.6
DI^2FGSM	1.4	54.3	57.2	74.6
MDI^2FGSM	0.6	24.9	27.1	36.4

References

[1] S. Baluja and I. Fischer, "Learning to attack: Adversarial transformation networks," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 32, no. 1, 2018.

[2] N. Carlini and D. Wagner, "Towards evaluating the robustness of neural networks," in *2017 ieee symposium on security and privacy (sp)*. Ieee, 2017, pp. 39–57.

[3] P.-Y. Chen, H. Zhang, Y. Sharma, J. Yi, and C.-J. Hsieh, "Zoo: Zeroth order optimization based black-box attacks to deep neural networks without training substitute models," in *Proceedings of the 10th ACM workshop on artificial intelligence and security*, 2017, pp. 15–26.

[4] N. Das, M. Shanbhogue, S.-T. Chen, F. Hohman, S. Li, L. Chen, M. E. Kounavis, and D. H. Chau, "Shield: Fast, practical defense and vaccination for deep learning using jpeg compression," in *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2018, pp. 196–204.

[5] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei, "Imagenet: A large-scale hierarchical image database," in *2009 IEEE conference on computer vision and pattern recognition*. Ieee, 2009, pp. 248–255.

[6] X. Dong, J. Bao, D. Chen, W. Zhang, N. Yu, L. Yuan, D. Chen, and B. Guo, "Cswin transformer: A general vision transformer backbone with cross-shaped windows," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2022, pp. 12 124–12 134.

[7] Y. Dong, F. Liao, T. Pang, H. Su, J. Zhu, X. Hu, and J. Li, "Boosting adversarial attacks with momentum," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 9185–9193.

[8] G. K. Dziugaite, Z. Ghahramani, and D. M. Roy, "A study of the effect of jpg compression on adversarial images," *arXiv preprint arXiv:1608.00853*, 2016.

[9] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," *arXiv preprint arXiv:1412.6572*, 2014.

[10] C. Guo, M. Rana, M. Cisse, and L. Van Der Maaten, "Countering adversarial images using input transformations," *arXiv preprint arXiv:1711.00117*, 2017.

[11] J. Hayes and G. Danezis, "Learning universal adversarial perturbations with generative models," in *2018 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2018, pp. 43–49.

[12] X. Jia, X. Wei, X. Cao, and H. Foroosh, "Comdefend: An efficient image compression model to defend adversarial examples," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2019, pp. 6084–6092.

[13] A. Kurakin, I. J. Goodfellow, and S. Bengio, "Adversarial examples in the physical world," in *Artificial intelligence safety and security*. Chapman and Hall/CRC, 2018, pp. 99–112.

[14] C. Ledig, L. Theis, F. Huszár, J. Caballero, A. Cunningham, A. Acosta, A. Aitken, A. Tejani, J. Totz, Z. Wang *et al.*, "Photo-realistic single image super-resolution using a generative adversarial network," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2017, pp. 4681–4690.

[15] F. Liao, M. Liang, Y. Dong, T. Pang, X. Hu, and J. Zhu, "Defense against adversarial attacks using high-level representation guided denoiser," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 1778–1787.

[16] B. Lim, S. Son, H. Kim, S. Nah, and K. Mu Lee, "Enhanced deep residual networks for single image super-resolution," in *Proceedings of the IEEE conference on computer vision and pattern recognition workshops*, 2017, pp. 136–144.

[17] 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.

[18] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards deep learning models resistant to adversarial attacks," 2018.

[19] S.-M. Moosavi-Dezfooli, A. Fawzi, O. Fawzi, and P. Frossard, "Universal adversarial perturbations," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2017, pp. 1765–1773.

[20] 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*, 2016, pp. 2574–2582.

[21] A. Mustafa, S. H. Khan, M. Hayat, J. Shen, and L. Shao, "Image super-resolution as a defense against adversarial attacks," *IEEE Transactions on Image Processing*, vol. 29, pp. 1711–1724, 2019.

[22] 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 (EuroS&P)*. IEEE, 2016, pp. 372–387.

[23] A. Prakash, N. Moran, S. Garber, A. DiLillo, and J. Storer, "Deflecting adversarial attacks with pixel deflection," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 8571–8580.

[24] W. Shi, J. Caballero, F. Huszár, J. Totz, A. P. Aitken, R. Bishop, D. Rueckert, and Z. Wang, "Real-time single image and video super-resolution using an efficient sub-pixel convolutional neural network," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 1874–1883.

[25] Y. Sun, Q. Xu, Y. Li, C. Zhang, Y. Li, S. Wang, and J. Sun, "Perceive where to focus: Learning visibility-aware part-level features for partial person re-identification," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2019, pp. 393–402.

[26] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, and R. Fergus, "Intriguing properties of neural networks," *arXiv preprint arXiv:1312.6199*, 2013.

[27] L. Tabelini, R. Berriel, T. M. Paixao, C. Badue, A. F. De Souza, and T. Oliveira-Santos, "Polylanenet: Lane estimation via deep polynomial regression," in *2020 25th International Conference on Pattern Recognition (ICPR)*. IEEE, 2021, pp. 6150–6156.

[28] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin, "Attention is all you need," *Advances in neural information processing systems*, vol. 30, 2017.

[29] C. Xie, J. Wang, Z. Zhang, Z. Ren, and A. Yuille, "Mitigating adversarial effects through randomization," *arXiv preprint arXiv:1711.01991*, 2017.

[30] C. Xie, Z. Zhang, Y. Zhou, S. Bai, J. Wang, Z. Ren, and A. L. Yuille, "Improving transferability of adversarial examples with input diversity," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2019, pp. 2730–2739.

Biography

Zi-Han Liu is a master student at the School of Control and Computer Engineering, North China Electric Power University. His research directions are smart grid and AI security.

Color Image Encryption Algorithm with ZigZag Transform and DNA Coding Based on Fractional Order 5D Hyperchaotic System

Fanqi Meng and Gang Wu
(Corresponding author: Fanqi Meng)

School of Mathematics and Statistics, Yancheng Teachers University
No.50, Kaifang Avenue, Yancheng 224002, P.R. China
Email: fanqim@126.com

(Received Mar. 29, 2023; Revised and Accepted Nov. 22, 2023; First Online Feb. 23, 2024)

Abstract

Image encryption is an important method for protecting information security. Deoxyribonucleic acid (DNA) coding, ZigZag transform, and Chaotic system technology have proven effective for image encryption. A novel color image encryption algorithm is proposed based on the ZigZag transform, DNA coding technology, and fractional order 5D hyper-chaotic system (F5DHS) to enhance image information security. Firstly, the chaotic matrices are generated from F5DHS using control parameters and initial values. Secondly, the modified ZigZag confusing method is adopted to confuse the three components of the color image and then perform DNA coding. Finally, the DNA-encoded matrix is obfuscated and diffused through a chaotic matrix before performing DNA decoding to obtain an encrypted image. Simulation results and security analysis demonstrate that the algorithm can withstand multiple attacks and has good image encryption performance.

Keywords: 5D Hyper-chaotic System; Image Encryption; DNA Coding; ZigZag Transform

1 Introduction

As information technology continues to advance, we are witnessing the emergence of 5G, big data, and artificial intelligence. However, with the rapid increase in the volume of data, the security of information transmission and storage is facing greater challenges. Any unauthorized access, occupation, or damage to network information not only results in economic losses to computer users but also poses a significant threat to the security of the entire society and even the nation. Therefore, network information security has become a crucial area of focus in scientific research. Amongst all forms of information, image security holds particular significance as it serves as the primary medium for the exchange of information.

As image data is characterized by a large amount of data, strong pixel correlation, and high redundancy, traditional encryption methods are no longer suitable for image encryption. To better combine image features for information protection, various technologies have been applied in the field of image encryption. In 1989, Matthews proposed an encryption method using logistic mapping that combined chaotic systems with cryptography [13]. Chaotic systems are suitable for designing image encryption algorithms due to their sensitivity to initial value, pseudo-randomness, and unpredictability. Fridrich applied chaotic systems to image encryption in 1998, generating a chaotic sequence through two-dimensional Baker chaotic map iteration and using it in the image encryption process [3]. Subsequently, researchers have proposed various complex chaotic image encryption algorithms. For instance, Hua *et al.* improved the chaotic performance of one-dimensional chaotic map by modulating the output of a one-dimensional function through a sine chaotic map [22]. Hanis *et al.* proposed an improved Logistic chaotic map that expands the range of chaotic trajectory, expands the key space, and strengthens the sensitivity of the initial value [8]. Other proposed methods include an image encryption algorithm based on 2D discrete-time mapping designed by Liu *et al.* [12], a color image encryption method based on Arnold transform and Hadamard single-pixel imaging proposed by Qu *et al.* [20]. Although some progress has been made in the research of chaotic image encryption, the security of a single image encryption method based on the chaotic system depends on the complexity of the chaotic system, and the efficiency of the algorithm is low. Therefore, exploring the possibility of combining chaos theory with other theories to improve the security of image encryption is worth considering.

The ZigZag transform is a method that can be used to permute image pixels, and it is both simple and effective. Essentially, this method involves scanning the elements of a matrix in a particular order, known as the ZigZag

order, starting from the upper left corner and moving towards the lower right corner, in order to scramble the data. Due to its simplicity and low time complexity, the ZigZag transform has been extensively employed in the field of image and video encryption. Gao *et al.* [5] applied a dynamic row scrambling and ZigZag transform method in image encryption. Guo *et al.* [7] proposed a reverse ZigZag transformation method for image encryption. In addition, following the development of genetic engineering, some researchers have proposed using DNA sequences and operators to change the pixel value of the diffusion part and designing image encryption algorithms based on DNA sequences [4, 6, 10]. By combining chaotic systems with DNA encoding technology, more secure and efficient encryption algorithms can be projected. To this end, Yan *et al.* [17] proposed a method for image encryption using a 1D logistic map and DNA coding sequence. Wu *et al.* [11]presented an image encryption algorithm derived from a 2D chaotic map and DNA encoding. Wang *et al.* [16] presented an image encryption method based on DNA encoding and compressed sensing. Wu *et al.* [15] proposed a color image DNA encryption using NCA map. Zhang *et al.* [21] combined DNA encoding, hyperchaotic system, phase-truncated FRFT, and Arnold transform to apply an asymmetric image encryption method. However, most image encryption algorithms based on DNA encoding are combined with integer-order chaotic systems, and it is known that fractional-order chaotic systems possess more abundant dynamic features due to their high nonlinearity and nonlocal features [9, 18]. Thus, to enhance the security and key space of image encryption algorithms, a novel image encryption algorithm with ZigZag transform and DNA approach based on F5DHS is proposed in this paper.

The paper is organized as follows: Section 2 provides an overview of the preliminary materials and mathematical models used in this study. Section 3 outlines the process of the color encryption algorithm ZigZag transform and DNA encoding based on F5DHS. In Section 4, numerical experiments are conducted to verify the security and feasibility of the encryption algorithm. Lastly, Section 5 offers some conclusions.

2 Preliminary Materials

2.1 Fractional-order 5D Hyper-chaotic System

Fractional calculus is an extension of integer calculus. Dynamic systems calculated from fractional differential equations have more complex dynamic characteristics and can generate more complex chaotic sequences. The Caputo type differential equation is defined as [14]

$$D_t^q f(t) = \frac{1}{\Gamma(w-q)} \int_0^t \frac{f^w(\tau)}{(t-\tau)^{q-w+1}} d\tau, \qquad (1)$$

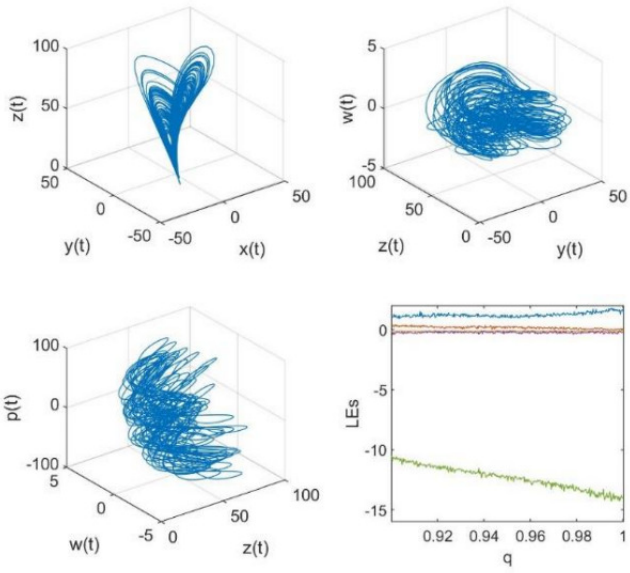


Figure 1: Phase diagram and Lyapunov exponent diagram of F5DHS

where $\Gamma(\cdot)$ is the gamma function and $t \geq 0$, $w \in Z^+$, $w-1 < q < w$.

In this paper, the Lorentz system proposed in Ref. [19] is generalized to the fractional order 5D hyperchaotic system according to the definition of Caputo differential equation. The F5DHS is given by

$$\begin{cases} D_t^q x(t) = a(y(t) - x(t)), \\ D_t^q y(t) = cx(t) + dy(t) - x(t)z(t) + p(t), \\ D_t^q z(t) = -bz(t) - x^2(t), \\ D_t^q w(t) = ey(t) + fw(t), \\ D_t^q p(t) = -rx(t) - kp(t). \end{cases} \qquad (2)$$

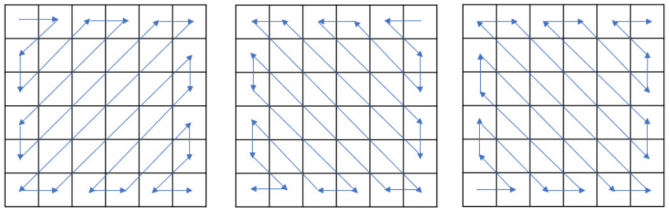
where q represent the fractional order of F5DHS. When the parameters of the F5DHS are set as $a = 35$, $b = 7$, $c = 35$, $d = 5$, $e = -0.5$, $f = -0.1$, $r = 15.5$, $k = 0.5$ $q = 0.975$, and the initial value $(x_0,\ y_0,\ z_0,\ w_0,\ p_0) = (0.2,\ 0.2,\ -0.1,\ -0.1,\ -0.1)$. using the predictor–corrector algorithm [2] to solve the above equation. The diagram of F5DHS phase and Lyapunov exponent are obtained as shown in Figure 1. Obviously, the F5DHS is in the chaotic state, which has better randomness and larger secret key space.

2.2 ZigZag Transform

The ZigZag transform is a method of arranging the elements in a quantization coefficient matrix in a "Z" shape pattern and storing them in a one-dimensional array. Then, the one-dimensional array is transformed into a two-dimensional matrix in a certain way. In image processing technology, each pixel is saved in a two-dimensional array, and then the ZigZag transform is applied to the two-dimensional array. The transformed result is updated in the image, resulting in the final scram-

Table 1: DNA encoding rules

	1	2	3	4	5	6	7	8
A	00	00	10	10	01	01	11	11
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01
T	11	11	01	01	10	10	00	00



(a) Upper Left (b) Upper Right (c) Lower Left

Figure 2: Extend ZigZag Scrambling Method Diagram

bled image. This paper uses the extended ZigZag method shown in Figure 2 to scramble the color image.

2.3 DNA Encoding and Operations

The DNA sequence is comprised of four bases: Adenine, Cytosine, Thymine, and Guanine, represented by the letters A, C, T, and G respectively. A and T are complementary, as are C and G. These bases can be represented by binary numbers: 00, 10, 01, and 11, with A being 00, C being 10, T being 01, and G being 11. Out of the 24 possible combinations of these four bases, only eight are valid DNA coding combinations, which are detailed in Table 1. Each pixel value of a digital image can be expressed as a 4-bit DNA code. For example, a pixel value of 189 can be encoded as TCCA (10 11 11 01) using rule 6. The operations of addition, subtraction, and XOR between DNA sequences are defined in Tables 2. 3, and 4.

Table 2: DNA addition operation

	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

Table 3: DNA subtraction operation

	A	T	C	G
A	A	G	C	T
T	T	A	G	C
C	C	T	A	G
G	G	A	T	A

Table 4: DNA XOR operation

	A	T	G	C
A	A	T	G	C
T	T	A	C	G
G	G	C	A	T
C	C	G	T	A

3 Image Encryption Scheme

3.1 Encryption Algorithm

The encryption process of the color image encryption algorithm with ZigZag transform and DNA coding based on fractional order 5D hyperchaotic system is shown in Figure 3. The specific implementation details of the encryption scheme are as follows:

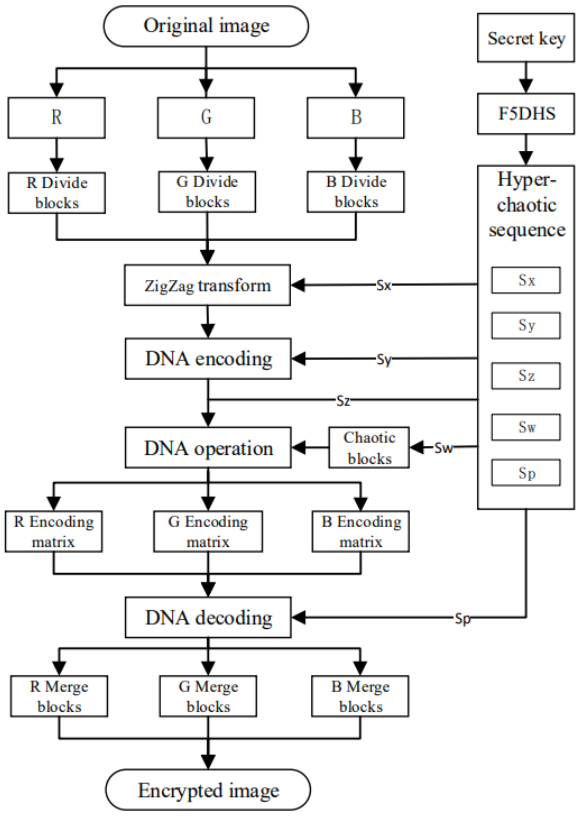


Figure 3: Flowchart of the proposed algorithm

Step 1: Set the secret key values x_0, y_0, z_0, w_0, p_0, a, b, c, d, e, f, r, k, q of F5DHS, and get the hyperchaotic sequences Sx, Sy, Sz, Sw, Sp from F5DHS. Then the range of Sx, Sy, Sz, Sw, Sp are calculated by Formula (3).

$$\begin{cases} Sx = \left(round\left(|Sx| \times 10^{10}\right)\right) mod\ 3 \\ Sy = \left(round\left(|Sy| \times 10^{10}\right)\right) mod\ 8 + 1 \\ Sz = \left(round\left(|Sz| \times 10^{10}\right)\right) mod\ 3 \\ Sw = \left(round\left(|Sw| \times 10^{10}\right)\right) mod\ 255 \\ Sp = \left(round\left(|Sp| \times 10^{10}\right)\right) mod\ 8 + 1 \end{cases} \tag{3}$$

Step 2: The color image I with size of $M \times N$ is separated into three primary colors: Rm, Gm, Bm.

Step 3: Divide Rm, Gm, Bm into equal blocks $Rx(i)$, $Gx(i)$, $Bx(i)$ respectively.

Step 4: The chaotic sequence $Sx(i)$ represents three methods of ZigZag transformation in Figure 2, and then uses the corresponding ZigZag transformation method to scramble $Rx(i)$, $Gx(i)$, $Bx(i)$ to obtain $Rx\_z(i)$, $Gx\_z(i)$, $Bx\_z(i)$.

Step 5: The chaotic sequence Sw is converted into equal blocks $Sw(i)$, and the size of $Sw(i)$ is equal to $Rx\_z(i)$, $Gx\_z(i)$, $Bx\_z(i)$.

Step 6: $Rx\_z(i)$, $Gx\_z(i)$, $Bx\_z(i)$, $Sw(i)$ are encoded according to the DNA coding rules defined by $Sy(i)$.

Step 7: $Sw(i)$ calculate with $Rx\_z(i)$, $Gx\_z(i)$, $Bx\_z(i)$ to the DNA calculation methods defined by $Sz(i)$ to obtain $Rx\_z\_c(i)$, $Gx\_z\_c(i)$, $Bx\_z\_c(i)$ respectively.

Step 8: Converting $Rx\_z\_c(i)$, $Gx\_z\_c(i)$, $Bx\_z\_c(i)$ into pixel value matrix of image $Rx\_z\_c\_d(i)$, $Gx\_z\_c\_d(i)$, $Bx\_z\_c\_d(i)$ using DNA decoding rules defined by $Sp(i)$.

Step 9: Combine matrix block $Rx\_z\_c\_d(i)$, $Gx\_z\_c\_d(i)$, and $Bx\_z\_c\_d(i)$ into $Rx\_z\_c\_d$, $Gx\_z\_c\_d$, and $Bx\_z\_c\_d$.

Step 10: Merger $Rx\_z\_c\_d$, $Gx\_z\_c\_d$, and $Bx\_z\_c\_d$ into the encrypted color image.

3.2 Decryption Algorithm

The decryption process is essentially the reverse of encryption, requiring the use of the secret key from the encryption algorithm in order to decrypt the ciphertext. During decryption, there are several critical points to consider. Firstly, the DNA encoding method and the DNA operation rules of the ciphertext image must also be determined by Sy, Sz, Sp. Secondly, the DNA operations performed during decryption are the inverse of those used during encryption. Finally, the DNA-encoded image data blocks are subject to an inverse ZigZag transformation and then combined to create the plaintext image.

3.3 Simulation Result

The Lenna color image (Figure 4(a1), size 256 × 256) Fruits color image (Figure 4(b1), size 512 × 480) and Baboon color image (Figure 4(c1), size 512 × 512) are used to test the encryption algorithm. The secret key $x_0 = 0.2$, $y_0 = 0.2$, $z_0 = -0.1$, $w_0 = -0.1$, $p_0 = -0.1$, $a = 35$, $b = 7$, $c = 35$, $d = 5$, $e = -0.5$, $f = -0.1$, $r = 15.5$, $k = 0.5$, $q = 0.975$. The encrypted color images can be obtained as in Figure 4(a2, b2, c2) and the corresponding decrypted color images are shown in Figure 4(a3, b3, c3).

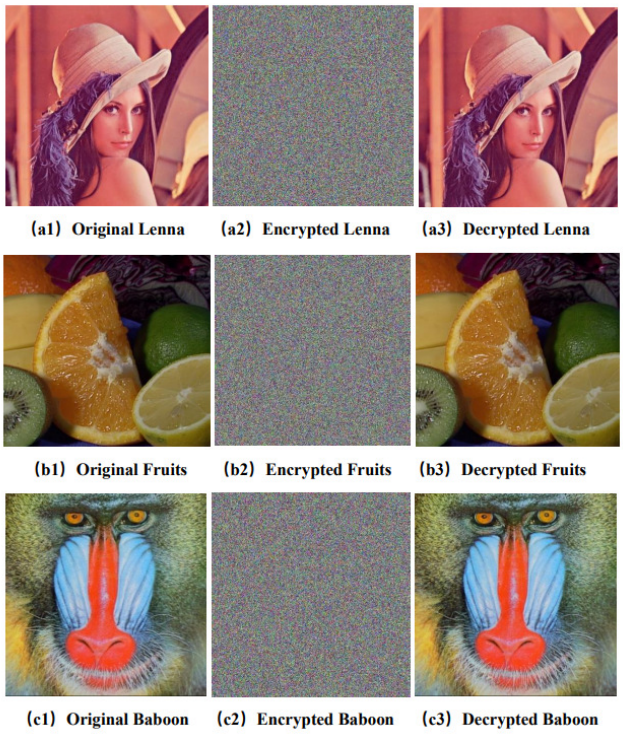


Figure 4: Original (a1)-(c1), encrypted (a2)-(c2) and decrypted (a3)-(c3) of test images

4 Security Analyses

4.1 Key Space

To satisfy the Kerckhoffs criterion and be considered a strong encryption algorithm, it must possess a sufficiently large key space to withstand brute-force attacks. The security keys of the encryption algorithm in this article are comprised of chaotic system parameters a, b, c, d, e, f, r, k, q and initial values x_0, y_0, z_0, w_0, p_0. If the computational accuracy is 10^{-8}, the size of key space would be lager than $10^{14\times8} > 2^{360}$. Since our proposed algorithm has a large enough key space, it is capable of withstanding brute-force attacks.

4.2 Key Sensitivity Analysis

A strong and reliable key system should possess a high level of sensitivity to its keys. For instance, when we made minor adjustments to x_0, w_0, a, c and $q$in the secret key for the Lenna picture, the resulting decrypted image, shown in Figure 5, reveals that even slight modifications to the secret key can prevent successful decryption of the original image. This highlights the crucial importance of a secure and robust key system. Our encryption algorithm has been specifically designed to exhibit an exceptional degree of sensitivity to the secret key, thereby ensuring the utmost security and protection against potential threats.

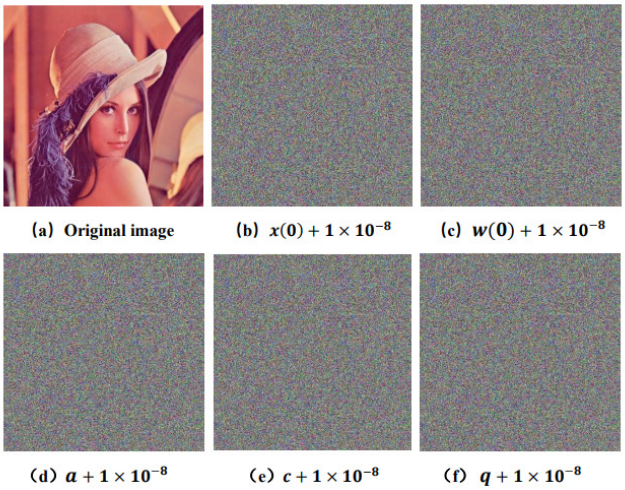


Figure 5: Key Sensitively test (a) Original image (b) $x\,(0)+1\times10^{-8}$ (c) $w_0+1\times10^{-8}$ (d) $a+1\times10^{-8}$ (e) $c+1\times10^{-8}$ (f) $q+1\times10^{-8}$

4.3 Histogram Analysis

Histograms represent the distribution of pixels in an image, and they are an important metric for measuring the resistance of cryptographic algorithms to statistical analysis. If the histogram pixel distribution of a ciphertext image is uniform, meaning the pixel distribution is flat, it becomes difficult to obtain information from it through statistical analysis. In Figure 6, the histograms of the encrypted and original Lenna color images are shown for each of the R, G, and B color channels. The results demonstrate that the histogram pixel distribution of the ciphertext Lenna image is more uniform than that of the plaintext image. Therefore, the encryption algorithm we have designed is capable of resisting histogram attacks.

4.4 Correlation Analysis

The correlation between adjacent pixels of a digital image is often significant, and statistical analysis can be used to crack encryption algorithms that do not sufficiently account for this. Therefore, an encryption algorithm must minimize the correlation between the pixels of the cipher-

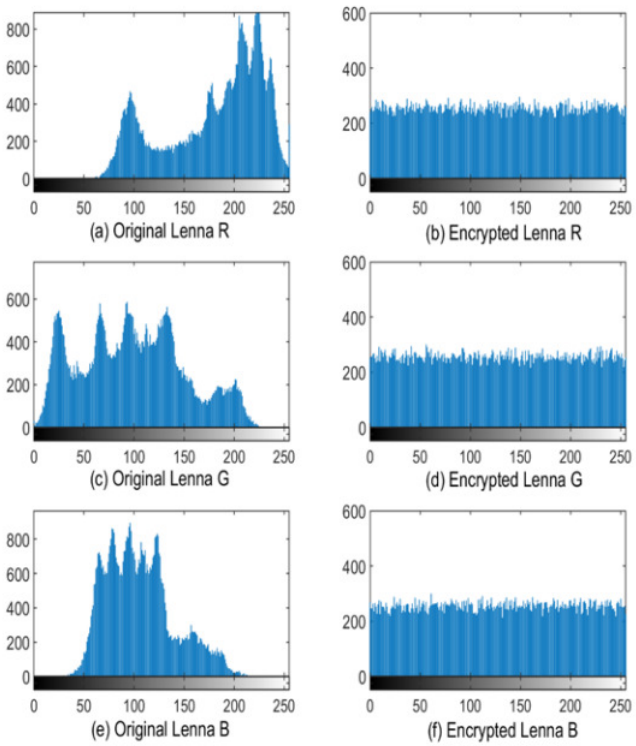


Figure 6: Histogram of image. (a) (c) (e) Histogram of original Lenna R. G. B, (b) (d) (f) Histogram of encrypted Lenna R. G. B

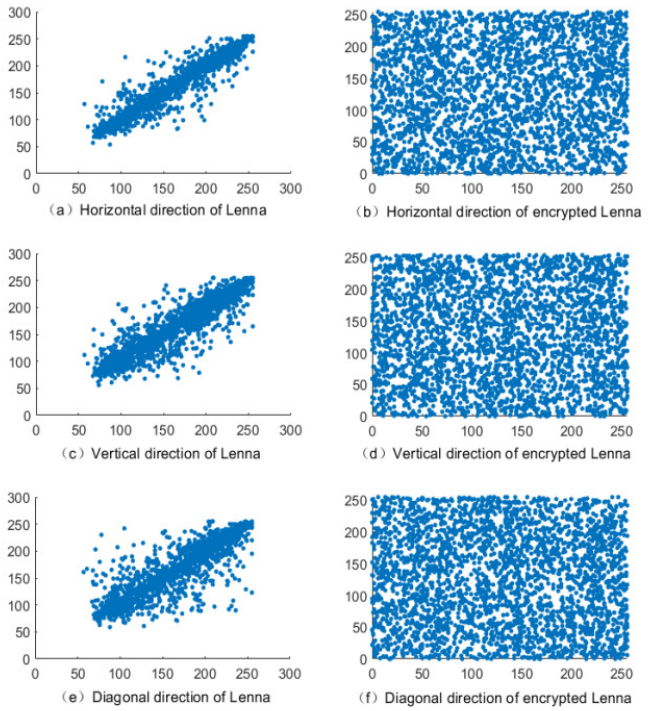


Figure 7: Distribution of adjacent pixels (a) (c) (e) Horizontal, Vertical, Diagonal of Lenna, (b) (d) (f) Horizontal, Vertical, Diagonal of encrypted Lenna

Table 5: The results of correlation analysis

Test image		Original image			Encrypted image		
		R	G	B	R	G	B
Lenna	H	0.94933	0.95028	0.91311	0.00206	-0.01386	-0.03479
	V	0.97329	0.97473	0.94895	-0.00643	-0.00663	-0.01286
	D	0.92699	0.93137	0.88146	0.01036	-0.00832	0.03226
Fruits	H	0.99113	0.99073	0.98261	-0.01286	-0.02040	-0.00227
	V	0.98464	0.98444	0.96904	-0.04316	-0.02325	0.01239
	D	0.94774	0.92942	0.87928	0.00079	-0.02222	0.03102
Baboon	H	0.91874	0.87174	0.85343	0.01275	0.01061	-0.01370
	V	0.8621	0.7740	0.73417	-0.03162	-0.02756	0.01770
	D	0.90325	0.88231	0.83817	0.02039	0.02537	-0.00645

Table 6: Results of entropy analysis

Test image	S	R	G	B
Lenna	7.9991	7.9973	7.9974	7.9971
Fruits	7.9998	7.9993	7.9993	7.9992
Baboon	7.9998	7.9993	7.9992	7.9992

Table 7: Comparison with other algorithms

Test image	R	G	B
Lenna	7.9973	7.9974	7.9971
Ref. [12]	7.9896	7.9893	7.9896
Ref. [4]	7.9973	7.9969	7.9971
Ref. [10]	7.9893	7.9896	7.9903
Ref. [15]	7.9892	7.9898	7.9899
Ref. [1]	7.9901	7.9912	7.9921

text image. This can be achieved by calculating the correlation coefficient, which can be represented by

$$E(m) = \frac{1}{Y}\sum_{i=1}^{Y} m_i \tag{4}$$

$$D(m) = \frac{1}{Y}\sum_{i=1}^{Y} (m_i - E(m))^2 \tag{5}$$

$$Cov(m,n) = \frac{1}{Y}\sum_{i=1}^{Y} (m_i - E(m))(n_i - E(n)) \tag{6}$$

$$r_{mn} = \frac{Cov(m,n)}{\sqrt{D(m)} \times \sqrt{D(n)}} \tag{7}$$

Where m, n are the grayscale values of two adjacent pixels and Y is to the total number of random pixels. In the conducted experiment using images of Lenna, Fruits, and Baboon, we randomly selected 3000 pairs of pixels from the horizontal, vertical, and diagonal directions of both the original and ciphertext images. The results of this experiment are presented in Table 5. Additionally, Figure 7 displays the adjacent pixel distribution of Lenna and its encrypted image. The findings from Table 5 and Figure 7 demonstrate that the original image exhibits strong correlation between pixels, whereas the encrypted image displays randomly distributed points.

4.5 Information Entropy Analysis

Information entropy is a measure utilized to evaluate the randomness present in a ciphertext image. It is mathematically defined as:

$$H(k) = -\sum_{i=0}^{M-1} P(k_i)\log_2 P(k_i) \tag{8}$$

Where $P(k_i)$ means that the probability of pixel value k_i occurrence, and M denotes the gray level of image. When the gray value of an image is 256, the theoretical value of information entropy is $H = 8$. Table 6 displays the information entropy values for the ciphertext images of Lenna, Fruits, and Baboon, as well as their respective R, G, and B channels. From the data presented in Table 6. Table 7 shows that the proposed encryption algorithm is compared with other algorithms in the literature. It can be observed that our proposed algorithm exhibits an ideal level of randomness and is superior to the algorithms in the literature.

4.6 Differential Attack Analysis

Differential attack analysis involves an attacker making minor modifications to the original image, encrypting the modified image using the encryption method, and then comparing the resulting ciphertext images to detect any correlation between the original and encrypted images that can be exploited to extract image information. To assess the effectiveness of an encryption algorithm in resisting differential attacks, researchers typically employ two metrics: the Unified Average Change Intensity (UACI) and the Number of Pixel Changes Rate (NPCR). The UACI and NPCR values are calculated as follows:

$$UACI = \frac{1}{K}\sum_{i,j} \frac{|C_0(i,j) - C_1(i,j)|}{255} \times 100\% \tag{9}$$

$$NPCR = \frac{1}{K}\sum_{i,j} D(i,j) \times 100\% \tag{10}$$

Table 8: UACI and NPCR for Lenna, Fruits and Baboon

Test image	NPCR (%)			UACI (%)		
	R	G	B	R	G	B
Lenna	33.314	33.334	33.414	99.606	99.643	99.625
Fruits	33.513	33.506	33.484	99.620	99.614	99.617
Baboon	33.445	33.503	33.491	99.619	99.620	99.616

$$D(i,j) = \begin{cases} 0 & if\ C_0(i,j) = C_1(i,j) \\ 1 & else \end{cases} \quad (11)$$

where B_0 and B_1 are pixel values for encrypted images changed in the same position. During our experiment, we evaluated the UACI and NPCR values using different original and encrypted images. The majority of the UACI and NPCR values obtained through our proposed algorithm, as observed in the experimental results, were in close proximity to 33.43% and 99.61%, respectively. These results indicate that our algorithm is highly effective in preventing differential attacks.

5 Conclusions

This paper introduces a novel chaotic system constructed using a fractional-order 5D hyper-chaotic system, which generates more complex chaotic sequences. Based on this system, a color image encryption scheme is proposed that utilizes ZigZag transform and DNA coding technology. The chaotic sequences generated by the F5DHS system control DNA operations, coding, and decoding, ensuring robust and secure encryption. The high dimensionality of the F5DHS system used in the encryption process results in a sufficiently large key space. Experimental results confirm the effectiveness of the proposed encryption scheme, which is capable of withstanding various attacks and is therefore suitable for image encryption.

References

[1] C. Dong, "Color image encryption using one-time keys and coupled chaotic systems," *Signal Process. Image Communication*, vol. 29, no. 5, pp. 628–640, 2014.

[2] N. J. Ford D. Kai and A. D. Freed, "A predictor–corrector approach for the numerical solution of fractional differential equations," *Nonlinear Dynamics*, vol. 29, no. 1, pp. 3–22, 2002.

[3] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[4] Z. Gan Y. Lu X. Chai, X. Fu and Y. Chen, "A color image cryptosystem based on dynamic dna encryption and chaos," *Signal Process*, vol. 155, no. 1, pp. 44–62, 2019.

[5] H. Gao and X. Wang, "An image encryption algorithm based on dynamic row scrambling and zigzag transform, chaos," *Solitons and Fractals*, vol. 147, no. 6, p. 110962, 20121.

[6] F. G. Guimarães R. Enayatifar and P. Siarry, "Index-based permutation-diffusion in multiple-image encryption using dna sequence," *Optics and Lasers in Engineering*, vol. 115, no. 1, pp. 131–140, 2019.

[7] Z. Guo and P. Sun, "Improved reverse zigzag transform and dna diffusion chaotic image encryption method," *Multimedia Tools and Applications*, vol. 81, no. 1, pp. 11301–11323, 2022.

[8] S. Hanis and R. Amutha, "A fast double-keyed authenticated image encryption scheme using an improved chaotic map and a butterfly-like structure," *Nonlinear Dynamics*, vol. 95, no. 1, pp. 421–432, 2019.

[9] T. Huang L. Yuan S. Zheng L. Chen, H. Yin and L. Yin, "Chaos in fractional-order discrete neural networks with application to image encryption," *Neural Networks*, vol. 125, no. 1, pp. 174–184, 2020.

[10] H. Kan X. Wu and J. Kurths, "A new color image encryption scheme based on dna sequences and multiple improved 1d chaotic maps," *Applied Soft Computing*, vol. 37, no. 1, pp. 24–39, 2015.

[11] X. F. Liao J. H. Wu and B. Yang, "Image encryption using 2d hénonsine map and dna approach," *Signal Process*, vol. 153, no. 1, pp. 11–23, 2018.

[12] H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2d discrete-time map," *Signal Process*, vol. 113, no. 1, pp. 104–112, 2015.

[13] R. Matthews, "On the derivation of a chaotic encryption algorithm," *Cryptologia*, vol. 13, no. 1, p. 29C41, 1989.

[14] I. Podlubny, *Fractional Differential Equations*. New York: Academic Press, 1999.

[15] X. Wang H. Kan X. Wu, K. Wang and J. Kurths, "Color image dna encryption using nca map-based cml and one-time keys," *Signal Process*, vol. 148, no. 1, pp. 272–287, 2018.

[16] X. Wang and Y. Su, "Image encryption based on compressed sensing and dna encoding," *Signal Processing Image Communication*, vol. 12, no. 1, p. 116246, 2021.

[17] X. Y. Wang X. P. Yan and Y. J. Xian, "Chaotic image encryption algorithm based on arithmetic sequence scrambling model and dna encoding operation," *Multimedia Tools and Applications*, vol. 80, no. 1, pp. 10949–10983, 2021.

[18] L. Xiong Z. Wang X. Li, J. Mou and J. Xu, "Fractional-order double-ring erbium-doped fiber laser chaotic system and its application on image encryption," *Optics and Laser Technology*, vol. 140, no. 1, p. 107074, 2021.

[19] Q. Yang and M. Bai, "A new 5d hyperchaotic system based on modified generalized lorenz system," *SNonlinear Dynamics*, vol. 88, no. 1, pp. 189–221, 2017.

[20] Y. Yin H. Wu G. Qu, X. Meng and W. He, "Optical color image encryption based on hadamard single-pixel imaging and arnold transform," *Optics and Lasers in Engineering*, vol. 137, no. 20, p. 106392, 2021.

[21] Z. Zhong Y. B. Zhang, L. Zhang and L. Yu, "Hyperchaotic image encryption using phase-truncated fractional fourier transform and dna-level operation," *Optics and Lasers in Engineering*, vol. 143, no. 7, p. 106626, 2021.

[22] B. Zhou Z. Hua and Y. Zhou, "Sine chaotification model for enhancing chaos and its hardware implementation," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 2, pp. 25–36, 2018.

Biography

Fanqi Meng received the Ph.D. degree from Hohai University, China. He is currently an Associate Professor in Yancheng Teachers University, China. His research interests include information hiding and steganalysis and fractional order dynamical system.

Gang Wu is a student in Yancheng Teachers University, China. His research interests focus on network and information security.

A Note on One Lightweight Authenticated Key Agreement for Fog-enabled IoT Deployment

Lihua Liu[1], Yingqing Jia[1], and Zhengjun Cao[2]
(Corresponding author: Lihua Liu)
Department of Mathematics, Shanghai Maritime University[1]
Haigang Ave 1550, Shanghai, 201306, China[1]
Department of Mathematics, Shanghai University, China[2]
Email: liulh@shmtu.edu.cn
(Received Mar. 25, 2023; Revised and Accepted Nov. 24, 2023; First Online Feb. 23, 2024)

Abstract

We show that the key agreement scheme [Int. J. Inf. Sec., 21(6), 2022, 1373–1387] is flawed, in which the user encrypts the temporary ID using a symmetric key encryption in order to keep anonymity. It is a paradox if the pre-shared key for such a symmetric key encryption is already available. We want to stress that the ultimate use of a key agreement scheme is just to establish a shared key for some symmetric key encryption, but not vise versa. We also reiterate the signification of an identifier which has often been neglected by some researchers.

Keywords: Authentication; Key Agreement; Key Transfer; Salted Password Hashing; Symmetric Key Encryption

1 Introduction

Fog computing related to the nodes in between the host and the cloud, was intended to bring the computational capabilities of the system close to the host machine. It reduces the amount of data that needs to be sent to the cloud, and provides better privacy as industries can perform analysis on their data locally. But data management becomes tedious since the transmission of data involves encryption, decryption, authentication, etc.

In 2017, Khan [11] investigated fog computing security. Kharel [12] presented an architecture for smart health monitoring system based on fog computing. Aazam *et al.* [1, 2, 18, 20, 22] discussed the architecture of fog computing, its future research directions, and research challenges. Gope *et al.* [9, 13] designed a privacy-aware key agreement scheme for secure smart grid communication. In 2020, Pan *et al.* [19] presented an enhanced secure smart card-based password authentication scheme. Ali *et al.* [4] provided a clogging resistant secure authentication scheme for fog computing services. Battula *et al.* [6] set up a generic stochastic model for resource availability in fog computing environments. Liu and Cao [15] showed that one lightweight authentication and key agreement scheme for Internet of Drones was not truly anonymous. Lu and Hwang *et al.* [5, 16] designed a key generation scheme without a trusted third party for access control in multilevel wireless sensor networks. In 2023, Lin and Hsu [14] proposed a chaotic maps-based privacy-preserved three-factor authentication scheme for telemedicine systems. Hwang *et al.* [10] presented an improved of enhancements of a user authentication scheme.

Recently, Abdussami *et al.* [3] have presented a key agreement scheme for fog-enabled IoT scenario. Though the scheme is interesting, we find it is flawed because the user has to invoke a symmetric key encryption to securely transfer the temporary ID to CS. But the final key derived from a key agreement scheme is just served as a shared key for some symmetric key encryption, which is a heavy cryptographic primitive in comparison to key agreement. The scheme has confused key transfer with key agreement. We also find that the scheme is vulnerable to guessing password attack, because the password is not salted. It neglects the fact that an identifier is the characteristics that distinguish it from others, which should be public and easily available. We want to stress that an identifier can be hidden in a concrete session, but it is publicly accessible in the system, otherwise such an identifier loses its signification.

2 Preliminaries

Key agreement, key distribution, key exchange, and key transfer [17], are often confused, but their common target is to establish a shared key between users. The resulting key in a key agreement scheme is not preexisting. However, the resulting key in a key transfer scheme is preexisting, which should be recovered intactly.

The difference between key agreement and key transfer seems unfamiliar to some researchers. To illustrate it, we now review Diffie-Hellman key exchange [8] and RSA [21] (see Table 1). Apparently, RSA requires a com-

plex system setup, which relies on Public Key Infrastructure (PKI) to enable Bob to invoke Alice's true public key. Its authentication originates directly from the reliance on PKI. Such reliance could be unavailable for some scenarios. Whereas, a lightweight key agreement scheme is more applicable to this case. The usual size of RSA modulus is not less than 2048 bits. Such modular exponentiation is too expensive for some devices. So, RSA is used to transfer session keys, instead of original data.

3 Review of the Scheme

The scheme has four entities: IoT device, Fog node (FN), Cloud server (CS), and User. The user will first authenticate with the cloud server. The cloud server will store the data sensed by the IoT devices received via fog nodes and give access to the authorized users. IoT devices and user devices are not trusted entities. It assumes that the adversary can compromise the private credentials such as secret keys and session keys. Its security requirements include authentication, integrity, forward secrecy, and user anonymity.

Let ID_i, PW_i be the identity and password of ith user. $H(\cdot)$ is a hash function. A physically unclonable function (PUF) responses differ from one different PUF instance for the same challenge, but it gives the same response for the same challenge in an instance. The user registration can be depicted as follows (Table 2).

4 A paradox

In the scheme the user has to use a symmetric key encryption to transfer the new temporary identifier, T_{idnew}, i.e.,

$$B_i = E_{H(R_{i1}\|T_{id})}(A_i\|T_{id}\|T_U\|T_{\text{idnew}}) \tag{1}$$

The fingerprint $H(R_{i1}\|T_{id})$ acts as a session key.

We find the scheme tries to use the current session key to negotiate a new session key $H(T_{id}\|R_{i1}\|T_C)$. But there is no ultimate difference between

$$H(R_{i1}\|T_{id}) \quad \text{and} \quad H(T_{id}\|R_{i1}\|T_C),$$

when they are used for session keys. Both are random outputs of a same hash function corresponding to two different inputs. As we know, a symmetric key encryption is rarely used for transferring session keys because it requires that both sides know a pre-agreed secret key. It is a paradox to use a pre-shared secret key to merely negotiate a new secret key.

5 A Possible Revision

As we discussed before, the negotiated key is ultimately used for a subsequent symmetric key encryption to transfer data. So, it is unnecessary to separate the target of mutual authentication and that of data transfer. In the proposed scenario, we find, the user and cloud server can **concurrently** achieve the two targets. See the following Table 3.

In the revised scheme, the ciphertext is

$$\hat{C} = E_{H(R_{i1}\|T_{id})}(A_i\|T_{id}\|T_U\|T_{\text{idnew}}\|h\|m) \tag{2}$$

in which two more components h, m are simultaneously encrypted. Its confidentiality comes directly from the original scheme. Besides, the checking of

$$h = H(R_{i1}\|T_{\text{idnew}}) \tag{3}$$

suffices for mutual authentication. Any adversary cannot generate such a fingerprint corresponding to the random temporary identifier T_{idnew}, because the component R_{i1} are only known to the legal user and the cloud server.

6 The Signification of an Identifier

ID-based encryption introduced by Shamir [23], is a type of public-key encryption in which the public key of a user is some unique information about the user's identity. Parties may encrypt messages with no prior distribution of keys between individual participants. This is very useful in cases where pre-distribution of authenticated keys is inconvenient or infeasible.

The discussed threat model assumes that user devices are not trusted entities. The data stored in user devices can be retrieved by using the power analysis attack (see §3.3, [3]). In order to protect the user's identity and password, the user device only stores $\{A_i, T_{id}, r_i, C_i\}$. It claims that the adversary cannot get the true identity Id_i and password PW_i even if the device is compromised, under the assumption that guessing the password and identity of the user separately is possible, whereas guessing both parameters in polynomial time is impractical.

The assumption ignores a basic fact: *any identifier in the whole system, which is the characteristics that distinguish it from others, is public and easily available.* Notice that an identifier can be hidden in a concrete session, but it is publicly accessible in the system [7]. Some researchers have neglected the difference between session-invisible identifier and system-visible identifier.

Taking into account the signification of an identifier, we find, the scheme is vulnerable to guessing password attack. Actually, according to the assumption a powerful adversary can access A_i, r_i which are stored in a target user device. The target Id_i is also accessible because it is a system-visible parameter, otherwise such an identifier loses its signification. So, the adversary can test password dictionaries to search for a *password* such that $H(Id_i\|password) = A_i \oplus r_i$.

7 Conclusion

In this note, we show that the Abdussami *et al.*'s key agreement scheme is flawed. We clarify the difference between key transfer and key agreement. We also reiterate

Table 1: Diffie-Hellman key exchange versus RSA

Diffie-Hellman key exchange	RSA
Setup. A prime p, a generator $g \in \mathbb{F}_p^*$.	*Setup.* Alice picks two big primes p, q, computes $n = pq$. Pick e and compute d such that $ed \equiv 1 \bmod \phi(n)$. Set the public key as (n, e), the private key as d.
$A \to B$. Alice picks an integer x_A to compute $y_A \equiv g^{x_A} \bmod p$. Send y_A to Bob.	
$A \leftarrow B$. Bob picks an integer x_B to compute the key $k \equiv y_A^{x_B} \bmod p$, and $y_B \equiv g^{x_B} \bmod p$. Send y_B to Alice.	$A \leftarrow B$. For $m \in \mathbb{Z}_n^*$, Bob checks the certification of public key (n, e), and computes $c \equiv m^e \bmod n$. Send c to Alice.
$A \downarrow$. Alice computes the key $k \equiv y_B^{x_A} \bmod p$.	$A \downarrow$. Alice computes $m \equiv c^d \bmod n$. (Usually, m is a session key, not a concrete message)

Table 2: User registration and authentication with cloud server

User		Cloud server
	Registration	
Select Id_i, PW_i, and compute $A_i = H(Id_i \Vert PW_i) \oplus r_i$, where r_i is a random number. Pick a temporary identity T_{id}. Generate challenge-response pairs $C_i = (C_{i1}, C_{i2}, \cdots)$, $R_i = (R_{i1}, R_{i2}, \cdots)$ by $PUF_i(\cdot)$.	$\xrightarrow[\text{secure channel}]{A_i, T_{id}, C_i, R_i}$	
Store $\{A_i, r_i, T_{id}, C_i\}$.		Store $\{A_i, T_{id}, C_i, R_i\}$ for the user.
	Mutual authentication and key agreement	
Enter Id_i, PW_i. The user device checks if $A_i = H(Id_i \Vert PW_i) \oplus r_i$. Generate the response R_{i1}, and select T_{idnew}, the time-stamp T_U. Compute $B_i = E_{H(R_{i1} \Vert T_{id})}(A_i \Vert T_{id} \Vert T_U \Vert T_{\text{idnew}})$.	$\xrightarrow[\text{open channel}]{B_i, T_U, C_{i1}, T_{id}}$	Check if $T_C - T_U \le \triangle T$. Decrypt B_i and check the consistency of A_i, T_{id}. Update T_{id} with T_{idnew}. Compute $S_C = H(T_{id} \Vert R_{i1} \Vert T_C), q_i = H(S_C \Vert A_i)$, $D_i = E_{H(R_{i1} \Vert T_{id})}(A_i + 1 \Vert T_C)$.
Check if $T_U - T_C \le \triangle T$. Decrypt D_i. Check the consistency of $A_i + 1$. If ok, compute $S_U = H(T_{id} \Vert R_{i1} \Vert T_C)$, and check if $q_i = H(S_U \Vert A_i)$.	$\xleftarrow{D_i, T_C, q_i}$	
	Subsequent data transfer	
For a message m, compute the ciphertext $\hat{C} = E_{S_U}(m)$	$\xrightarrow{\hat{C}}$	Compute the plaintext $m = D_{S_C}(\hat{C})$

Table 3: A possible revision

User		Cloud server
	Data transfer	
Enter Id_i, PW_i. The user device checks if $A_i = H(Id_i \Vert PW_i) \oplus r_i$. Generate the response R_{i1}, and select T_{idnew}, the time-stamp T_U. For a message m, compute $S_U = H(R_{i1} \Vert T_{id})$, $h = H(R_{i1} \Vert T_{\text{idnew}})$, $\hat{C} = E_{S_U}(A_i \Vert T_{id} \Vert T_U \Vert T_{\text{idnew}} \Vert h \Vert m)$.	$\xrightarrow[\text{open channel}]{\hat{C}, T_U, C_{i1}, T_{id}}$	Check if $T_C - T_U \le \triangle T$. Decrypt $\hat{C}$ and check the consistency of A_i, T_{id}. Verify that $h = H(R_{i1} \Vert T_{\text{idnew}})$. Update T_{id} with T_{idnew}.

the signification of an identifier. The findings could be helpful for the future work on designing anonymous key agreement schemes.

Acknowledgment

We thank the National Natural Science Foundation of China (61411146001). We are grateful to the reviewers for their valuable suggestions.

References

[1] M. Aazam, S. Zeadally, and K. Harras, "Deploying fog computing in industrial internet of things and industry 4.0," *IEEE Trans. Ind. Informatics*, vol. 14, no. 10, pp. 4674–4682, 2018.

[2] M. Aazam, S. Zeadally, and K. Harras, "Fog computing architecture, evaluation, and future research directions," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 46–52, 2018.

[3] M. Abdussami, R Amin, and S. Vollala, "LASSI: a lightweight authenticated key agreement protocol for fog-enabled iot deployment," *Int. J. Netw. Secur.*, vol. 21, no. 6, pp. 1373–1387, 2022.

[4] Z. Ali and *et al.*, "A clogging resistant secure authentication scheme for fog computing services," *Comput. Networks*, vol. 185, p. 107731, 2021.

[5] K. Anggriani, N. Wu, and M. S. Hwang, "Research on data hiding schemes for AMBTC compressed images," *Int. J. Netw. Secur.*, vol. 24, no. 6, pp. 1114–1123, 2022.

[6] S. Battula and *et al.*, "A generic stochastic model for resource availability in fog computing environments," *IEEE Trans. Parallel Distributed Syst.*, vol. 32, no. 4, pp. 960–974, 2021.

[7] Z. J. Cao, "A note on 'efficient provably-secure dynamic id-based authenticated key agreement scheme with enhanced security provision'," *IEEE Trans. Dependable Secur. Comput.*, doi 10.1109/TDSC.2023.3302300.

[8] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[9] P. Gope and B. Sikdar, "Privacy-aware authenticated key agreement scheme for secure smart grid communication," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3953–3962, 2019.

[10] M. S. Hwang, H. W. Li, and C. Y. Yang, "An improved of enhancements of a user authentication scheme," *Int. J. Netw. Secur.*, vol. 25, no. 3, pp. 508–514, 2023.

[11] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions," *J. Cloud Comput.*, vol. 6, p. 19, 2017.

[12] J. Kharel, H. Reda, and S. Shin, "An architecture for smart health monitoring system based on fog computing," *J. Commun.*, vol. 12, no. 4, pp. 228–233, 2017.

[13] P. Kumar and *et al.*, "Lightweight authentication and key agreement for smart metering in smart energy networks," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4349–4359, 2019.

[14] T. W. Lin and C. L. Hsu, "Chaotic maps-based privacy-preserved three-factor authentication scheme for telemedicine systems," *Int. J. Netw. Secur.*, vol. 25, no. 2, pp. 194–200, 2023.

[15] L. H. Liu and J. Cao, "Analysis of one lightweight authentication and key agreement scheme for internet of drones," *Int. J. Electron. Inf. Engineering*, vol. 13, no. 4, pp. 142–148, 2021.

[16] Y. C. Lu and M. S. Hwang, "A cryptographic key generation scheme without a trusted third party for access control in multilevel wireless sensor networks," *Int. J. Netw. Secur.*, vol. 24, no. 5, pp. 959–964, 2022.

[17] A. Menezes, P. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. USA: CRC Press, 1996.

[18] C. Mouradian and *et al.*, "A comprehensive survey on fog computing: State-of-the-art and research challenges," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 1, pp. 416–464, 2018.

[19] H. Pan, H. Yang, and M. Hwang, "An enhanced secure smart card-based password authentication scheme," *Int. J. Netw. Secur.*, vol. 22, no. 2, pp. 358–363, 2020.

[20] A. Rahmani and *et al.*, "Exploiting smart e-health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," *Future Gener. Comput. Syst.*, vol. 78, pp. 641–658, 2018.

[21] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[22] O. Salman and *et al.*, "Iot survey: An SDN and fog computing perspective," *Comput. Networks*, vol. 143, pp. 221–246, 2018.

[23] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of Annual Cryptology Conference, Advances in Cryptology (CRYPTO'84)*, pp. 47–53, Santa Barbara, California, USA, Aug. 1984.

Biography

Lihua Liu, associate professor with Department of Mathematics at Shanghai Maritime University, received her PhD degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics and cryptography.

Yingqing Jia is currently pursuing her master degree from Department of Mathematics at Shanghai Maritime University. Her research interests include information theory and applied mathematics.

Zhengjun Cao, associate professor with Department of

Mathematics, Shanghai University, received his PhD degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He had served as a post-doctor in Computer Sciences Department, Université Libre de Bruxelles. His research interests include cryptography, discrete logarithms and quantum computation.

Design and Implementation of a Central Node-controlled Off-chain Payment Channel Rebalancing Scheme

Wei-Jun Gao[1], Ya-Qian Yue[2], and Xiao-Qin Wang[3]

(Corresponding author: Ya-Qian Yue)

School of Computer and communication, Lanzhou University of Technology[1]

No. 36, Peng-Jia-Ping Road, Lanzhou 730050, China

Email:yyaqian2023@163.com

(Received Mar. 29, 2023; Revised and Accepted Nov. 24, 2023; First Online Feb. 23, 2024)

Abstract

The emergence of an off-chain payment channel network provides a reliable solution for blockchain scalability. However, channel imbalance in practical applications increases the transaction cost of nodes, leads to poor sustainability of payment channels, and even affects network stability. This paper proposes a central node-controlled off-chain payment channel rebalancing scheme for channel imbalance, using a combination of algorithms and smart contracts to establish a credible, safe, and win-win mutual rebalancing platform for nodes who want to achieve channel balance, and verifies the effectiveness of the scheme, providing a new idea of low consumption and no cost for the rebalancing channel.

Keywords: Blockchain; Channel Imbalance; Off-chain Payment Channel Network; Rebalancing

1 Introduction

With the development of technology and the deepening of information sharing, network attack methods emerge in an endless stream, and attackers try to steal, modify and abuse user information. In this context, network protection technology [1] is increasingly improved, such as privacy protection [2], key management [3], identity authentication [4] and other protective means are constantly optimized, and the birth of blockchain technology has become an effective tool for network security protection. Blockchain provides data security, autonomy, transparency, auditability, privacy, and many other benefits, and has been widely used in various fields such as finance, Internet of Things, healthcare, energy, Biometrics, and government affairs [5–10]. The off-chain payment channel network retains the advantages of blockchain security and decentralization [11], reduces the pressure on on-chain storage by moving transactions down the chain, ensures transaction processing volume, and enables low-cost and low latency transactions for on-chain micro-payments. However, channel imbalance [12] has become an important issue limiting the development of off-chain payment channel networks.

Channel imbalance is caused by excessive one-way payments at one end of the channel. Channel funds are transferred in one direction, and after several transfers, the distribution of funds at one end becomes zero, and if both ends of the channel want to transact at this point, the channel must be closed and a new channel established. The opening and closing of the channel need to be published on the chain, and the closing of the channel will increase the path length of transaction transmission of certain nodes, resulting in long transaction delays and high fees.

At present, there are two common ways to deal with the channel imbalance problem. One is routing to achieve channel rebalancing, which uses channels with a higher balance to transmit transactions, effectively avoiding further deterioration of unbalanced channels, but still lacks in improving the balance of imbalanced channels. Secondly, the node takes the initiative to achieve channel rebalancing and adopts the loop payment to eliminate the fund offset problem when channel imbalance is monitored, which improves the channel balance degree but increases the time and fund cost of the node to rebalance the channel. To address the shortcomings of the current channel rebalancing scheme, this paper proposes a central node-controlled off-chain payment channel rebalancing scheme, which adopts the way of mutual borrowing and lending by nodes at both ends of the channel to solve the channel imbalance problem, aiming to reduce the funds and time spent by nodes in the rebalancing process.

The organization of this paper is as follows. Section 2 mainly introduces the basic knowledge of off-chain payment channel networks. Section 3 describes the research status of the off-chain payment channel network and the main solutions to the problem of channel imbal-

ance. Section 4 shows the "central node control off-chain payment channel rebalancing scheme" model diagram and describes the detailed design and implementation process of each module in the model diagram. In Section 5, the experiment verifies the correctness, effectiveness and expansibility of the "central node-controlled off-chain payment channel rebalancing scheme". Section 6 summarizes the work done in this paper and discusses the limitations, applicability and future research direction of this scheme.

2 Background

Blockchain technology has been implemented in P2P networks without relying on trusted third parties, changing the existing payment model and creating a new type of commercial payment system, but it has problems such as low throughput and extended transaction times. The current mainstream payment platform, Visa, can process an average of *2,000* transactions per second [13], while blockchain can theoretically process up to *7* transactions per second [14]. In order to break the scalability bottleneck of blockchain, on-chain scaling technology, inter-chain scaling technology and off-chain payment channel network have emerged.

The on-chain expansion technology mainly has two ways to adjust the blockchain parameters and update the system consensus algorithm. Such as increasing the block size to increase the block capacity, changing the communication method between blockchain nodes to improve the block out rate, and updating the consensus algorithm to reduce the transaction confirmation time, but the technique has certain limitations, such as increasing the block size may lead to network congestion and updating the system consensus algorithm cannot be completed in a short period of time.

Inter-chain scaling is mainly based on cross-chain technology [15], which realizes blockchain scaling through inter-chain value transfer, however, this technology is in the concept certification stage, lacking commercial landing applications, and can not be quickly put into practical applications.

With the off-chain payment channel network [16], after both parties to a transaction create a payment channel with a smart contract, both parties can make multiple transactions. If one party has a desire to close the channel or disputes a transaction in the process, the blockchain will act as an arbitration platform to check and confirm the status of the channel. The network ensures that transactions are executed correctly and securely by running a Recoverable Sequence Maturity Contrace (RSMC) and single-path atomic transactions and cross-channel transactions by running a Hashed Timelock Contracts (HTLC).

2.1 Payment Channels

A payment channel is a transaction path created peer-to-peer by both parties to a transaction, allowing both parties to update and maintain the funds in the channel off-chain, thereby enabling off-chain payments. The process of off-chain channel payments consists of following steps. First, open a channel. Each party to the transaction takes out funds and deposits them into the channel to generate the initial transaction. Both parties attach signatures to the initial transaction and broadcast it to the chain, indicating the completion of the channel creation. Second, Conduct the transaction. Both sides of the transaction exchange funds in the channel and the distribution of funds in the channel will be updated after each transaction. In the process, if one side maliciously publishes a false transaction, all the funds of the user in the channel will be returned to the other side as a penalty. Finally, Close the channel. When one side of the channel runs out of funds or wants to leave the channel, any side of the channel only needs to publish the latest channel status to the chain, and after the status is published, it means the channel closure is completed.

2.2 Payment Channel Network

The formation of a payment channel network not only enables users to transact across channels, but also reduces the pressure on network channel information storage. In the network, users who do not create a channel want to make transactions, the routing algorithm will find a suitable path for them to transmit the transaction, and the sender of the transaction only needs to pay the intermediate node transaction forwarding fees. For a better understanding, the illustration of the cross-channel trading is given in Figure 1.

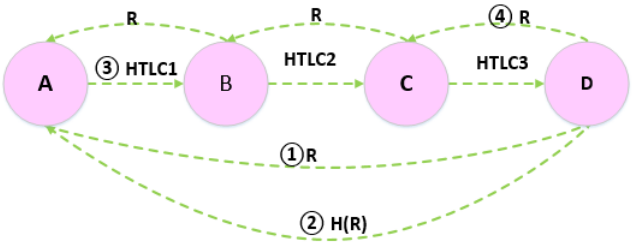


Figure 1: The illustration of the cross-channel trading

Suppose user A wants to transact with D, but no payment channel is established between A and D. The transaction execution process is as follows: A randomly generates the original image R and passes R to D; D hashes the received R to generate H(R) and passes it to A; A executes the routing algorithm to find the transaction transmission path A− >B− >C− >D that can reach D. Each node in the path signs a time lock with the neighboring

node respectively. After the time lock contract on the transmission path is signed, user D presents the original image R of H(R) to C to unlock the funds from C. Then R is passed to the next user in turn to unlock the funds of the neighboring users. Finally, the transaction between user A and D is realized, and for users B and C who transmit the transaction, they will receive a transmission fee, which is generally relatively low.

3 Related Work

When the off-chain payment channel network was created, its research mainly focused on routing algorithms, such as the hybrid routing algorithm Flare [17], which used a combination of common nodes and beacon nodes to find paths for payment nodes, improved the path finding rate and decentralized centralization, and laid a consolidated foundation for the routing algorithms that followed. In recent years, routing algorithms have considered some inherent limitations in the network, such as fund overload [18], channel imbalance [19], routing cost [20], and security issues [21]. For channel imbalance, Giovanni et al. [22] proposed to reduce channel imbalance by charging transaction fees at the gateway nodes, the rate of which depends on the balance difference between the nodes at both ends of the channel; Khalil et al. [23] proposed REVIVE, which allows any set of users to safely rebalance the channel according to the channel owner's preference, to ensure the balance of funds between the forwarding nodes. Mercan et al. [18] proposed balance-aware routing, which calculates the channel imbalance before the transaction is forwarded and then selects the gateway to be forwarded, thus alleviating the channel imbalance. Conoscenti et al. [24] proposed a passive rebalancing scheme to reduce the payment failure rate due to channel imbalance. Hong et al. [25] proposed the asynchronous rebalancing idea CYCLE, where imbalanced nodes eliminate the fund offset by implementing loop payments on closed-loop routing. Avarikioti et al. [26] proposed an optional rebalancing protocol that effectively decomposes the rebalancing solution into incentive-compatible cycles, thus preserving the node balance while atomic payments are executed.

With the development and growth of off-chain payment channel networks, studies on topological properties have emerged, such as Seres [27] on the degree distribution, robustness, and random failures of (Lightning Network LN), Guo et al. [28] on the connectivity, channel capacity, and routing efficiency of LN, Zabka et al. [29] on the geographical distribution of LN, and Lisi et al. [30] on the topology of lightning networks for a specific time period.

Later work has shown that there are security risks in off-chain payment channel networks [31], such as Malavolta et al. [32] described possible wormhole attacks in LN networks, followed by the multi-hop anonymity and privacy-preserving payment channel network MAPPCN [33], and for attack models, such as Thakur et al. [34] proposed a conspiracy attack and Perez et al. [35] proposed a balance detection attack. There are also researches on the privacy protection of off-chain Payment channel networks. Zhang et al. [36] proposed a hybrid multi-hop mechanism, including Payment channel network PCN, Onion routing and side chain, so as to ensure privacy-protecting off-chain payment. The CryptoMaze protocol proposed by Mazumdar et al. [37] not only avoids the formation of multiple off-chain contracts on the side of the path sharing of routing partial payments, but also ensures the no-connectibility of partial payments.

4 Scheme Design

4.1 Design Ideas

In this paper, a channel rebalancing network is formed in which each node has a channel rebalancing mini-network centered on itself, and the channel balancing degree in the mini-network is set by the central node as a way to limit the payment behavior of each node and keep the channel within a certain balancing degree.

For the nodes in the off-chain payment channel network that want to participate in the channel rebalancing network, they need to submit the channel information that they have created. After receiving the channel information from the node, the channel rebalancing network creates a rebalancing channel information table centered on the node. All nodes in the channel rebalancing network that meet the channel rebalancing requirements need to execute the channel rebalancing operation unconditionally. In the design, the following points are considered:

1) Information security, the distribution of funds of the nodes in the channel is not leaked.

2) Capital protection, no loss of node funds during rebalancing operation.

3) No impact on the normal trading activities of the nodes.

According to the above requirements, this paper divides the rebalancing scheme into three modules,channel screening, rebalancing execution and channel clearing. The scheme principle is shown in Figure 2.

Channel Screening Module: Screen the channels in the rebalancing channel information table that needs to adjust the fund distribution and calculate the funds needed to rebalance the channel.

Rebalancing execution module: According to the rebalancing funds calculated by the channel screening module, rebalancing transfers are executed on the corresponding channels.

Channel clearing module: When a node leaves the channel rebalancing network, in order to ensure that the nodes in the network do not lose funds in the rebalancing process, it can leave only after clearing the channel debt relationship connected with the node, at which time the

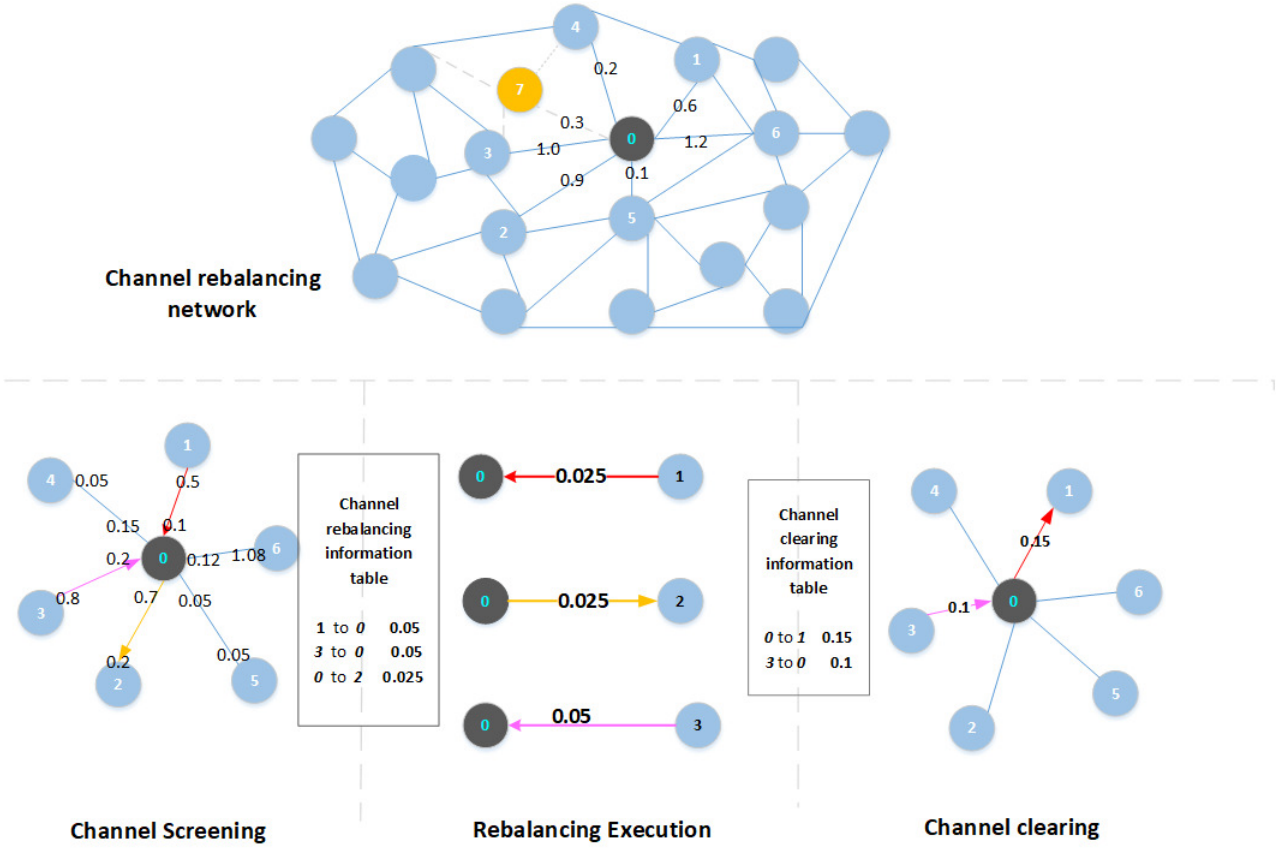


Figure 2: Channel rebalancing scheme diagram

network automatically clears the information of the leaving node and the channel information connected with the node.

Considering that cross-channel rebalancing may affect the trading activities of nodes, the design is such that each node only actively regulates the payment channel it creates and places the execution of rebalancing in idle time when the node has no trading activities. In this way, cross-channel rebalancing will not be involved, and due to the immediacy of the transaction of the created channel, it will not affect the normal transaction activities of nodes.

Nodes that want to participate in the channel rebalancing network, before entering the network, have to submit their own channel information form. Considering the information security, the information provided only includes the addresses and channel capacity of nodes at both ends of established channels that are publicly in the payment channel network. Taking node *0* in 2 as an example, the submitted channel information is shown in Table 1.

After receiving the node channel information, compare the node information of the channel rebalancing network and create a node-centered rebalancing channel information table, which contains the node addresses and fund distribution at both ends of the channel, and the table is only stored at the central node, which is not involved in the channel fund distribution leakage problem because it is established about the channel information table created

Table 1: Node *0* channel information table

Node1	Node2	Capacity
0	1	0.6
0	2	0.9
0	3	1.0
0	4	0.2
0	5	0.1
0	6	1.2
0	7	0.3

by the central node. For example, according to Table 1 submitted by node *0*, after comparing with the nodes in the network, it is found that node *7* is not involved in the channel rebalancing network, so the rebalancing information created for node *0* is shown in Table 2.

4.2 Detailed Design

4.2.1 Model Definition

We represent the channel rebalancing network as a digraph $G^{'} = \left(V^{'}, E^{'}\right)$ where $V^{'} = \{v_1, v_2, v_3, ...v_n\}$ is the set of nodes in $G^{'}$, $e^{'}_{i,j} \in E^{'} = \left\{(v_i, v_j) \,|v_i, v_j \in V^{'}\right\}$

Table 2: Node 0 channel information table

Node1	Node2	Balance1	Balance2	Capacity
0	1	0.1	0.5	0.6
0	2	0.7	0.2	0.9
0	3	0.2	0.8	1.0
0	4	0.15	0.05	0.2
0	5	0.05	0.05	0.1
0	6	0.12	1.08	1.2

is the set of edges in $E^{'}$. Take any node i in $V^{'}$, We define the small network formed by the central node i as a directed graph $G_N^i = \left(V_N^i, E_N^i\right)$, where $V_N^i = \left\{v_{N_1}, v_{N_2}, v_{N_3}, ...v_{N_k|k\leq n}\right\}$ is the set of nodes in $G_N^{'}$, $e_{N_{i,j}}^i \in E_N^i = \left\{\left(v_{N_i}, v_{N_j}\right)|v_{N_i}, v_{N_j} \in V_N^i\right\}$ is the set of channel edges in G_N^i. The funds deposited by nodes i and j when creating a channel are denoted as b_{N_i} and b_{N_j}, and the channel capacity is denoted as $c_{N_{i,j}}$, we have:

$$c_{N_{i,j}} = b_{N_i} + b_{N_j} \tag{1}$$

For the channel $e_{N_{i,j}}^i$, we define the imbalance degree of the channel as $b_{i,j}^{im}$:

$$b_{i,j}^{im} = \frac{|b_{N_i} - b_{N_j}|}{c_{N_{i,j}}} \qquad b_{i,j}^{im} \in (0,1) \tag{2}$$

In Formula (2), when $b_{N_i} = b_{N_j}$, we have $b_{i,j}^{im} = 0$, then equation (2) is also equivalent to:

$$\frac{b_{N_i}}{c_{N_{i,j}}} = \frac{b_{N_j}}{c_{N_{i,j}}} = 0.5 \tag{3}$$

Formula (3) indicates the most ideal channel equilibrium state, that is, the same funds at both ends of the channel, but it is difficult to achieve this situation in the real network, so we set a changeable value $b_{i,j}^{im^{'}}$ to indicate the difference between the channel imbalance degree acceptable to the central node and the optimal balance degree *0.5* in the small network formed by the central node, the value is set by the central node V_{N_i}. That is, the channel unbalance that the central node refuses to accept. The funds of the node i will remain within the variation δ_1 and δ_2, node i funding will meet $b_{N_i} \in (\delta_1, \delta_2)$, there are:

$$\left\{\begin{array}{l} \delta_1 = c_{N_{i,j}} * \left(0.5 - b_{i,j}^{im^{'}}\right) \\ \delta_2 = c_{N_{i,j}} * \left(0.5 + b_{i,j}^{im^{'}}\right) \end{array}\right\} \tag{4}$$

The channel selection algorithm will be designed based on the funding requirements of node i in Formula (4).

4.2.2 Model Implementation

The channel selection module is implemented by FindRebalancingChannel(FRC) algorithm, which is used to find out the imbalanced channel in $G_N^i = \left(V_N^i, E_N^i\right)$ and calculate the funds required for the channel rebalancing. The algorithm pseudo-code is shown in Algorithm 1.

Algorithm 1 FRC

Input: $ReInfor = ReChannelInformlist$, $b_{i,j}^{im^{'}}$
1: $OPB = 0.5$
2: **for** $c_{N_{i,j}}$ in *ReInfor* **do**
3: $\delta_1 = c_{N_{i,j}} * (OPB - b_{i,j}^{im^{'}})$
4: $\delta_2 = c_{N_{i,j}} * (OPB - b_{i,j}^{im^{'}})$
5: **end for**
6: **for** b_{N_i} in *ReInfor* **do**
7: **if** $b_{N_i} < \delta_1$ **then**
8: $ReBalance = b_{N_i} - \delta_1$
9: **end if**
10: **if** $b_{N_i} > \delta_2$ **then**
11: $ReBalance = b_{N_i} - \delta_2$
12: **end if**
13: **end for**
Output: $C\_id, ReBalance$

Algorithm 1 is based on the acceptable imbalance value $b_{i,j}^{im^{'}}$ rejected by the central node to calculate the capital balance range $[\delta_1, \delta_2]$ of all channels centered on this node. If the funds at the end of the central node i are not in the range, the channel is picked out. The calculated rebalancing fund *ReBalance*, a positive value, indicates the the channel imbalance is caused by the higher-end funds of the central node i than the j end funds. At this time, the channel imbalance needs to be solved by transferring funds from i end to the j end. A negative value indicates that the channel imbalance is caused by higher funds at the node j end is higher than the central node i, and the imbalance needs to be resolved by transferring funds from j end to the i end.

In Rebalancing execution module, perform rebalancing transfer on the selected unbalanced channel. Before rebalancing transfer, set up fund detection to ensure that the node funds at both ends of the channel are not lost. The Rebalancing contract designed in this paper is shown in Algorithm 2.

In Algorithm 2, the transfer direction is judged first. A positive *ReBalance* value indicates that the transfer direction is from the node i to j, which means that the node i is helping the node j to balance the channel they have established by borrowing, and then checking whether the node j has the ability to repay, which is shown in the contract as *ReBalance*$<b_{N_j}$ the rebalancing transfer can only be performed if the contract is, otherwise, the rebalancing fails. Similarly when *ReBalance* is negative, to perform a rebalancing transfer, it is necessary to satisfy *ReBalance*$<b_{N_i}$. In this module, it is also necessary to record the *ReBalance* of each rebalancing transfer in each channel, which is used for the liquidation of the next module.

In Channel clearing module, before a node leaves the

Algorithm 2 Rebalancing

Input: $b_{N_i} = getBalance\,(account_i)$
$b_{N_j} = getBalance\,(account_j)$
int[] $ClearBalance = [0]$
if $ReBalance > 0$ **then**
  if $ReBalance < b_{N_j}$ **then**
    reTransfer($account_j$)
    pushContent($ReBalance$)
  end if
else
  if $|ReBalance| < b_{N_i}$ **then**
    reTransfer($account_i$)
    pushContent($ReBalance$)
  end if
end if
Output: $ClearBalance$

network, it must clear the debts of all channels connected to it. This capability is implemented through the CleanChannel contract shown in Algorithm 3.

Algorithm 3 CleanChannel

int $total = 0$
for $i = 0; i <$ ClearBalance.length; i++ **do**
  $total = total + ClearBalance[i]$
end for
if $total > 0$ **then**
  reTransfer($account_i$)
else
  reTransfer($account_j$)
end if

In Algorithm 3, the *ReBalance* of the channel's historical rebalancing transfer is first cleared, and the result is placed in *total*. The positive or negative value of *total* indicates the direction of debt repayment, and the positive values indicate that in the rebalancing prosess with the help of the nodes i of mutual funds is more than node j, then the node j needs to repay the excess fund of node i. Similarly, a negative value of *total* means that the node i needs to repay the excess funds from the node j. Based on the positive and negative values of *total*, the repayment transfer is then executed.

5 Experiments and Analysis of Results

5.1 Validating the FRC Algorithm

5.1.1 Experimental Design

This experiment collectes the channel capacity created at a node named bfx-lnd1 in LN at some point on March 2, 2023, and its frequency distribution is shown in Figure 3.

Figure 3 shows that the channel capacity created by this node is mostly distributed within *0* to *2* BTC, with

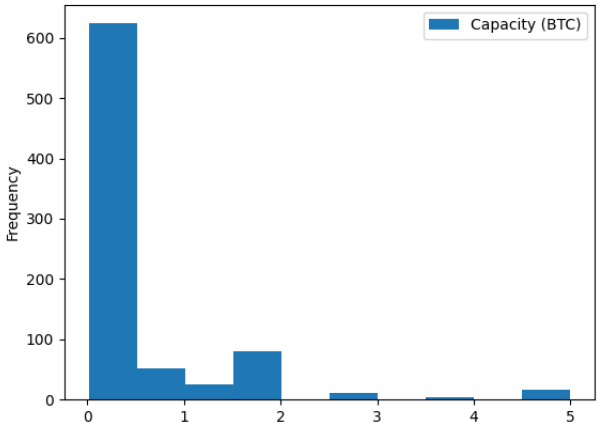


Figure 3: Channel capacity created by bfx-lnd1 nodes

only a few channels exceeding *2* BTC. In the channel capacity shown in the figure above, this paper randomly selected *100* channel capacities to participate in the channel rebalancing network of this scheme. Since the fund distribution at both ends of the channel is not available in the network, for the distribution of funds at both ends of the channel, this paper generates the channel rebalancing network by taking a random number in *0* and $c_{N_{i,j}}$, and the two ends of the funds satisfy the following condition.

$$\left\{ \begin{array}{l} b_{N_i} \quad | \quad b_{N_i} \in [0, c_{N_{i,j}}] \\ b_{N_j} + b_{N_j} = c_{N_{i,j}} \end{array} \right\} \tag{5}$$

The fund distribution at both ends of the *100* channels generated by the above method is shown in Figure 4.

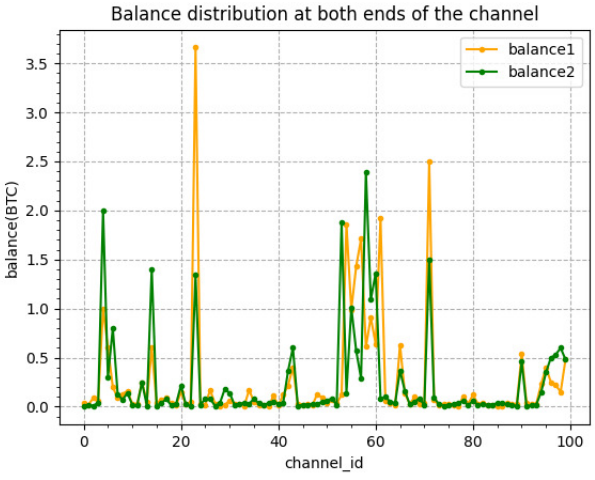


Figure 4: Distribution of funds at both ends of the channel

Figure 4 shows that among the *100* channels, most channels have channel imbalance problems, and among

the unbalanced channels, there are extremely unbalanced channels. But there are a few channels where the distribution of funds relatively balanced. Following that, the channel imbalance $b_{i,j}^{im}$ of the *100* channels selected above is calculated, and their distributions are shown in Figure 5.

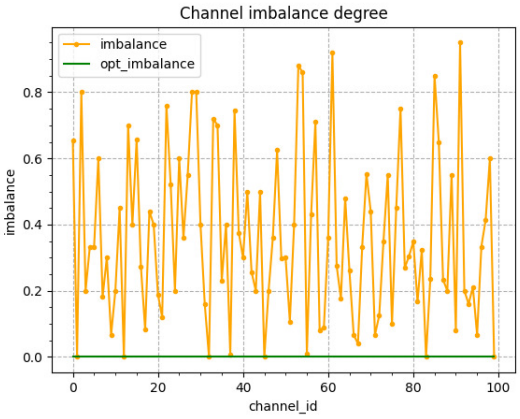


Figure 5: Channel imbalance degree

The green line in Figure 5 shows the optimal balance of *0.5*, and the yellow line shows the imbalance $b_{i,j}^{im'}$ of the channel. As can be seen from Figure 5, most channels deviate from the optimal balance, and the number of channels included in different balance levels is different. For the FRC algorithm mentioned in Section 4.2.2, we make the following analysis:

1) The smaller the $b_{i,j}^{im'}$, the more channels need to be rebalanced. The reason is that most channels will meet the channel balance requirements set by the central node V_{N_i} with the fund range of the node (δ_1, δ_2) increasing.

2) As $b_{i,j}^{im'}$ increases, the gap between the average paying capacity of channels and that of channels before the implementation of the rebalancing scheme will narrow. This is because the (δ_1, δ_2) shrinks with $b_{i,j}^{im'}$ increasing, indicating that the central node has a higher requirement on the balance degree of channels in the network, and at this time, only a few channels participate in the rebalancing scheme. Therefore, the average paying capacity of channels in a small network composed of central nodes will not increase significantly.

According to the above analysis, we need to perform the FRC algorithm under different $b_{i,j}^{im'}$. To measure the number of channels that can perform rebalancing operations and the average payment capacity of channels in the small network composed of central nodes.

5.1.2 Results Analysis

In this paper, we implement the FRC algorithm in Python language and measure the span of *0.005* as $b_{i,j}^{im'} \in [0.00,0.50]$, within the different $b_{i,j}^{im'}$ under the execution of the FRC algorithm, the number of channels that can perform rebalancing operations is collected from volume and the average channel payment capacity in a small network composed of central nodes, and the results are shown in Figure 5 and Figure 6 respectively.

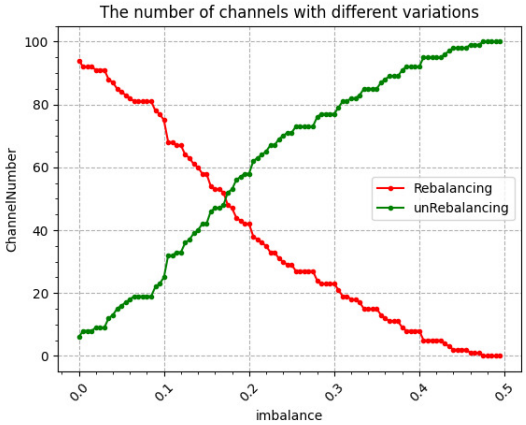


Figure 6: Number of channels

In Figure 6, the red dash indicates the number of channels that can be adjusted by the rebalancing scheme under a certain imbalance degree that the central node refuses to accept. As can be seen from the trend of Figure 6, with the increase of imbalance degree, the number of adjustable channels is decreasing. The green dash line indicates the number of channels which cannot be adjusted by rebalancing scheme under a certain imbalance degree, and their number shows an upward trend with the increase of imbalance. Notably, at the same imbalance, there is $unRebalancing + Rebalancing = 100$.

In Figure 7, the blue broken line represents the average payment capacity of channels in a small network composed of central nodes after the execution of a rebalancing scheme in an imbalance degree. The average payment capacity of channels in the network decreases with the increase of imbalance. The yellow broken line represents the average paying capacity of channels when no rebalancing operation scheme is executedin a imbalance. As can be seen from Figure 7, with the increase of imbalance, the gap between them decreases obviously. When imbalance increases to a certain extent, the two broken lines actually coincide. In this case, it means that the rebalancing scheme loses its rebalancing ability, so the central node should avoid this critical value when choosing an acceptable imbalance degree imbalance. In this experiment, the critical value is equal to *0.475*.

Through the above experiments, the rationality of 5.1.1 analysis on FRC algorithmis proved, and the effectiveness

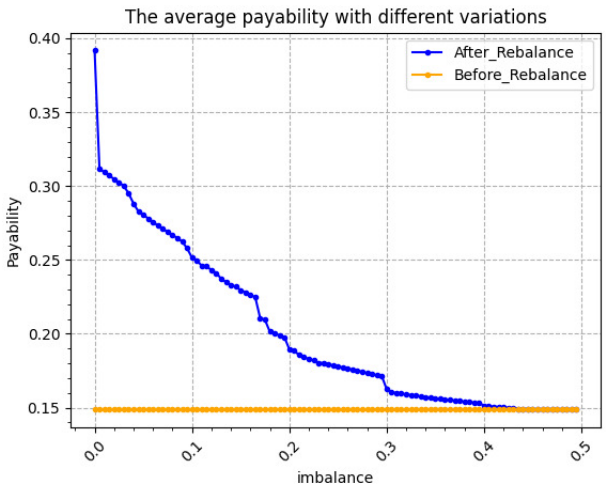


Figure 7: Channel Average Payment Capacity

of FRC algorithm in improving channel balance degree is verified.

5.2 Validating Smart Contracts

5.2.1 Experimental Design

This paper implements the Rebalancing and CleanChannel contracts on Remix, the official open-source online integrated development environment of Ethereum. For the Rebalancing contract, the functional requirements are verified by testing the Rebalancing greater than 0 and less than 0 mentioned in 4.2.2, as shown in Table 3.

The CleanChannel contract needs to calculate the sum of the Rebalancing values recorded by the Rebalancing contract, and realize the repayment operation in the corresponding *ReBalance* account according to the positive and negative values. Its test table is shown in Table 4.

5.2.2 Results Analysis

According to the Rebalancing and CleanChannel contract testing requirements in 5.2.1, the *ReBalance* values shown in Table were set in this paper, and the test results are shown in Table 5.

Let *ReBalance = 100,000,000,000,000,000,000* sat, in Table 5, the first judgment rebalancing transfer direction is b_{N_i} to b_{N_j}, and then determine b_{N_i} whether there is the ability to repay, because the b_{N_i} account balance is *999,999,999,999,993,876,17* sat, less than *100,000,000,000,000,000,000* sat, so it is not executed the b_{N_i} transfers *100,000,000,000,000,000,000* sat to b_{N_j}. When *ReBalance = -200* sat, the first judgment rebalancing transfer direction is b_{N_j} to b_{N_i} transfer *200* sat, and then check b_{N_i} whether there is the ability to repay, and since the b_{N_i} balance at this time is *999,999,999,999,965,105,60* sat, which is completely greater than *200* sat, so the execution of b_{N_j} to b_{N_i} transfer *200* sat, the b_{N_i} balance is *999,999,999,999,965,107,60* sat after transfer b_{N_i}. The analysis of the above results shows that the Rebalancing contract is designed to meet the requirements for rebalancing under certain conditions.

According to the rebalancing values recorded in Rebalancing contract, CleanChannel contract is executed, and the measured funds at both ends of the channel are shown in Table 6.

In Table 6, after the two rebalancing transfers in Table 5, the clearing yields *total = -100* sat, indicating that during the rebalancing b_{N_i} has made use of an extra b_{N_j} *100* sat, at this time, the b_{N_j} balance is *999,999,999,999,989,998,06* sat, and after receiving *100* sat from b_{N_i}, the b_{N_j} balance is *999,999,999,999,989,999,06* sat. The successful transfer from b_{N_i} to b_{N_j} indicates that the CleanChannel contract we designed implements channel clearing function.

In Tables 5 and 6, the data highlighted in red indicate that the experimental values do not match the theoretical values. We find that the experimental values are lower than the theoretical values in red-marked data. The reason for this deviation is that when the contract is deployed on the Remix platform, the platform automatically adds the cost of executing the contract, and the cost is spent by the account where the contract is deployed, so when the account executes the contract, the balance of the account will be lower than the value of balance before the account is spent minus the spent funds. Taking *ReBalance = 100* sat in Table 5 as an example when b_{N_i} paying *100* sat to b_{N_j}, the b_{N_i} balance should be *999,999,999,999,937,279,64* sat, but it is only *999,999,999,999,937,233,52* sat, and the decrease *416,2* sat is used as a fee for the execution of this contract.

5.3 Solution Scalability Verification

In order to verify the scalability of the scheme, *1500* channels in LN were randomly selected for experiments. First, the average channel unbalance degree of these channels is calculated, and the calculated result is *0.0977*. Then, with a span of *0.02*, $b_{i,j}^{im'} \in [0.00, 0.10]$, we measured the change of the average paying capacity of channels in the small network formed by the central node as the number of channels increases, and then calculate the increasing multiple of the average paying capacity of channels after using different schemes. The experimental results are shown in Figures 8 and 9.

In Figure 8, different colors of broken lines represent different $b_{i,j}^{im'}$ values, the virtual broken line represents the average channel payment ability before the implementation of the plan, and the solid line represents the average channel payment ability after the implementation of the plan.The results show that: under the same $b_{i,j}^{im'}$, the average paying capacity of channels is significantly improved after the implementation of the scheme, and the increasing trend is not affected by the number of channels, which indicates that the scheme has good scalability. Under dif-

Table 3: Rebalancing Contract test table

Rebalancing transfer direction	**Rebalancing transfer, conditions**	b_{N_i} **theoretical value**	b_{N_j} **theoretical value**
$ReBalance>0$	$ReBalance<b_{N_j}$	$b_{N_i} - ReBalance$	$b_{N_j} + ReBalance$
	$ReBalance>b_{N_j}$	b_{N_i}	b_{N_j}
$ReBalance<0$	$\|ReBalance\|>b_{N_i}$	b_{N_i}	b_{N_j}
	$\|ReBalance\|<b_{N_i}$	$b_{N_i} + ReBalance$	$b_{N_j} - ReBalance$

Table 4: CleanChannel contract test table

Channel clearing value	**Reimbursement, direction**	b_{N_i} **theoretical value**	b_{N_j} **theoretical value**
$total$	$total>0$	$b_{N_i} + total$	$b_{N_j} - total$
	$total<0$	$b_{N_i} - total$	$b_{N_j} + total$

Table 5: Rebalancing contract execution after both ends of the channel funding table

***ReBalance*(sat)**	b_{N_i}, **(sat)**	b_{N_j} **(sat)**	$\mathbf{1}b_{N_i}$ **(sat)**	$\mathbf{1}b_{N_j}$ **(sat)**	$\mathbf{1}b_{N_i}$ **theoreti. value (sat)**	$1b_{N_j}$ **theoreti. value (sat)**
100	*999,999, 999,999, 937,280, 64*	*999,999, 999,999, 993,875, 17*	*999,999, 999,999, 937,233, 52*	*999,999, 999,999, 993,876, 17*	*999,999, 999,999, 937,279, 64*	*999,999, 999,999, 993,876,* 17
100,000,000,000,000,000,000,	*999,999, 999,999, 936,233, 52*	*999,999, 999,999, 993,876, 17*	*999,999, 999,999, 935,223, 52*	*999,999, 999,999, 993,876, 17*	*999,999, 999,999, 936,233, 52*	*999,999, 999,999, 993,876, 17*
-200	*999,999, 999,999, 965,105, 60*	*999,999, 999,999, 953,583, 80*	*999,999, 999,999, 965,107, 60*	*999,999, 999,999, 953,529, 80*	*999,999, 999,999, 965,107, 60*	*999,999, 999,999, 953,581, 80*
-100,000,000,000,000,000,009	*999,999, 999,999, 996,510, 60*	*999,999, 999,999, 952,529, 60*	*999,999, 999,999, 996,510, 60*	*999,999, 999,999, 951,529, 60*	*999,999, 999,999, 996,510, 60*	*999,999, 999,999, 952,529, 60*

Table 6: CleanChannel contract execution after both ends of the channel funding table

***total*(sat)**	b_{N_i}, **(sat)**	b_{N_j} **(sat)**	$\mathbf{1}b_{N_i}$ **(sat)**	$\mathbf{1}b_{N_j}$ **(sat)**	$\mathbf{1}b_{N_i}$ **theoretical value (sat)**	$\mathbf{1}b_{N_j}$ **theoretical value (sat)**
-100	*999,999, 999,999, 950,375, 11*	*999,999, 999,999, 989,998, 06*	*999,999, 999,999, 950,061, 23*	*999,999, 999,999, 989,999, 06*	*999,999, 999,999, 950,374, 11*	*999,999, 999,999, 989,999, 06*

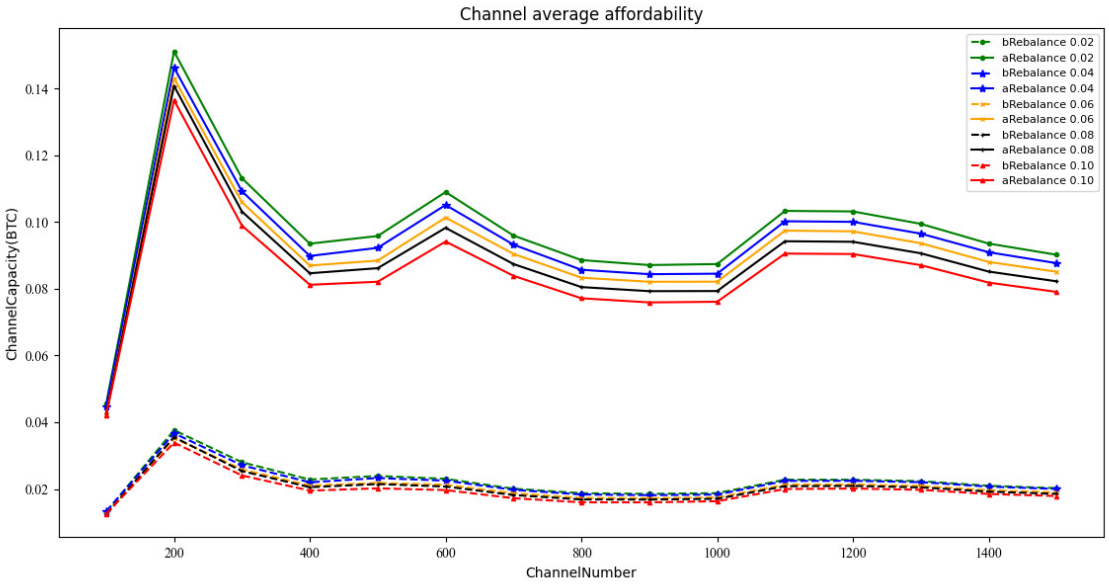


Figure 8: Channel average affordability

ferent scenarios, before and after the implementation of the scheme, there is a significant increase in the average payment capacity of the channel as $b_{i,j}^{im'}$ the average payment capacity of the channels decreases as the number of channels increases, the reason for this phenomenon is that as the $b_{i,j}^{im'}$, which is due to the fact as the number of channels increase, the central node's balancing requirements for the entire network increase, marking the rebalancing ability weaker and therefore the average payment capacity of the channel decreases. Several peaks in the graph casused by the relatively large initial funds at both ends of each newly added channel, and have no special meaning.

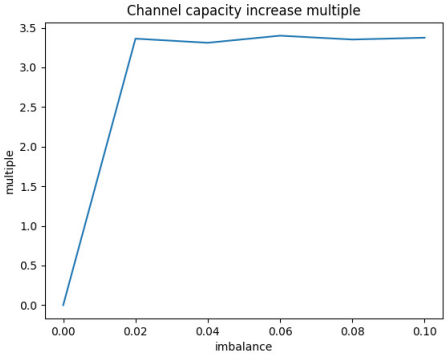


Figure 9: Channel capacity increase multiple

The broken line in Figure 9 shows the increase multiples of the average paying capacity of channels after using the scheme compared with before using it under different $b_{i,j}^{im'}$. As can be seen from the figure, the increase multiples are basically stable between 3 and 3.5 times, indicating that the scheme has a significant effect on improving the average paying capacity of channels.

6 Conclusions

Aiming at the channel imbalance problem in the off-chain payment channel network, this paper proposes an off-chain payment channel Rebalancing scheme controlled by the central node, and designs the channel selection algorithm FRC, smart contract rebalancing and CleanChannel to implement the scheme. The main contributions of this paper are as follows:

1) Through the hierarchical use of node and channel information, not only protects the privacy of nodes and channels, but also ensures the integrity of information required by the central node when rebalancing channels.

2) Channel selection algorithm FRC, so that the nodes in the off-chain payment channel network can flexibly adjust the fund distribution of the fund needs, so as to improve the channel balance.

3) Rebalancing contract is proposed, which realizes the rebalancing operation and avoids the risk of the node losing funds by checking the fund balance at both ends of the channel.

4) The designed CleanChannel contract fully guarantees that the funds of nodes will not be lost in the rebal-

ancing process, and further guarantees the reliability of the rebalancing scheme.

The "off-chain payment channel rebalancing scheme controlled by central node" not noly reduces the cost of node rebalancing channel, but also improves the flexibility and durability of the payment channel. The scheme will hopefully be applied to lightning Network, Raiden Network, Celer Network, etc, thus enabling the off chain payment channel network to provide reliable and efficient payment solutions in various scenarios such as real-time payment, high-frequency trading, micropayment, micropayment and Internet of Things payment, and to promote innovation and development in the payment field.

However, when setting the channel imbalance degree $b_{i,j}^{im'}$ rejected by the central node, the scheme does not consider the difference in the demand for the balance degree of each channel in the small network composed of the central node, and lacks the dynamic analysis of the channel. In the future work, we will study the current mainstream off-chain payment channel network and design a more flexible one for the central node. In addition, the active protection of node channel fund information needs to be strengthened, and then we will create a stronger fortress for channel fund information through information access control, information encryption and other means.

Acknowledgments

This study was supported by the National Natural Science Foundation of China (No.61762059). The authors are also particularly grateful to the reviewers for their suggestions.

References

[1] Z. Guo, "Cryptanalysis of a certificateless conditional privacy-preserving authentication scheme for wireless body area networks," *International Journal of Electronics and Information Engineering*, vol. 11, no. 1, pp. 1–8, 2019.

[2] M. M. Nabi and F. Nabi, "Cybersecurity mechanism and user authentication security methods," *International Journal of Electronics and Information Engineering*, vol. 14, no. 1, pp. 1–9, 2022.

[3] L. Liu and J. Cao, "Analysis of one lightweight authentication and key agreement scheme for internet of drones," *International Journal of Electronics and Information Engineering*, vol. 13, no. 4, pp. 142–148, 2021.

[4] P. Fan, Y. Liu, J. Zhu, X. Fan, and L. Wen, "Identity management security authentication based on blockchain technologies." *Int. J. Netw. Secur.*, vol. 21, no. 6, pp. 912–917, 2019.

[5] L. Xue, "The application of blockchain technology in the financial field," in *2021 International Conference on Forthcoming Networks and Sustainability in AIoT Era (FoNeS-AIoT)*. IEEE, 2021, pp. 130–134.

[6] T. Alam, "A survey on the use of blockchain for the internet of things," *International Journal of Electronics and Information Engineering*, vol. 13, no. 3, pp. 119–130, 2021.

[7] D. Sentausa and D. Habsara Hareva, "Decentralize application for storing personal health record using ethereum blockchain and interplanetary file system," in *2022 1st International Conference on Technology Innovation and Its Applications (ICTIIA)*, 2022, pp. 1–6.

[8] U. Cali, M. Kuzlu, S. N. Gupta Gourisetti, S. Mishra, M. Pasetti, C. Lima, T. Hughes, F. Rahimi, and P. Nitu, "Standardization efforts for blockchain in energy domain and power grid applications," in *2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain)*, 2022, pp. 1–6.

[9] J. Du, L. Li, X. Xiong, and Y. Zheng, "A blockchain covert communication method based on voting contract," in *2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA)*, 2023, pp. 1280–1282.

[10] N. Hamian, M. Bayat, M. R. Alaghband, Z. Hatefi, and S. M. Pournaghi, "Blockchain-based user re-enrollment for biometric authentication systems," *IJ of Electronics and Information Engineering*, vol. 14, no. 1, pp. 18–38, 2022.

[11] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, "A survey on blockchain technology: Evolution, architecture and security," *Ieee Access*, vol. 9, pp. 61 048–61 073, 2021.

[12] R. Pickhardt and M. Nowostawski, "Imbalance measure and proactive channel rebalancing algorithm for the lightning network," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2020, pp. 1–5.

[13] R. Dennis and J. P. Disso, "An analysis into the scalability of bitcoin and ethereum," in *Third International Congress on Information and Communication Technology: ICICT 2018, London*. Springer, 2019, pp. 619–627.

[14] A. Gervais, "On the security, performance and privacy of proof of work blockchains," Ph.D. dissertation, ETH Zurich, 2016.

[15] S. Lin, Y. Kong, S. Nie, W. Xie, and J. Du, "Research on cross-chain technology of blockchain," in *2021 6th International Conference on Smart Grid and Electrical Automation (ICSGEA)*. IEEE, 2021, pp. 405–408.

[16] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. Gün Sirer *et al.*, "On scaling decentralized blockchains: (a position paper)," in *International conference on financial cryptography and data security*. Springer, 2016, pp. 106–125.

[17] P. Prihodko, S. Zhigulin, M. Sahno, A. Ostrovskiy, and O. Osuntokun, "Flare: An approach to routing in lightning network," *White Paper*, vol. 144, 2016.

[18] S. Mercan, E. Erdin, and K. Akkaya, "Improving transaction success rate in cryptocurrency payment channel networks," *Computer Communications*, vol. 166, pp. 196–207, 2021.

[19] L. M. Subramanian, G. Eswaraiah, and R. Vishwanathan, "Rebalancing in acyclic payment networks," in *2019 17th International Conference on Privacy, Security and Trust (PST)*. IEEE, 2019, pp. 1–5.

[20] E. Erdin, M. Cebe, K. Akkaya, S. Solak, E. Bulut, and S. Uluagac, "A bitcoin payment network with reduced transaction fees and confirmation times," *Computer Networks*, vol. 172, p. 107098, 2020.

[21] H. Xue, Q. Huang, and Y. Bao, "Epa-route: Routing payment channel network with high success rate and low payment fees," in *2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2021, pp. 227–237.

[22] G. Di Stasi, S. Avallone, R. Canonico, and G. Ventre, "Routing payments on the lightning network," in *2018 IEEE international conference on internet of things (IThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*. IEEE, 2018, pp. 1161–1170.

[23] R. Khalil and A. Gervais, "Revive: Rebalancing off-blockchain payment networks," in *Proceedings of the 2017 acm sigsac conference on computer and communications security*, 2017, pp. 439–453.

[24] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Hubs, rebalancing and service providers in the lightning network," *Ieee Access*, vol. 7, pp. 132 828–132 840, 2019.

[25] Z. Hong, S. Guo, R. Zhang, P. Li, Y. Zhan, and W. Chen, "Cycle: Sustainable off-chain payment channel network with asynchronous rebalancing," in *2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 2022, pp. 41–53.

[26] Z. Avarikioti, K. Pietrzak, I. Salem, S. Schmid, S. Tiwari, and M. Yeo, "Hide & seek: Privacy-preserving rebalancing on payment channel networks," in *Financial Cryptography and Data Security: 26th International Conference, FC 2022, Grenada, May 2–6, 2022, Revised Selected Papers*. Springer, 2022, pp. 358–373.

[27] I. A. Seres, L. Gulyás, D. A. Nagy, and P. Burcsi, "Topological analysis of bitcoin's lightning network," in *Mathematical Research for Blockchain Economy: 1st International Conference MARBLE 2019, Santorini, Greece*. Springer, 2020, pp. 1–12.

[28] Y. Guo, J. Tong, and C. Feng, "A measurement study of bitcoin lightning network," in *2019 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2019, pp. 202–211.

[29] P. Zabka, K.-T. Foerster, S. Schmid, and C. Decker, "Empirical evaluation of nodes and channels of the lightning network," *Pervasive and Mobile Computing*, vol. 83, p. 101584, 2022.

[30] A. Lisi, D. D. F. Maesa, P. Mori, and L. Ricci, "Lightnings over rose bouquets: an analysis of the topology of the bitcoin lightning network," in *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2021, pp. 324–331.

[31] Y. Qin, Q. Hu, D. Yu, and X. Cheng, "Malice-aware transaction forwarding in payment channel networks," in *2021 IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*. IEEE, 2021, pp. 297–305.

[32] G. Malavolta, P. Moreno-Sanchez, A. Kate, M. Maffei, and S. Ravi, "Concurrency and privacy with payment-channel networks," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 455–471.

[33] S. Tripathy and S. K. Mohanty, "Mappcn: Multi-hop anonymous and privacy-preserving payment channel network," in *Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers*. Springer, 2020, pp. 481–495.

[34] S. Thakur and J. G. Breslin, "Collusion attack from hubs in the blockchain offline channel network," in *Mathematical Research for Blockchain Economy: 1st International Conference MARBLE 2019, Santorini, Greece*. Springer, 2020, pp. 31–44.

[35] C. Pérez-Sola, A. Ranchal-Pedrosa, J. Herrera-Joancomartí, G. Navarro-Arribas, and J. Garcia-Alfaro, "Lockdown: Balance availability attack against lightning network channels," in *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24*. Springer, 2020, pp. 245–263.

[36] Q. Zhang, S. Cao, Y. Ni, T. Chen, and X. Zhang, "Enabling privacy-preserving off-chain payment via hybrid multi-hop mechanism," in *ICC 2022-IEEE International Conference on Communications*. IEEE, 2022, pp. 13–18.

[37] S. Mazumdar and S. Ruj, "Cryptomaze: Privacy-preserving splitting of off-chain payments," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 2, pp. 1060–1073, 2022.

Biography

Wei-Jun Gao received his Bachelor of Science degree from Lanzhou University in 1997 and his Master of Science degree from Chinese Academy of Sciences in 2000. He has been engaged in teaching and scientific research at Lanzhou University of Technology since 2000. His research interests include software engineering, distributed computing and cloud computing, big data processing, and

graphics and image processing.

Ya-Qian Yue received her B.S. degree in Network Engineering from Lanzhou Institute of Technology in 2021, and is now studying for her M.S. degree in School of Computer and Communication at Lanzhou University of Technology. Her main research interests are network and information security, and blockchain.

Xiao-Qin Wang received the B.S. degree in Network Engineering from Xinjiang Normal University in 2021, and is now a master's student in the School of Computer and Communication of Lanzhou University of Technology. Her main research interests are network and information security, blockchain.

A Lightweight Image Encryption Algorithm Based on a Dual Chaotic System and Dynamic S-box

Rui-Hong Chen, Qiu-Yu Zhang, Ling-Tao Meng, and Yi-Lin Liu
(Corresponding author: Qiu-yu Zhang)

School of Computer and communication, Lanzhou University of Technology
No. 287, Lan-Gong-Ping Road, Lanzhou 730050, China
Email: c2745168470@163.com,zhangqylz@163.com

(Received Apr. 6, 2023; Revised and Accepted Nov. 22, 2023; First Online Feb. 23, 2024)

Abstract

To solve the problems of long encryption time, low encryption throughput, large memory usage, high energy consumption, and weak encryption performance of existing image encryption algorithms in the resource-constrained multimedia Internet of Things (MIoT) for secure communication, a lightweight image encryption algorithm based on dual chaotic system and dynamic S-box was proposed. Firstly, the digital image is compressed after blocking by discrete cosine transform (DCT) coding technology. Then, the encryption key is generated from the initial key and the grey value of the compressed image. The generated encryption key is used as the initial value and control parameter for two-dimensional (2D) logistic mapping and tent mapping, and the key sequence is generated after each iteration. The generated key sequence is used to permute pixel bits and generate the S-box. Finally, the S-box dynamically generated by the tent mapping is used to diffuse the permuted pixel bits and obtain the encrypted image. The experimental results show that compared with the existing methods, the encryption time of the proposed algorithm is reduced by 3.0230s on average, the throughput of the system is increased by 0.0673Mbps on average, and the memory usage is low, with high encryption efficiency and security strength.

Keywords: Dynamic S-box; Image Compression; Image Encryption; Lightweight Encryption; Logistic-Tent Dual Chaotic System

1 Introduction

With the rapid development of social media networks and the MIoT, the demand for multimedia data sharing has increased significantly, but MIoT devices have resource constraints in terms of energy consumption, computing power, running time, and storage space [21]. Therefore, to enable secure and confidential communication with minimal power consumption in resource-constrained devices, lightweight cryptographic algorithms can meet both security and performance requirements, compared with traditional general cryptographic algorithms, lightweight cryptographic algorithms generally have the characteristics of low throughput, moderate security level, and high performance, and can be applied in MIoT to solve the problems of low system throughput and long response time in the encryption process [11].

In recent years, in resource-constrained IoT application scenarios, have used the SHA (Secure Hash Algorithm) series of hash algorithms, the SM series of national secret algorithms, AES (Advanced Encryption Standard) and other symmetric cryptographic algorithms, RSA (Rivest Shamir Adleman) and ECC (Ellipse Curve Cryptography) and other public key cryptographic algorithms [17,25] traditional cryptographic algorithms represented by traditional cryptography generally have performance limitations, such as relatively low computational efficiency, and it is difficult to obtain better encryption effects. Existing image encryption technologies mainly include chaotic encryption [7, 8], DNA coding [23], quantum encryption [27], optical encryption [24], cellular automaton encryption [18] and neural network [26] as well as other encryption methods. These encryption technologies have good encryption performance, but due to the strong correlation between pixels and high data redundancy, the implementation is more complex or difficult to ensure the security of encryption, and the memory consumption is large, the encryption efficiency is not high, and it does not meet the requirements of lightweight cryptographic algorithms.

With the rapid development of chaos theory, chaos encryption technology has gradually become the main direction of image encryption. A chaotic cryptosystem can have excellent characteristics in terms of computing power, security, complexity and other aspects, and the combination of a chaotic system and image compression

can not only reduce the amount of data and storage space of encrypted images but also reduce the consumption of space resources. To increase the security strength and encryption efficiency of the whole cryptographic algorithm, the single nonlinear structure S-box in the block cypher algorithm can be used to confuse and spread the image pixel value, and the quality of the indicators of the S-box directly determines the quality of the cryptographic algorithm [28]. Currently, due to the increasing amount of multimedia content, several lightweight cryptographic algorithms have emerged, that enable MIoT nodes to communicate securely with minimal computational complexity and bandwidth. Considering the transmission of images in resource-constrained MIoT, many scholars combine chaotic schemes with related technologies to optimize the performance of image encryption algorithms in constrained environments and achieve better encryption performance. For example, decreasing the encryption speed due to increasing the dimension of chaos and the computation step affects the effect of encryption, which is not suitable for resource-constrained IoT devices.

To solve the above problems, to make the lightweight cryptographic algorithm better take into account the requirements of the throughput, security and performance, this paper presents a lightweight image encryption algorithm based on a dual chaotic system and dynamic S-box, which uses the compression properties of DCT coding to compress the original image, and uses the Logistic-Tent dual chaotic system and dynamic S-box to encrypt the compressed image. The main contributions of this work are as follows:

1) A lightweight image encryption algorithm based on Logistic-Tent dual chaotic system and dynamic S-box is proposed, which takes into account balance between throughput, security level and performance.

2) Using the DCT coding compression feature, according to the statistical properties of the image signal in the frequency domain, the correlation between adjacent pixels is eliminated, the amount of data in the encrypted image is reduced, and the encryption efficiency is improved.

3) The designed Logistic-Tent dual chaotic system and dynamic S-box have stronger traversability and higher key space, and the initial parameters of the chaotic system and the average pixel value of the compressed image are iteratively generated to generate the encryption key, and the random permutation and diffusion of pixel bits are performed, which increases the correlation between the key and the image and improves the security of the image.

The rest of the text is arranged as follows: Section 2 reviews the relevant research. Section 3 describes the lightweight image encryption algorithm, dynamic S-box construction, and the encryption and decryption processes. Section 4 gives the experimental results and analysis of the proposed algorithm, and compares it with the experimental data of the existing related algorithms. Section 5 summarizes the work in this paper.

2 Related Works

In recent years, the hybrid digital image encryption method combining chaotic systems and other methods has been favoured and concerned by many scholars, and the existing results can have the characteristics of better key space and more system parameters, and achieve complementary advantages. Yousaf *et al.* [28] proposed an image encryption method that evolved a highly nonlinear S-box through the action of puzzle subgroups on the set of elements in magic, taking into account both complexity and ease of use. Kumar *et al.* [19] proposed a chaotic image encryption algorithm based on enhanced Thorp scrambling and Zigzag scanning convolution, which has high security. Zheng *et al.* [30] proposed an algorithm for constructing dynamic S-boxes based on chaos mapping and apply the idea of obfuscation to the construction of S-boxes, which has a good key space and can resist common attacks. Arif *et al.* [3] proposed a method based on substitution and substitution, combined with single S-box encryption, which has a high sensitivity to plaintext attacks. Idrees *et al.* [16] proposed an image encryption algorithm using S-box and dynamic Henon position exchange, which improved the security of encrypted images, but occupied more storage resources. Farah *et al.* [5] proposed a cryptographic algorithm based on the obfuscation/diffusion Shannon feature, using the Jaya algorithm to generate S-boxes. Farah *et al.* [4] proposed an algorithm for constructing S-boxes using chaos mapping and genetic algorithms, and the constructed S-boxes have better randomness and anti-attack ability. Ibrahim *et al.* [15] proposed a dynamic S-box construction method based on the key-dependent permutation of elliptic curve points, but the computational overhead of dynamic S-box construction limits the achievable encryption throughput. Hayat *et al.* [13] proposed a method to generate block cyphers using elliptic curves, and the generated S-box has high randomness and security. Zahid *et al.* [29] proposed a method to construct dynamic S-boxes through linear trigonometric transformations, which effectively improved the randomness of trigonometric transformations to generate S-boxes.

At present, most of the communication between MIoT devices is done in the form of images, and MIoT devices are often attacked by illegal elements because of small storage space and large losses. To solve these problems, scholars have proposed a variety of lightweight image encryption algorithms. For example, Alghamdi *et al.* [1] proposed a lightweight image encryption algorithm based on Logistic mapping, permutation and AES, which reduces the time required for encryption while ensuring certain security. Ferdush *et al.* [6] proposed an image encryption scheme based on Arnold and Logistic, which effectively reduced the time required for encryption and

improved encryption efficiency. Almalkawi *et al.* [2] proposed a lightweight compressed image encryption scheme with joint chaotic mapping, which can resist most attack types, but the disadvantage of this scheme is that it uses a one-for-time cypher scheme when generating keys. Liu *et al.* [20] proposed a lightweight image encryption algorithm based on a messaging algorithm with chaotic external messages, and the messaging algorithm adopted allows simple messages to be delivered locally to solve global problems, which will make the interaction between neighbouring pixels without additional space cost, thereby reducing resource consumption. Gupta *et al.* [10] proposed a new lightweight image key-based image encryption algorithm using Chebyshev chaotic mapping and cross-blending, which uses a mixture of crossover and Chebyshev mapping to create session keys, which is highly secure but slow in encryption. On this basis, Gupta *et al.* [9] proposed a lightweight image encryption algorithm based on a logistic-tent map and genetic algorithm, which effectively reduced the complexity and improved the encryption efficiency. Hasan *et al.* [12] proposed a scheme for encrypting medical images using two permutation techniques, which are highly secure but also highly complex. Hedayati *et al.* [14] used a scan-based block compression algorithm and selective encryption algorithm to encrypt images, which effectively reduced the time complexity and reduced the amount of encrypted data. Mondal *et al.* [22] proposed a lightweight image encryption scheme based on chaotic mapping and diffusion circuit, which controls the random number sequence used for pixel bit permutation and diffusion through the chaotic sequence, which reduces complexity and computational overhead.

In summary, the existing lightweight image encryption algorithm adopts a low-dimensional chaotic system with a simple structure and easy software and hardware to implement, but there are problems such as short periodicity, limited computing accuracy and low security, while the high-dimensional chaotic system has more control parameters and can better resist various attacks, but it is not suitable for MIoT devices with limited resources due to high complexity. Therefore, this paper uses DCT coding compression, dynamic S-box and Logistic-Tent dual chaos system to present a lightweight image encryption algorithm suitable for resource-constrained application scenarios.

3 The Proposed Scheme

To solve the problems of low system throughput, low encryption efficiency, and high memory usage in the confidential transmission of MIoT devices by existing image encryption algorithms, the algorithm compresses the original images and then encrypts them, thereby reducing the amount of encrypted data and effectively shortening the time required for encryption. In terms of security, a dynamic S-box is developed based on Tent mapping, and the key sequence generated by the 2D Logistic mapping is used to permute and diffuse the image pixel bits. Figure 1 shows the processing flow of the lightweight image encryption algorithm of the proposed algorithm. The proposed algorithm includes four processing steps: DCT coding image compression, key generation, dynamic S-box construction, and image encryption.

3.1 DCT Coding Image Compression Processing

The application of DCT coding for image data compression can reduce the digital information representing the image's luminance (or colour value) and achieve the purpose of data compression. To reduce the processing time and improve the encryption efficiency, the 2D discrete cosine transform is used for image compression. The specific steps are as follows:

Step 1: Divide the original image I with size $M\times N$ into 8×8 image blocks, and use Equation (1) to convert the image block with pixel density $f(x,\ y)$ into a matrix $F(u,\ v)$, which is the same size as the image block of the original image I, and the two conversion parameters u and v point to the spatial frequency.

$$F(u,v)=\frac{2}{\sqrt{M\times N}}C_uC_v\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\cos\left(\frac{\prod(2y+1)v}{N}\right)\cos\left(\frac{\prod(2x+1)u}{M}\right) \tag{1}$$

where $u=0,1,...M-1, v=0,1,...,N-1$. When $u=0, C_u=\sqrt{1/2}$, when $u\neq 0, C_u=0$, when $v=0, C_v=\sqrt{1/2}$, when $v\neq 0, C_v=0$.

Step 2: Obtain the DCT quantization coefficient. First, after 2D-DCT conversion, 64 coefficients are obtained:the important DC coefficient (DC component) and the low-frequency AC coefficient (AC component), located in the upper left corner, while the remaining high-frequency AC coefficient is less important for the human visual system. Then, the other coefficients are discarded by retaining the important coefficients using the quantification step.

Step 3: After quantization, a large part of the data in the matrix has become 0, and the Zigzag is used to convert the quantized two-dimensional matrix into a one-dimensional array. According to the arrangement shown in Figure 2, the DCT coefficients were first arranged from a data series, and then the compressed image $\boldsymbol{I}_c$ was obtained by using Huffman coding.

3.2 Key Generation

First, calculate the sum of all pixels of the compressed image $\boldsymbol{I}_c$ sum to obtain the pixel average K, and then use the sum of pixels sum and the initial key (x_0, y_0, z_0, k, u) to calculate the encryption key $(x_0^{'}, y_0^{'}, z_0^{'}, k^{'}, u^{'}, K)$ that is,

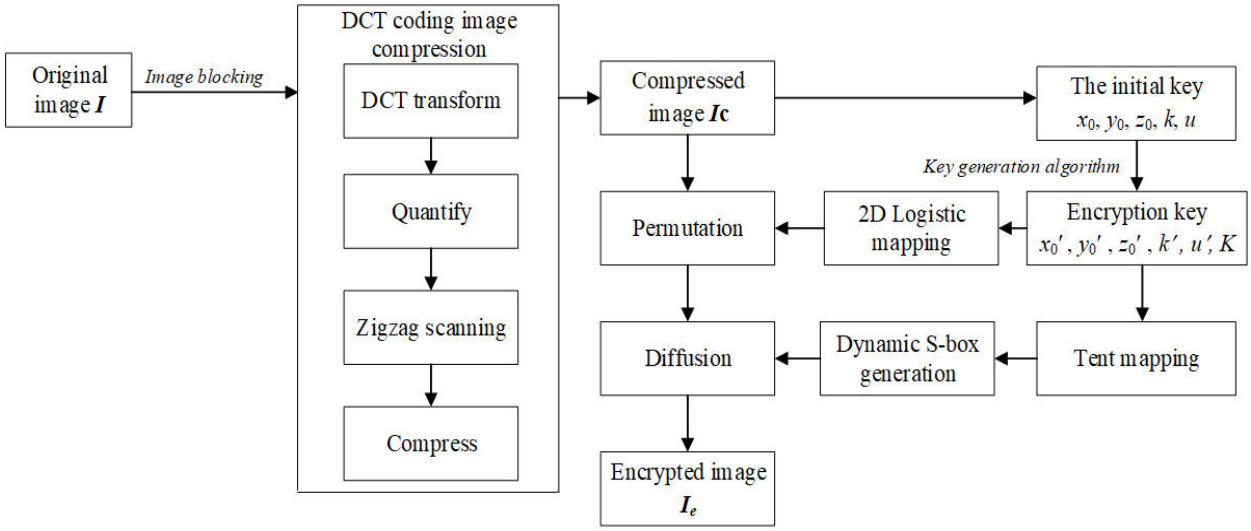


Figure 1: The lightweight image encryption algorithm processing flow.

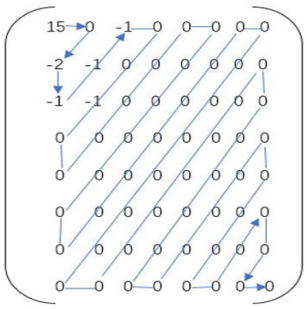


Figure 2: Arrangement of DCT coefficients.

use the 2D Logistic mapping of Equation (2) to obtain the initial value (x_0, y_0) and control parameter k, and use the tent mapping of Equation (3) to obtain the initial value z_0 and control parameter u.

$$\begin{cases} x(n+1) = y(n) \\ y(n+1) = k * y(n)(1 - x(n)) \end{cases} \tag{2}$$

where the control parameters $k \in (0, 2.28)$, the initial state $x, y \in (0, 1)$.

$$z_{(n+1)} = \begin{cases} (z_n/u) & 0 < z_n < 0.5 \\ (1 - z_n)/(1 - u) & 0.5 \leq 0 \leq 1 \end{cases} \tag{3}$$

where $z_n \in (0, 1)$, and u are the control parameters that control the dynamic properties of the tent mapping. When controlling parameter u>1, the map has a bifurcation phenomenon, that is, the tent mapping has a chaotic phenomenon. When $u = 2$, the chaotic sequence produced by the tent mapping approximately obeys a uniform distribution.

2D Logistic mapping has better randomness and key space and controls the dynamics of chaos mapping. The specific processing process of encryption key generation is shown in Algorithm 1.

Algorithm 1 : Key generation algorithm

Input: Compressed image $\boldsymbol{I}_c$, The initial key x_0, y_0, z_0, k, u

Output: Encryption key $x_0^{'}$, $y_0^{'}$, $z_0^{'}$, $k^{'}$, $u^{'}$, K

1: The compressed image $\boldsymbol{I}_c$ is traversed in the order from left to right and top to bottom to obtain a sequence $\boldsymbol{I}_c{}'$ with size $M \times N$

2: Calculates the sum of all pixels:$sum = \sum_{x=0}^{M*N} I_c(i)^{'}$

3: Calculates the average of all pixel sums:

$$K = floor\left(\frac{sum}{M \times N}\right)$$

4: $x_0^{'} = (x_0 + x_0 * sum) mod 1$; /* Calculate the encryption key $x_0^{'}$, $y_0^{'}$, $z_0^{'}$, $k^{'}$, $u^{'}$

5: $y_0^{'} = (y_0 + y_0 * sum) mod 1$;

6: $z_0^{'} = (z_0 + z_0 * sum) mod 1$;

7: $u^{'} = (u + u * sum) mod 1$;

8: $k^{'} = (k + k * sum) mod 1$;

9: **return** $x_0^{'}$, $y_0^{'}$, $z_0^{'}$, $k^{'}$, $u^{'}$, K

3.3 Dynamic S-box Construction Based on Tent Mapping

The S-box is nonlinear and is the basic structure for performing permutation calculations, providing better security. To design a satisfactory S-box, this paper uses Tent mapping to construct a dynamic S-box. This is because the tent mapping algorithm is simple, it can effectively reduce storage space, encryption and decryption speed, has high efficiency, and high security, suitable for MIoT

devices to transfer information.

For grayscale or colour images of size $M \times N$, the processing flow of using Tent mapping to construct a dynamic S-box is shown in Figure 3.

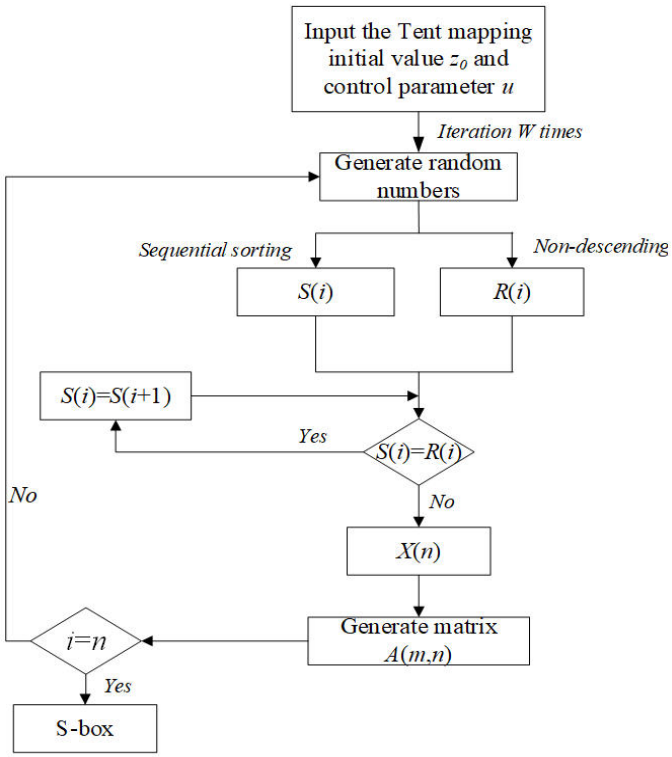


Figure 3: Dynamic S-box construction process.

The specific construction steps of the dynamic S-box are as follows:

Step 1: Take the initial value z_0 of the tent map and the control parameter u iteration W imes to obtain a sequence of random numbers $\boldsymbol{L}$ of length W, where $\boldsymbol{L}$=$\{L(1), L(2), L(3), ..., L(i)\}, (0 \leq i \leq n, L(i) = 256)$.

Step 2: Record the interval sequence the number of the elements in the subsequence as m, start numbering from 0, when the value of m reaches 255, start the next subsequence number, and so on.

Step 3: The sequence of interval numbers that generate random numbers is denoted as $\boldsymbol{S}$, where $\boldsymbol{S}$=$\{S(1), S(2), S(3), ..., S(i)\}, (0 \leq i \leq n)$.

Step 4: Sort the corresponding random values in the sequence $\boldsymbol{S}$ in non-descending order to obtain the interval number sequence $\boldsymbol{R}$=$\{R(1), R(2), R(3), ..., R(i)\}$, if $\boldsymbol{S}$(i)$\neq$ $\boldsymbol{R}$(i), then use the elements in the sequence $\boldsymbol{R}$(i) to form the sequence $\boldsymbol{X}$(n) into a two-dimensional matrix $\mathbf{A}$ of 16×16 in the order of first left and then right, and then up and down, if $\boldsymbol{S}$(i)=$\boldsymbol{R}$(i), then make $\boldsymbol{S}$(i)=$\boldsymbol{S}$(i+1), and judge again.

Step 5: $\mathbf{A}(x, y)$ represents the value of the x row y column in the matrix, use Equation (4) to convert the value at position $\mathbf{A}(x, y)$ in the matrix to another position $\mathbf{A}(x^{'}, y^{'})$, and convert the values in the matrix in the order of row priority to obtain an 8×8 S-box.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod (256) \quad (4)$$

Step 6: If $i \neq n$, repeat Steps 3 to 5 to generate the S-box again, this process can be cycled multiple times, generating multiple S-boxes.

In the construction of the above S-box, only simple sorting, replacing and remaining operations are involved, which can effectively reduce the memory occupation of the algorithm and help reduce the running time.

3.4 Encryption Process

In Figure 1, the key generation algorithm of Algorithm 1 is used to generate encryption keys to control 2D Logistic mapping and Tent mapping, and the key sequence is generated for image pixel bits to perform permutation and diffusion operations and generate dynamic S-boxes. The specific encryption steps are as follows:

Step 1: Image compression of the original image $\boldsymbol{I}$ through the DCT encoding image compression process given in Section 3.1 to generate the compressed image $\boldsymbol{I}_c$.

Step 2: Bring the initial key $\boldsymbol{I}_c$, The initial key (x_0, y_0, z_0, k, u) and the compressed image Ic into the key generation algorithm of Algorithm 1 to obtain the encryption key ($x_0^{'}$, $y_0^{'}$, $z_0^{'}$, $k^{'}$, $u^{'}$, K).

Step 3: Iterate the tent mapping according to Section 3.3 to generate an 8×8 S-box. To randomly disperse the displaced pixels using a dynamic S-box, the S-box can be represented by a matrix of size 16×16. The matrix of 16×16 is traversed from left to right and top to bottom to obtain a sequence $\boldsymbol{S}$ of length 256. Where $\boldsymbol{S}$(i) represents the i-th element of the sequence $\boldsymbol{S}$, i=0, 1, ..., 255.

Step 4: Substituting x_0, y_0, k into Equation (2) and iterating 1000+$M \times N$, in order to obtain more stable data, the data generated from 1001 iterations to 1000+ $M \times N$ times are used as valid data to generate a sequence list1 with length $M \times N$.

Step 5: Use Equation (5) to sort and calculate the sequence $\boldsymbol{L}_{seq}$ to obtain the sorted index sequence $\boldsymbol{L}_1$.

$$L_1 = \arg sort(L_{seq}) \quad (5)$$

where argsort() is a function in Python for sorting elements in a sequence of arrays from smallest to largest, and returns the index after the elements are sorted.

Step 6: Traverse the compressed image $\boldsymbol{I}_c$ in order from top to bottom, left to right, and obtain a sequence $\boldsymbol{I}_c{}'$ of size $M\times N$, $\boldsymbol{I}_c{}'(i)$ represents the i-th element in the sequence $\boldsymbol{I}_c{}'$ (i=0, 1, ..., $M\times N$-1).

Step 7: According to the value of sequence $\boldsymbol{L}_1$, the elements in sequence $\boldsymbol{I}_c{}'$ are replaced according to the permutation processing method in Figure 4 to obtain a new sequence $\boldsymbol{I}_{c1}{}'$.

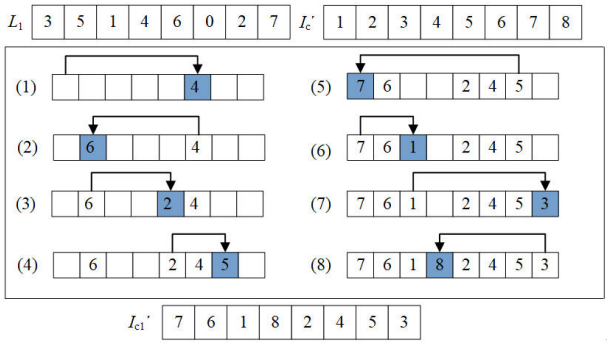


Figure 4: Permutation process.

Step 8: Determine the first-pixel value of the diffusion according to the value of the first element in the sequence $\boldsymbol{L}_1$, use the sequence $\boldsymbol{S}$ and the pixel and the average $\boldsymbol{K}$ to obtain the first grey value of the diffusion, and then store it in the first position of the empty sequence $\boldsymbol{I}_{c2}{}'$. The calculation formula is shown in Equation (6), where $\boldsymbol{L}_1(0)$ represents the first element in the sequence $\boldsymbol{L}_1$.

$$\begin{cases} index = I_{c1}{}'(L_1(0)) \oplus K \oplus L_1(i) \\ I_{c2}{}'(L_1(0)) = S(index) \end{cases} \tag{6}$$

Step 9: Equation (7) is continued to be used to diffuse other pixels, and then the diffusion of each pixel will be affected by the previous pixel, to obtain the final sequence $\boldsymbol{I}_{c2}{}'$.

$$\begin{cases} index = I_{c1}{}'(L_1(0)) \oplus I_{c2}{}'(L_1(i-1)) \oplus L_1(i) \\ I_{c2}{}'(L_1(i)) = S(index) \\ i = 1, 2, ..., M * N \end{cases} \tag{7}$$

Step 10: Convert the sequence $\boldsymbol{I}_{c2}{}'$ in row-first order using Equation (8) to the matrix form $\boldsymbol{P}$ of $M\times N$, which is the final encrypted image $\boldsymbol{I}_e$.

$$P = reshape(I_{c2}{}', M, N) \tag{8}$$

where reshape() is a function in Python that converts elements in an array to matrix form.

3.5 Decryption Process

The decryption process is the reverse of the encryption process. The specific process is as follows:

Step 1: Enter the encryption key (x_0', y_0', z_0', k', u', K), and obtain the sorted sequence $\boldsymbol{L}_1$ by Equation (9).

$$L^{-1} = \arg sort(list) \tag{9}$$

Step 2: Traverse all pixels of the encrypted image $\boldsymbol{I}_e$ in order from left to right, top to bottom to generate a sequence $\boldsymbol{I}_{c2}{}'$.

Step 3: Through Equation (10), the sequence $\boldsymbol{I}_{c1}{}'$ is obtained by using the reverse process of diffusion.

$$\begin{cases} index = S(I_{c2}{}'(L_1(0))) \\ I_{c1}{}'(L_1(0)) = index \oplus K \oplus L_1(0) \\ I_{c1}{}'(L_1(i)) = S(I_{c2}{}'(L_1(\mathrm{i}))) \oplus K \oplus L_1(i) \\ i = 1, 2, ...M*N-1, \end{cases} \tag{10}$$

Step 4: Through Equation (11), the sequence $\boldsymbol{I}_c{}'$ is obtained by using the reverse process of permutation.

$$\begin{cases} I_c{}'(L_1(0)) = I_{c1}{}'(L_1(M*N-1)) \\ I_c{}'(L_1(i+1)) = I_c{}'(L_1(i)) \\ i = M*N-2, ..., 1, 0 \end{cases} \tag{11}$$

Step 5: Convert the sequence $\boldsymbol{I}_{c}{}'$ through Equation (12) to the matrix $\boldsymbol{I}_c$.

$$I_c = reshape(I_c{}', M, N) \tag{12}$$

Step 6: The obtained compressed image $\boldsymbol{I}_c$ is inversely encoded and quantized by the inverse discrete cosine transform (IDCT) to restore the original image $\boldsymbol{I}$.

4 Experimental Results

Experimental hardware environment: Intel(R) Core(TM) i5-7572U 1.60GHz, 16GB. The software environment is Windows 10, PyCharm (Professional Edition) 2020.3.2 x64. The performance evaluation of the proposed algorithm is mainly evaluated from four aspects: encryption image quality, lightweight algorithm, encryption security level, and chaotic characteristics of S-box. Four images of 256×256 grayscale images are used for experimental test images: Lena, Peppers, Cameraman, and Baboon.

4.1 Encrypted Image Quality Analysis

The peak signal-to-noise ratio (PSNR) [1] is one of the objective evaluation indicators to measure image quality. The lower the PSNR value of the encrypted image and the worse the image quality of the encrypted image, the better the encryption effect. The PSNR is generally expressed through the mean squared error (MSE). For images of size $M\times N$, MSE is calculated as in Equation (13):

$$MSE = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I(i,j)-I'(i,j)\right)^2 \tag{13}$$

where M and N represent the width and height of the image, I is the original image, and I is the reconstructed image.

PSNR is based on the MSE definition, which is calculated as shown in Equation (14):

$$PSNR = 10\log_{10}(\frac{255^2}{MSE}) \tag{14}$$

The ratio of the data stream length of the image before compression to the data stream length of the compressed image is called the compression ratio. Table 1 shows the PSNR values of Lena, Peppers, Cameraman, and Baboon encryption/decryption when the compression ratio is 16:1. Table 2 compares the PSNR values of the proposed algorithm with the existing methods [3,6,20] of Lena encrypted image.

As can be seen from Table 1, the PSNR value of the encrypted image is low, and it is difficult for humans to observe the useful information in the image with the naked eye from the encrypted image, indicating that the proposed algorithm has good encryption performance. The PSNR values of the decrypted images are greater than 38dB, indicating that the proposed algorithm has a high-quality of decrypted image.

As can be seen from Table 2, the PSNR value of the proposed algorithm is lower than that of the comparative Ref. [3,6,20] which indicates that the encryption effect of the proposed algorithm is better than that of the comparative Ref. [3,6,20]. Therefore, the proposed algorithm has good encryption performance.

4.2 Encrypted Efficiency Analysis

4.2.1 Encryption Time, Encryption Throughput Analysis

Encryption speed is very important for the practicality of image encryption algorithms. At present, encryption time is an important indicator to measure the execution efficiency of MIoT devices when processing massive amounts of data. The longer it takes to encrypt an image, the less efficient the encryption becomes. Conversely, the more efficient the encryption. Table 3 compares the encryption time of Lena's image in the proposed algorithm with existing methods [5,6,16,19,22].

In addition, encryption throughput (ET) refers to the ability of a system to process data per second, which is an important indicator of system performance. Higher throughput, shorter algorithm execution times and faster encryption. Conversely, the slower the encryption. The calculation formula is shown as Equation (15) (unit: Mbps):

$$ET = \frac{C}{t} \tag{15}$$

where ET represents the encryption throughput, C is the size of the encrypted image, and t is the encryption time.

As can be seen from Table 3, the proposed algorithm takes 0.8625s to encrypt a 256×256 Lena image, and the encryption throughput can reach 0.2174Mbps. Compared with the existing methods [5,6,16,19,22], the average encryption time is reduced by an average of 3.0320s, and the encryption throughput is increased by an average of 0.0673Mbps. Therefore, the proposed algorithm takes less time, the encryption speed is faster, and it has good encryption efficiency, which can be used for real-time compression and encryption of images in MIoT.

4.2.2 Memory Consumption Analysis

In general, an efficient image encryption algorithm is to minimize communication overhead and occupies less storage space. Therefore, the code size of the individual algorithms involved in the encryption/decryption process store is an important metric for measuring the performance of the algorithm. The larger the code size of the algorithm, the greater the communication overhead, the more resources consumed, the lower the encryption efficiency, and vice versa, the higher the encryption efficiency. Table 4 shows the code size analysis of the proposed algorithm and the existing method [10,17].

As can be seen from Table 4, the code size of the algorithm generating the key and constructing the S-box in this paper is small (21094Byte), which is lower than [17], indicating that the memory occupation is lower than the [17]. Since the Chebyshev mapping and crossing method is used in [10] to generate session keys, the key size is small, so its code size is small, and the memory footprint is lower than that of the proposed algorithm. Therefore, the proposed algorithm occupies less storage space, effectively reduces the burden of channel transmission, and improves operational efficiency.

4.2.3 Time Complexity Analysis

Time complexity is an important indicator to measure the quality and operation efficiency of algorithms [14]. Assuming that the size of the image is $N \times N$, the time complexity of the encryption algorithm is divided into the following parts: the time complexity of 2D DCT compression encoding is $O((N^2)logN)$, the time complexity of key generation is $O(N^2/CR)$, the time complexity of permutation and diffusion is $O(N/CR)$, and the time complexity of building S-box is $O(N^2)$, then the time complexity of the proposed algorithm is $O((logN + 3/CR + 1)N^2)$. Table 5 compares the time complexity of the proposed algorithm with the existing methods [2,5,12,20,29].

As can be seen from Table 5, the time complexity of the proposed algorithm is lower than that of the comparative Ref. [2,5,12,20,29]. Therefore, the proposed algorithm has lower time complexity.

4.2.4 Energy Analysis

The energy [28] is a measure of changes in the colour or brightness of pixels in an image. The total energy value of the constant image is 1. Compared with the original image, the encrypted image tends to have lower energy,

Table 1: PSNR values for encryption/decryption of 4 test images when the compression ratio is 16:1

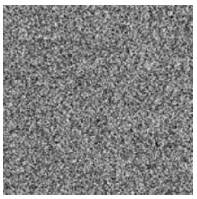
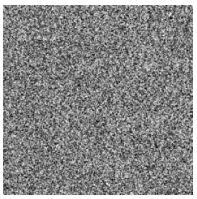
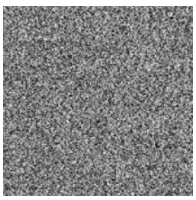
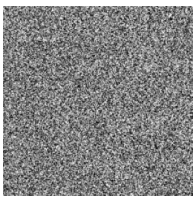
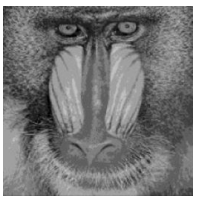
Original image	Encrypted image	PSNR /dB	Decrypted image	PSNR /dB
 Lena		8.4860		41.2280
 Peppers		8.6880		39.6430
 Cameraman		8.2064		38.2500
 Baboon		9.7029		40.2060

Table 2: Comparison of PSNR values of Lena's encrypted image

Method	Proposed	Ref. [3]	Ref. [6]	Ref. [20]
PSNR(dB)	8.4860	9.2376	11.8325	8.5510

and the lower the energy value, the better the security effect of the encryption algorithm. Table 6 compares the energy values of encrypted images between the proposed algorithm and the existing methods [15, 16, 28, 29]. The formula for calculating energy E is as follows:

$$E = \sum_{i,j} p(i,j)^2 \tag{16}$$

where $p(i,j)$ represents the total number of grayscale symbiotic matrices at (i,j).

As can be seen from Table 6, the energy value of the encrypted image of the proposed algorithm is lower than that of Ref. [16, 28, 29] and close to Ref. [15]. Therefore, compared with other encryption algorithms, the proposed algorithm has higher security, better attack resistance and good encryption performance.

4.3 Histogram Analysis

The histogram [22] is used to determine the distribution of pixels in an image. In general, the ideal encrypted image histogram has a uniform frequency distribution and is highly resistant to statistical attacks. Figure 5 shows the histograms of the original images of the four test images and the corresponding encrypted images.

As can be seen from Figure 5, the histogram grey value distribution of plaintext images is uneven, while the distribution of histogram grey values of encrypted images tends to be flat. Therefore, the proposed algorithm can well hide the pixel distribution information of the original image and can resist the statistical analysis attack using the histogram information.

Table 3: Compared with the average encryption time and encryption throughput of Lena's images

Method	Image size	Encryption time /s	Encryption throughput /Mbps	Hardware environment
Proposed	256×256	0.8625	0.2174	Intel(R) Core(TM) i5-7572U /1.60GHz, 16GB
Ref. [19]	256×256	10.4400	0.0180	Intel Pentium N3540 /2.16GHz, 8GB
Ref. [16]	256×256	2.6264	0.0714	-
Ref. [5]	256×256	2.4433	0.0767	Intel i3 /2.53 GHz, 2 GB
Ref. [6]	256×256	2.2270	0.0842	Intel core i7 /2.90 GHz, 16GB
Ref. [22]	256×256	1.5000	0.5000	Intel(R) Core(TM)-i5 M450 16GB

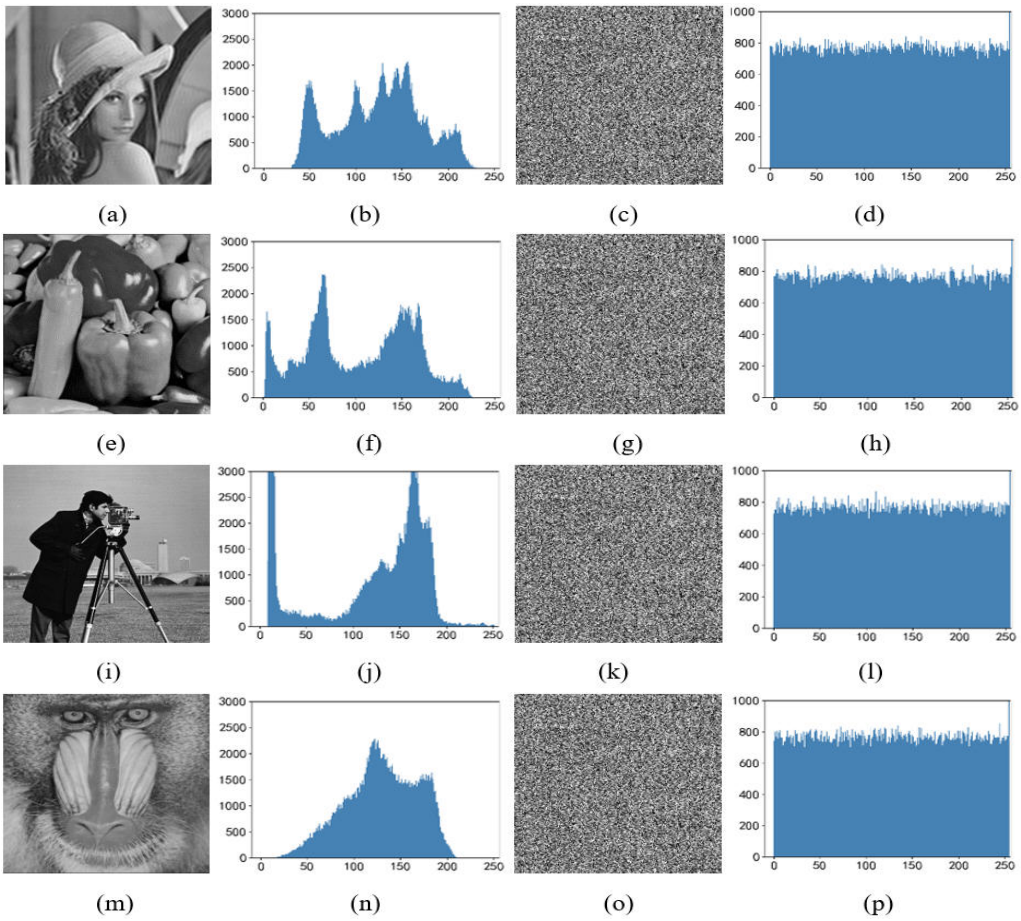


Figure 5: Histogram analysis of the original image and encrypted image, (b)(d), (f)(h), (j)(i), (n)(p) are histograms of the original image and the encrypted image corresponding to the four test images, respectively.

Table 4: Code size comparison with existing methods

Method	Proposed	Ref. [17]	Ref. [10]
Code size (Byte)	21094	22016	441

4.4 Information Entropy Analysis

The information entropy [16] is a criterion for evaluating the distribution of grey values in images, which reflects the randomness of the distribution of grey values in images. The image information entropy H(s) is shown as

Table 5: Compared with the time complexity

Method	Time complexity
Proposed	$O((logN+3/CR+1)N^2)$
Ref. [5]	$O(2N^2(logN))$
Ref. [29]	$O(4^n)$
Ref. [2]	$O((logN+11/CR+1)N^2)$
Ref. [20]	$O(3N^2)$
Ref. [12]	$O(I(N^2))$

Table 6: Energy comparison

Method	Image	Energy
Proposed	Lena	0.01562
	Peppers	0.01563
	Camerman	0.01560
	Baboon	0.01562
Ref. [28]	Lena	0.01780
Ref. [16]	Baboon	0.01610
Ref. [15]	Baboon	0.01560
Ref. [29]	Lena	0.01564

Equation (17) (unit bits):

$$H(s)=-\sum_{i=1}^{m}P(s_i)\log_2\frac{1}{P(s_i)} \tag{17}$$

where m represents the number of symbols (pixel grey levels) emitted by the source, s_i represents the grey value size of the image, and $P(s_i)$ represents the probability size of the symbol s_i.

The information entropy of the encrypted image should be as close as possible to the ideal value of 8. If the entropy value of the ciphertext image is less than 8, the plaintext image is predictable. Table 7 compares the entropy values of the proposed algorithm with the existing methods [2,3,6,11,19,22,29].

As can be seen from Table 7, the average value of the information entropy value of the proposed algorithm is higher than that of Ref. [3,6,11,22,29] and slightly lower than that of Ref. [2,19], indicating that the information entropy of the proposed algorithm can be better than the ideal value than the existing methods, and it has strong resistance to entropy attacks.

4.5 Differential Attack Analysis

The differential attack [29] is common in cryptography. To secure the performance of the proposed algorithm against differential attacks, this paper uses the number pixels change rate(NPCR) and unified average changing intensity(UACI) to analyze. When one or more pixels in the plaintext image change, the ciphertext image changes significantly, and when the values of NPCR and UACI are close to the ideal values of 99.6094% and 33.4635%, the encryption is more resistant to differential attacks. Table 8 compares the differential attack performance of the proposed algorithm with the existing methods [2,3,6,11,19,22,29]. NPCR and UACI are defined as follows:

$$NPCR=\frac{\sum_{i,j}E(i,j)}{M\times N}\times 100\% \tag{18}$$

$$E(i,j)=\begin{cases}0, I_1(i,j)=I_2(i,j)\\ 1, I_1(i,j)\neq I_2(i,j)\end{cases} \tag{19}$$

$$UACI=\frac{1}{M\times N}\frac{\sum_{i,j}(I_1(i,j)-I_2(i,j))}{255}\times 100\% \tag{20}$$

where M and N are the width and height of the encrypted image, and I_1 and I_2 are the pixel values of the ciphertext image corresponding to the pixel value change.

As can be seen from Table 8, the difference between the NPCR mean and the ideal value of the proposed algorithm is lower than that of Ref. [2, 3, 6, 11, 19, 22, 29], which is closer to the theoretical value, and the difference between the mean and the ideal value of UACI is lower than that of Ref. [2,6,11,19,22,29], which is slightly higher than Ref. [3]. Therefore, the proposed algorithm can effectively resist differential attacks compared with existing methods.

4.6 Key Space Analysis

The key space is the ability to evaluate an algorithm's resistance to brute force attacks [5]. The security strength of lightweight encryption algorithms is generally required to be more than 80 bits, which is sufficient to resist brute force attacks. Therefore, to prevent the key from being cracked, from the perspective of security, the key space needs to be $\geq 2^{80}$, and when the key space is $\geq 2^{80}\approx 10^{24}$ can meet the security required by the device. The proposed algorithm encryption key requires five key values x_0, y_0, z_0, k, and u, the total key space of the proposed algorithm obtained by a large number of experimental tests is$10^{15}\times 10^{15}\times 10^{15}\times 10^{15}\times 10^{15}=10^{75}\approx 2^{250}$. Table 9 compares the key space between the proposed algorithm and the existing methods [5,9–11,19,22].

As can be seen from Table 9, the key space of the proposed algorithm is higher than that of Ref. [5,9–11,19]. Due to the use of cascading shadow mapping to generate encryption keys in Ref. [22], the complexity is high, making the key space slightly higher than the key space of the proposed algorithm.

4.7 Key Sensitivity Analysis

The key sensitivity [19] refers to the difference between ciphertext images obtained by encrypting the same plaintext image with the key before and after the change when the key changes slightly. Figure 6 shows the key sensitivity analysis of the Lena image. Where: Figure 6(a) is the original image, the ciphertext image, and the decrypted image obtained with the correct key. Figure 6(b) shows different decrypted images obtained using different error keys. Table 10 shows the comparison results of measuring

Table 7: Comparison with the information entropy of existing methods to encrypted image

Method	Lena	Peppers	Cameraman	Baboon	Average value
Proposed	7.9990	7.9993	7.9992	7.9993	7.9992
Ref. [11]	7.9967	-	-	7.9969	7.9968
Ref. [19]	7.9996	7.9993	7.9970	7.9992	7.9994
Ref. [3]	7.9993	7.9993	7.9995	7.9992	7.9987
Ref. [29]	7.9968	-	-	7.9964	7.9966
Ref. [6]	7.4077	-	-	7.9434	7.6756
Ref. [2]	7.9992	-	7.9993	7.9993	7.9993
Ref. [22]	7.9989	7.9989	-	7.9989	7.9989

Table 8: Comparison with NPCR and UACI values of existing methods

Method	Evaluation indicator	Lena	Peppers	Cameraman	Baboon	Mean value	Difference
Proposed	NPCR	99.6000	-	-	99.6038	99.6019	0.0071
	UACI	33.5550	33.4577	33.4460	33.4670	33.4814	0.0179
Ref. [11]	NPCR	99.5960	99.6020	99.6130	99.5988	99.6023	0.0075
	UACI	28.3875	-	-	27.3288	27.8582	5.6053
Ref. [19]	NPCR	99.6419	99.6196	99.6016	99.6153	99.6196	0.0102
	UACI	33.5582	33.5378	33.5737	33.5786	33.5621	0.0986
Ref. [3]	NPCR	99.6193	99.6414	99.6048	99.6060	99.6179	0.0085
	UACI	33.4860	33.4532	33.4856	33.4375	33.4656	0.0021
Ref. [29]	NPCR	99.6930	-	-	99.6840	99.6885	0.0791
	UACI	33.6100	-	-	33.4300	33.5200	0.0565
Ref. [6]	NPCR	99.3700	-	-	99.4900	99.4300	0.1794
	UACI	20.7500	-	-	23.3700	22.0600	11.4035
Ref. [2]	NPCR	99.6600	-	99.6300	99.6300	99.6400	0.0306
	UACI	33.5600	-	33.3400	33.6900	33.5300	0.0665
Ref. [22]	NPCR	99.5870	99.6010	-	99.6160	99.6013	0.0081
	UACI	30.7010	31.0360	-	27.8660	29.8677	3.5958

Table 9: Comparison with the key space of existing methods

Algorithm	Proposed	Ref. [11]	Ref. [19]	Ref. [5]	Ref. [10]	Ref. [9]	Ref. [22]
Key space	10^{75}	10^{24}	10^{60}	10^{56}	10^{24}	10^{24}	10^{96}

and evaluating the differences between different decrypted images by calculating the values of NPCR and UACI.

As can be seen from Figure 6, in the decryption process, when the decryption key changes slightly, the decrypted images are different, and it is difficult to identify the relevant information of the original image from these images, indicating that the proposed algorithm has a strong sensitivity to the key and can effectively resist brute force attacks.

It can be seen from Table 10 that the average values of NPCR and UACI are close to the theoretical values of 99.6094% and 33.4635%, indicating that the proposed algorithm is very sensitive to keys and can effectively resist exhaustive attacks.

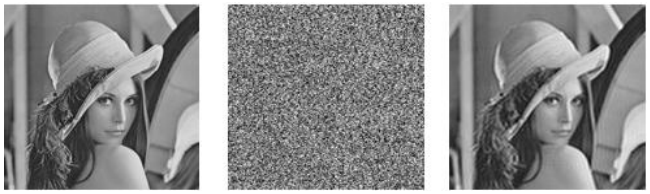
4.8 Security Performance Analysis of S-box

The proposed algorithm uses the characteristics of nonlinearity (NL), strict avalanche criterion (SAC), differential approximation rate (DP), and output bit-to-bit independence (BIC) to verify the performance of the generated S-box.

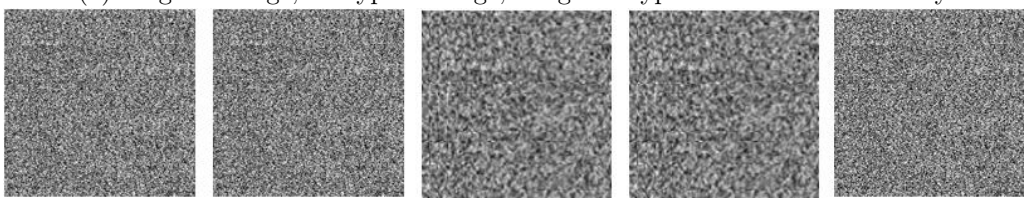
S-box nonlinearity (NL) [30] is a measure of resistance to linear cryptanalysis. In the security analysis of the S-box, the higher the value of nonlinearity, the stronger the S-box is resistant to attacks in the face of linear cryptanalysis. Suppose $f(x)$ is a Boolean function of n elements.

$$N_f = \underset{l \in L_n}{mid}\, d_H(f, l) \tag{21}$$

where N_f is the nonlinearity of $f(x)$, Ln is the set of linear sums of all n elements, and $d_H(f, l)$ is the Hamming



(a) Original image, encrypted image, image decrypted with the correct key



(b) Decrypted images with the key of $x_0 + 10^{-15}, y_0 + 10^{15}, z_0 + 10^{-15}, k + 10^{-15}, andu + 10^{-15}$

Figure 6: Key sensitivity analysis of Lena's image.

Table 10: NPCR and UACI comparison between decrypted images obtained with different decryption keys (%)

Evaluation indicator	x_0	y_0	z_0	k	u
NPCR	99.6146	99.6092	99.6185	99.5898	99.6036
UACI	33.7041	33.4465	32.7200	32.6928	33.1978

distance between f and l.

The proposed algorithm calculates the nonlinearity of the function through the Walsh spectrum, and the expression can be defined as:

$$S_{<f>}(w) = \sum_{x \in GF(2^n)} (-1)^{f(x) \oplus x \cdot w} \tag{22}$$

where $w \in GF(2^n)$, $x \cdot w$ is the dot product of x and w, and $x \cdot w = x_1 w_1 \oplus x_2 w_2 \oplus \ldots \oplus x_n w_n$.

The strict avalanche criterion (SAC) [4] states that when one input bit of a given sequence is modified, more than half of the output bits are altered. In general, the Boolean function is tested whether Boolean function meets the strict avalanche criterion by constructing a correlation matrix, and if the value of each element in the matrix is close to the ideal value of 0.5, it means that the S-box meets the SAC criterion, and Table 11 shows the SAC correlation matrix of the proposed algorithm. Among them, the maximum and minimum values are 0.5812 and 0.4375, respectively, and the average value is 0.4992, which is a 0.0008 difference from 0.5000.

Differential approximation rate (DP) [15] is an evaluation criterion to measure the ability of S-boxes to resist differential cryptanalysis and is usually expressed as DP_f as follows:

$$DP_f = \max_{\Delta x \neq 0, \Delta y} \left(\frac{\#\{x \in GF(2^n)\}}{2^n} \right) \left(\frac{|f(x) \oplus f(x + \Delta x) = \Delta y|}{2^n} \right) \tag{23}$$

where $GF(2^n)$ represents the set of inputs, 2^n represents the number of all set elements, Δx and Δy represent the input difference and output difference, respectively, and DP_f represents the maximum probability of the output. A higher value of DP_f means more resistance to attacks. Conversely, the weaker the ability to resist attack.

For the output inter-bit independence (BIC) performance test of the S-box, the value of any two output bits f_i, f_k $(i \neq k)$ XOR operation can be used to determine whether the value of the XOR operation meets the strict avalanche criterion, if the obtained value is nonlinear and meets the strict avalanche effect, it can be ensured that when a bit is reversed, the correlation coefficient of each output bit pair is close to 0, that is, BIC is satisfied.

Table 12 compares the security performance of the proposed algorithm compared with the existing methods [4, 5, 13, 15, 30] S-box.

As can be seen from Table 12, the mean NL of the proposed algorithm is 107.00, which is higher than the average value of Ref. [5, 13, 15, 30], because Ref. [4], uses a chaotic system based on elliptic curve points to construct the S-box, which is highly complex, so its NL value is higher than that of the proposed algorithm, indicating that the S-box constructed by the proposed algorithm has strong resistance in the face of linear cryptanalysis. Compared with Ref. [4, 5, 13, 15, 30] , the SAC value of the proposed algorithm is closer to the ideal value of 0.5000, indicating that the S-box constructed by the proposed algorithm meets the strict avalanche criterion and has a good security performance. Compared with Ref. [4, 5, 13, 15, 30] , the maximum difference value of the algorithm in Ref. [5, 13, 15, 30] is 10, the maximum difference value of Ref. [4] is 12, and the maximum difference value of S-box of the proposed algorithm is 10, indicating that the difference uniformity of S-box constructed in the proposed algorithm is better and the ability to resist at-

Table 11: SAC correlation matrix

0.5172	0.4688	0.5490	0.5781	0.4823	0.4844	0.5332	0.4844
0.5000	0.4980	0.4688	0.4823	0.4531	0.5333	0.4862	0.5137
0.5176	0.4688	0.5313	0.4705	0.5812	0.4666	0.5000	0.5088
0.4375	0.4667	0.5288	0.5000	0.5220	0.5062	0.4475	0.5315
0.4392	0.4844	0.4896	0.5413	0.4980	0.4549	0.5256	0.4531
0.5156	0.5137	0.5023	0.4688	0.5313	0.5313	0.5000	0.5176
0.5000	0.5156	0.4844	0.5469	0.4844	0.4888	0.4375	0.5019
0.5137	0.4862	0.5356	0.5625	0.4531	0.4844	0.4705	0.4990

Table 12: Comparison of S-box safety performance with existing methods

Method	NL(AVG)	SAC	The difference from 0.5000	DP	BIC-SAC	The difference from 0.5000
Proposed	107.00	0.4992	0.0008	10	0.4992	0.0008
Ref. [30]	104.00	0.4988	0.0012	10	0.5052	0.0052
Ref. [5]	106.25	0.5009	0.0009	10	0.4996	0.0040
Ref. [4]	108.00	0.4988	0.0012	12	0.4969	0.0031
Ref. [15]	106.50	0.5009	0.0009	10	0.4990	0.0010
Ref. [13]	106.25	0.5086	0.0086	10	0.5010	0.0010

tack is strong. The mean values of the Ref. [4,5,13,15,30] schemes were 0.5052, 0.4996, 0.4969, 0.4990, and 0.5010, respectively, and the average value of BIC-SCA in the proposed algorithm was 0.4992, which was only 0.0010 different from 0.5000. Comparative analysis shows that the output of the proposed algorithm is more independent than the inter-cells, indicating that the S-box constructed in the proposed algorithm has obvious advantages in resisting the attacks of differential and linear cryptanalysis.

In summary, the dynamic S-box constructed by the proposed algorithm performs well in nonlinearity, strict avalanche criterion, differential approximation rate and independence between output bits, it can effectively resist linear cryptanalysis attacks and differential cryptanalysis attacks, and has good security, which indicates that the chaotic dynamic S-box generated by the proposed algorithm has good nonlinearity and attack resistance.

5 Conclusions

In this paper, a lightweight image encryption algorithm based on a dual chaotic system and dynamic S-box is proposed, which considers the balance between throughput, security level and performance, and better solves the shortcomings of existing image encryption algorithms in terms of decryption image quality, encryption throughput, time complexity, memory usage and resistance statistics. The proposed algorithm uses DCT coding to compress the original image, effectively reducing the amount of encrypted data and improving the encryption speed. The designed Logistic-Tent dual chaotic system has better key space and randomness, which can generate better random key sequences. The generated random key sequence is XOR with the dynamic S-box to enhance the security of the encrypted image. The experimental results show that the quality of the decrypted image with the proposed algorithm is good, the time complexity is low, the encryption throughput is high, the security is high, and the defense against common attacks is effective. The proposed algorithm can maximize the requirements of device security interaction in MIoT and can be better adapted to constrained environments.

The disadvantage is that the proposed algorithm uses DCT-based compression technology in compression, and there are still some shortcomings in compression efficiency. Therefore, the next improvement direction is to further improve the efficiency of the encryption algorithm while ensuring the security of the image.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (No. 61862041). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] Y. Alghamdi, A. Munir and J. Ahmad, "A Lightweight Image Encryption Algorithm Based on Chaotic Map and Random Substitution," *Entropy*, vol. 24, no. 10, 1344, 2022.

[2] I. T. Almalkawi, R. Halloush, A. Alsarhan, et al., "A lightweight and efficient digital image encryption using hybrid chaotic systems for wireless network applications," *Journal of Information Security and Applications*, vol. 49, 102384, 2019.

[3] J. Arif, M. A. Khan, B. Ghaleb, et al., "A novel chaotic permutation-substitution image encryption

scheme based on logistic map and random substitution," *IEEE Access*, vol. 10, pp. 12966–12982, 2022.

[4] M. B. Farah, N. A. Azam, R. Guesmi, et al., "A new design of cryptosystem based on S-box and chaotic permutation," *Multimedia Tools Applications*, vol. 79, no. 27, pp. 19129–19150, 2020.

[5] M. B. Farah, A. Farah and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box " *Nonlinear Dynamics*, vol. 99, no. 4, pp. 3041–3064, 2020.

[6] J. Ferdush, M. Begum and M. S. Uddin, "Chaotic lightweight cryptosystem for image encryption," *Advances in Multimedia*, vol. 2021, Article ID 5527295, 2021.

[7] X. Y. Gao, J. Mou, S. Banerjee, et al., "An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 4, pp. 1535–1551, 2022.

[8] X. Y. Gao, J. Mou, L. Xiong, et al., "A fast and efficient multiple images encryption based on single-channel encryption and chaotic system," *Nonlinear Dynamics*, vol. 108, no. 1, pp. 613–636, 2022.

[9] M. Gupta, K. K. Gupta, M. R. Khosravi, et al., "An intelligent session key-based hybrid lightweight image encryption algorithm using logistic-tent map and crossover operator for internet of multimedia things," *Wireless Personal Communications*, vol. 121, no. 3, pp. 1857–1878, 2021.

[10] M. Gupta, K. K. Gupta and P. K. Shukla, "Session key based novel lightweight image encryption algorithm using a hybrid of Chebyshev chaotic map and crossover," *Multimedia Tools and Applications*, vol. 80, no. 25, pp. 33843–33863, 2021.

[11] M. Gupta, K. K. Gupta and P. K. Shukla,"Session key based fast, secure and lightweight image encryption algorithm," *Multimedia Tools and Applications*, vol. 80, no. 7. pp. 10391–10416, 2021.

[12] M. K. Hasan, S. Islam, R. Sulaiman, et al., "Lightweight encryption technique to enhance medical image security on internet of medical things applications," *IEEE Access*, vol. 9, pp. 47731–47742, 2021.

[13] A. Hayat, A. M. Abbas, S. Naz, et al., "A truly dynamic substitution box generator for block ciphers based on elliptic curves over finite rings," *Arabian Journal for Science and Engineering*, vol. 46,no. 9, pp. 8887–8899, 2021.

[14] R. Hedayati and S. Mostafavi, "A lightweight image encryption algorithm for secure communications in multimedia Internet of Things," *Wireless Personal Communications*, vol. 123, no. 2, pp. 1121–1143, 2021.

[15] S. Ibrahim and A. M. Abbas, "Efficient key-dependent dynamic S-boxes based on permutated elliptic curves," *Information Sciences*, vol. 558, pp. 246–264, 2021.

[16] B. Idrees, S. Zafar, T. Rashid, et al., "Image encryption algorithm using S-box and dynamic Hénon bit level permutation," *Multimedia Tools and Applications*, vol. 79, no. 9, pp. 6135–6162, 2020.

[17] A. Kifouche, M. S. Azzaz, R. Hamouche, et al., "Design and implementation of a new lightweight chaos-based cryptosystem to secure IoT communications," *International Journal of Information Security*, vol. 21, no. 6, pp. 1247–1262, 2022.

[18] A. Kumar and N. Raghava, "An efficient image encryption scheme using elementary cellular automata with novel permutation box," *Multimedia Tools and Applications*, vol. 80, no. 14, pp. 21727–21750, 2021.

[19] C. M. Kumar, R. Vidhya and M. Brindha, "An efficient chaos based image encryption algorithm using enhanced thorp shuffle and chaotic convolution function," *Applied Intelligence* , vol. 52, no. 3, pp. 2556–2585, 2022.

[20] H. Liu, B. Zhao, J. W. Zou, et al., "A lightweight image encryption algorithm based on message passing and chaotic map," *Security and Communication Networks* , vol. 2020, Article ID 7151836, 2020.

[21] Z. H. Lv, L. Qiao and H. B. Song, "Analysis of the security of Internet of multimedia things," *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, vol. 16, no. 3s, pp. 1–16, 2020.

[22] B. Mondal and J. P. Singh, "A lightweight image encryption scheme based on chaos and diffusion circuit," *Multimedia Tools and Applications*, vol. 81, no. 24, pp. 34547–34571, 2022.

[23] S. M. Wang, C. Y. Li, Q. Q. Peng, et al., "Chaotic color image encryption based on 4D chaotic maps and DNA sequence," *Optics & Laser Technology*, vol. 148, 107753, 2022.

[24] X. Y. Wang, S. Gao, L. Tian, et al., "Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory," *Information sciences*, vol. 507, pp. 16–36, 2020.

[25] B. Xing, D. D. Wang, Y. Q. Yang, et al., "Accelerating DES and AES Algorithms for a Heterogeneous Many-core Processor," *International Journal of Parallel Programming*, vol. 49, pp. 463–486, 2021.

[26] S. C. Xu, X. Y. Wang and X. L. Ye, "A new fractional-order chaos system of Hopfield neural network and its application in image encryption," *Chaos, Solitons & Fractals*, vol. 157, 111889, 2022.

[27] G. D Ye, K. X. Jiao and X. L. Huang, "Quantum logistic image encryption algorithm based on SHA-3 and RSA," *Nonlinear Dynamics*, vol. 104, no. 3, pp. 2807–2827, 2021.

[28] A. Yousaf, A. Razaq and H. Baig, "A lightweight image encryption algorithm based on patterns in Rubik's revenge cube," *Multimedia Tools and Applications*, vol. 81, no. 20, p. 28987–28998, 2022.

[29] S. H. Zahid, M. Ahmad, A. Alkhayyat, et al., "Efficient dynamic S-box generation using linear trigonometric transformation for security applications," *IEEE Access*, vol. 9, pp. 98460–98475, 2021.

[30] J. M. Zheng and Q. X. Zeng, "An image encryption algorithm using a dynamic S-box and chaotic maps," *Applied Intelligence*, vol. 52, no. 13, pp. 15703–15717, 2022.

Biography

Qiu-yu Zhang Researcher/Ph.D. supervisor, graduated from Gansu University of Technology in 1986, and then worked at school of computer and communication in Lanzhou University of Technology. He is vice dean of Gansu manufacturing information engineering research center, a CCF senior member, a member of IEEE and ACM. His research interests include network and information security, information hiding and steganalysis, multimedia communication technology.

Rui-hong Chen is currently a master's student of the School of Computer and Communication, Lanzhou University of Technology, China. She received her BS degree in computer science and technology from Kashi University, Xinjiang, China, in 2021. Her research interests include network and information security, multimedia data security and research on lightweight image encryption methods.

Ling-tao Meng is currently a master's student of the School of Computer and Communication, Lanzhou University of Technology, China. He received a BS degree in computer science and technology from the Lanzhou University of Technology, Gansu, China, in 2022. His research interests include network and information security, deep learning and image retrieval.

Yi-lin Liu is currently a master's student of the School of Computer and Communication, Lanzhou University of Technology, China. She received a BS degree in software engineering from Lanzhou University of Technology, in 2020. Her research interests include network and information security, multimedia data security and research on lightweight image encryption methods.

A Key Independence Group Key Management Scheme for Non-Reliable End-to-End Networks

Jian Zhou, Liyan Sun, and Shihua Huang
(Corresponding author: Jian Zhou)

Anhui University of Finance and Economics, Anhui Bengbu 233041, China[1]
Beijing University of Post and Communications, Beijing, Haidian 100083, China[2]
Email: ac_zj_course@163.com
(Received Apr. 10, 2023; Revised and Accepted Nov. 24, 2023; First Online Feb. 23, 2024)

Abstract

Due to the binding relationship between the decryption key and the encryption key based on single-decryption-key single-encryption-key key protocol, all members must participate in the rekeying process inevitably to update their key material at the cost of a large number of interactions in group key management. Therefore, current group key management schemes based on a reliable end-to-end link cannot meet the efficiency and security requirements for non-reliable end-to-end networks. To mitigate the problem, this paper proposed a group key management scheme based on a multi-decryption-key single-encryption-key key protocol, in which all decryption keys correspond to the same encryption key, and every member has a different decryption key that meets key independence to release the relationship between decryption key and encryption key. Only the joining or leaving member needs to participate in the rekeying to update the encryption key; other members keep their decryption key unchanged. In the security aspect, the suggested scheme guarantees forward/backward security based on the hard problem of the discrete logarithm. In the efficiency aspect, the message cost is not related to the network scale, and the dependence on reliable end-to-end links is reduced significantly since there are few interactions in rekeying. Therefore, our suggested scheme suits the non-reliable end-to-end link and long-time-delay networks.

Keywords: Group Key Management; Key Independence; Non-reliable End-to-End Link; Rekeying; Single-Encryption-Key Multi-Decryption-Key Key Protocol

1 Introduction

With the rapid development of wireless communication technology, wireless communication hardware modules are embedded in various devices to support special application scenarios for promoting various science researches, such as deep space exploration [1, 2], military unmanned aerial vehicle [3, 4],wild animal tracking [5, 6] and underwater communication [7, 8]. However in those scenarios, deployment area, transmission distance, communication medium, maintenance condition, mission complexity and entities capability are obviously different from traditional ground network [9], those factors affect the state of link negatively, networks members could have few internal resources to deal with terrible external environment. First network entities could be deployed in a large coverage space, for example satellites and probers could be deployed in several different planetary orbits in deep space networks, a links from source to destination may encounter distinct environments, so the state of the link is highly unstable [10]. Secondly network entities may hardly receive the manual maintenance services and possess enough spare equipment, for example the distance is more than 3.8410_5km among spacecraft and earth in deep space networks so as to it is impossible to send an astronaut or a new equipment in a short time [11],thus a damage link could not be recovered in time. Thirdly, a networks entity is destroyed or damaged easily so as to their links are corrupt by an adversary, for example, UAVs are easily captured by enemies in hostile airspace, the compromised entity could eavesdrop a link [12].Fourth the accurate state of network is predicted impossibly by a control center, in deep space network a member could frequently be out of control with ground control center as the link between them is non-reliable end-to-end, the control center hardly assure that global information is fresh and integrity [13]. Fifth different media are used for communication, for example communication relying on acoustic signal build an end-to-end link in underwater sensor networks, so as to underwater members spend more time than ground sensor networks [14]. Finally, the ability of mobile network individuals is severely limited by load and space, such as portable batteries, high gain antennas, high performance calculators and large capacity memory, which limit the performance of network protocols [15]. Therefore, those network states are unstable, their end-to-end links are unreliable and longtime delay, so the interruption and destruction frequently happen in-

evitably in communication, the existing network's architecture, protocols, security strategy and resource allocation methods based on reliable end-to-end link are insufficient to conform to the network deployment in the above applications.

The security of unreliable end-to-end link networks is a very important research context in future. However, complex variable network environment and long-delay unreliable end-to-end transmission further aggravate the network security problem. Key management is a core research content of network security [16]. Group key management [17] play an important role in providing cryptographic methods and technologies for group members to support identity authentication, secure access, secure channel and integrity verification and other security strategy [**?**,18]. However, group key management must handle more difficulties in unreliable end-to-end link networks than reliable end-to-end link networks. Firstly there are a large number of interactions among members for key distribution, storage, negotiation, revocation and cancellation in existed group key management, and their efficiency of key management could be related to network scale, so every member need spend much time in sending and receiving key material. Secondly, members are deployed in a larger coverage area so as to key material is exposed in the air in a long distance, so compromising key material is a large probability event for an adversary, it is note that the synchronization mechanism also is almost failure for keep the key material fresh as the longtime delay and unreliable end-to-end link. Thirdly forward/backward security as typical security problems of group key management security is still guaranteed difficultly in condition of long time delay and non-reliable end-to-end link, because the rekeying is implemented difficultly in proper time. Therefore, group key management is a challenge issue in non-reliable end-to-end link networks.

Currently exited group key management schemes almost are based on reliable end-to-end link and short time delay, so all members can keep up with each other for implementing group key management scheme successfully in a short time [19], such as in shared key agreement schemes [20, 21], every member can compute a common key after it receives key material from other members with reliable end-to-end links, once rekeying happens all members must participate in rekeying process since every member has same key which is constructed with all members' key material [19], which result in that any compromised member can disclose the shared key of whole network. In existed non-shared-key group key management schemes, decryption key is different from encryption key, but the features that decryption key is banding encryption key also incurs the 1-affect-n problem that all members must participate in rekeying. Therefore, some group key management schemes are proposed based on multi decryption key protocol [22] in which multi decryption keys are corresponding to an encryption key, every legal member has a different decryption key and it meets key independence, the shared encryption key is constructed with all decryption keys, therefore it is difficult for an attacker to break other decryption keys even if some member's decryption key has been compromised by the attacker. The proposed scheme guarantees the forward/backward security, the message cost is reduced as the interaction cost of rekeying is not related to the network scale, and the dependency of reliable end-to-end link is also reduced as only the joining or leaving member participates in the rekeying. Therefore the proposed scheme is suitable to the non-reliable end-to-end link networks.

The remainder of this paper structured as follows. Section 2 reviews the research progress of group key management in non-reliable end-to-end networks; section 3 illustrates the proposed scheme; in section 4 and section 5 the security and efficient of the proposed scheme is analyzed; in section 6 several typical group key management schemes are compared with our suggested scheme, section 7 gives the conclusion.

2 State of The art

According to the cryptographic algorithm and the relationship between encryption key and decryption key, current group key management schemes for non-reliable end-to-end networks can be divided into three types, including pre-distribution group key management scheme based on symmetric cryptography, group key management scheme based on identity cryptography; group key management scheme based on asymmetric cryptography.

The pre-distributed group key management schemes based on symmetric key are mainly applied to sensor networks because of few calculation cost, it is suitable for self-organizing networks whose network size, topological structure rules and global prior knowledge are learned by an off-line key generate center, such as RPKM (Random Preconfigure Key Management) [23, 24], the center distributes parts of keys for every member from a key pool according to the topology structure, network scale and key scale, on the upside, two members can build a secure link if they have same key since a key could be shared by some different members, on the downside, some members could be broken if a compromised member disclosed part of keys although the compromised keys could account for a small proportion in the key pool. A key is distributed at random for some members in a large scale network so as to updating the key is a difficult problem, those members owning the same key are found difficulty in rekeying in large scale network [25, 26]. Therefore the pre-distributed group key management schemes cannot guarantee the forward/backward security, and they do not meet key independence, the defect of unreliable end-to-end link also exacerbates the difficulty of locating and updating keys.

In Identity-based Group Key Management schemes (IGKM) [27, 28], every member has a unique attribute or is assigned a unique identity by a key management center, the key management center generates a primary key which

is banding to decryption key computed with a member's identity, so as to a members can cooperation to compute a shared key with its identify and the primary key to build a secure channel without interaction [29] since their identities can be discriminated easily. However, only two members are allowed to negotiate a shared key in every consultation, the whole network could be compromised if the primary key is disclosed, and the scheme cannot guarantees key independence because every decryption key is generated with the primary key and its identity, once a member leaves network all member must participate in rekeying.

The special merit of public key enriches security function and improves performance for group key management, such as single-encryption-key multi-decryption-key key protocol [30], Chinese remainder theorem, bilinear pairing, and threshold key protocol and so on. In group key management schemes based on asymmetric cryptography, those schemes can be divided into two types according to the relationship between decryption key and encryption key, some schemes are based on one-decryption-key one-encryption-key key protocol in which an decryption key is corresponding to an encryption key, and other schemes are based on one-encryption-key multi-decryption-key key protocol in which a few of decryption keys are corresponding to an encryption key. Distinguishing from the traditional one-encryption-key one-decryption-key key protocol, in single-encryption-key multi-decryption-key key protocol every member has a different decryption key that meets key independence, so a member could keep its decryption key unchanged even if the corresponding encryption key must be updated. Typical schemes include PKM (Polynomial-based Key Management) [31], SLP (Security Lock Management) [32]. OMEDP (One-encryption-key multi-decryption-key Encryption Decryption Key) [30, 33], AGKA (Asymmetric Group Key Agreement) [34, 35], AOGKM (Autonomic Group Key Management) [22], AKMSN (Autonomic Shared Key Management in Space Networks) [36], OMKAP (One-encryption-key Multi-decryption-key Key Agreement Protocol) [37], NRLGKM [38], SGKM. The group key management schemes based on public key organization still relie on link for key agreement and rekeying, but it reduces the influence of unreliable end-to-end links on group key performance through public key characteristics, key material structure characteristics and dynamic key operation.

Although there are some group key management schemes for short time delay and reliable end-to-end links, they still cannot meet the security requirements of non-reliable end-to-end link networks. There are few studies on group key management based on asymmetric cryptography to provide security strategy for non-reliable end-to-end link networks. However un-reliable end-to-end link networks would be applied widely into deep space exploration, military unmanned aerial vehicle, remote area communication, wild animal tracking,it will be focus in future, it is necessary to study unreliable end-to-end networks as early as possible.

3 The Proposed Scheme

In order to describe the protocol process clearly to understand, we first describe two-party protocol and three-party protocol, and finally present multi-party protocol.

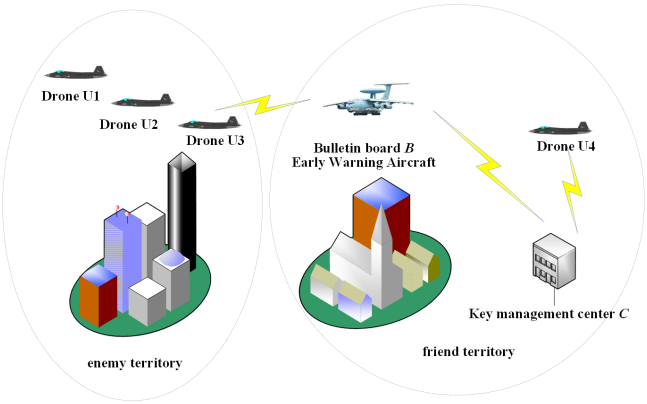


Figure 1: Network Structure

In suggested protocol, there are three kinds of entities: a key management server C, a bulletin board B and a number of legitimate members $u_i, i \in (1, 2, ..., n)$ .The C takes on the duty of collecting all decryption keys and generating an encryption key, its management range is limited, it cannot cover the whole network, the management range is only overlap bulletin board B, meanwhile it is absolute security for any legitimate member. The bulletin board B issues the encryption key publicly written by the C, it has enough memory to publish information on the encryption key material from all legitimate members and the C, all information written on B is public for any entity in networks. Each legitimate entity generates a different decryption key and sends it to the C, it gets a common encryption key from the B. For example, as shown in Figure 1, the legitimate members are a group of unmanned drones, they are composed into UAVs network deployed in a battlefield, a key management center is built on a safe location whose control area is limited and it is difficult to overlap the whole battlefield, the bulletin board is an early warning aircraft with which every drone has a high probability for communication.

The proposed protocol is based on the discrete logarithm algorithm, all legitimate members select F_p^* as finite group, is a generator of F_p^* and $\mathrm{H}(\cdot)$ is a hash function.

3.1 Two Parties Protocol

In two parties protocol, only two members $user_1$ and $user_2$ participate in the protocol. The protocol is composed of three phases including key agreement phase, encryption phase and decryption key.

3.1.1 Key Agreement Phase

In this phase, each member sends its secret decryption key to the C, subsequently the C generates a public encryption key with those secret decryption keys.

Step 1: A member $u_i, i \in (1,2)$ selects the random value x_{i1} and $x_{i2}, i \in (1,2)$ from the domain (1,p-1) as its decryption key $skey_i =< x_{i1}, x_{i2} >$, and send it to the with a security channel, the C keeps it secretly;

Step 2: After the C gathers all legitimate members' decryption keys, and keeps them as the decryption key set $\{< x_{i1}, x_{i2} >, i = 1,2\}$, subsequently it uses those decryption keys to compute a public encryption key $pkey =< pk_0 = g^{x_{11}x_{22}-x_{12}x_{21}}(modp), pk_1 = g^{x_{22}-x_{12}}(modp), pk_2 = g^{x_{11}-x_{21}}(modp) >$, and issues the public encryption key in the Bulletin board B.

3.1.2 Encryption Phase

In the encryption phase, a member gets an up-to-date public encryption key from the B. If the member need send a plaintext m to other members confidentially, it computes a ciphertext C of m with the public encryption key and a random value r, the r is selected from $(1, p-1)$. The is shown as following.

$$\begin{aligned} C &= < c_0 = mg^{(x_{11}x_{22}-x_{12}x_{21})r}(modp), \\ &\quad c_1 = g^{r(x_{22}-x_{12})}(modp), \\ &\quad c_2 = g^{r(x_{11}-x_{21})}(modp) > \end{aligned}$$

3.1.3 Decryption Phase

When a legal member receives a ciphertext C, it decrypts the ciphertext C with its decryption key. We assume the decrypter is u_i, it computes $g^{r(x_{22}-x_{12})x_{i1}}(modp)$ with $g^{r(x_{22}-x_{12})}(modp)$ and x_{i1},and computes $g^{r(x_{11}-x_{21})x_{i2}}(modp)$ with $g^{r(x_{11}-x_{21})}(modp)$ and x_{i2}. So the decryption result is $m^{'}$ as shown as following.

$$m^{'} = \frac{C}{\prod_{j=1}^{2} g^{r(x_{22}-x_{12})x_{ij}}(modp)}(modp)$$

3.1.4 Key Structure

We use matric structure to describe the relationship among decryption key. All decryption keys are composed into a matrix D, the row of matrix represents the decryption key of each member and the columns of matrix represents a component of decryption key, and $|D| \neq 0$.

$$D = \begin{vmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{vmatrix}$$

So the pubic key is expressed in matrix form as shown as following

$$\begin{aligned} pkey &= < pk_0 = g^{\begin{vmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{vmatrix}}(modp), \\ &\quad pk_1 = g^{\begin{vmatrix} 1 & x_{12} \\ 1 & x_{22} \end{vmatrix}}(modp), \\ &\quad pk_2 = g^{\begin{vmatrix} x_{11} & 1 \\ x_{21} & 1 \end{vmatrix}}(modp) > \end{aligned}$$

The following formula holds, its value is equal to the second part pk_1 of public encryption key.

$$g^{\frac{\begin{vmatrix} |D| & x_{12} \\ |D| & x_{22} \end{vmatrix}}{\begin{vmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{vmatrix}}}(modp) = g^{\begin{vmatrix} 1 & x_{12} \\ 1 & x_{22} \end{vmatrix}}(modp) = g^{(x_{22}-x_{21})}(modp).$$

And the third part pk_2 of public encryption key is got from the following formula.

$$g^{\frac{\begin{vmatrix} x_{11} & |D| \\ x_{21} & |D| \end{vmatrix}}{\begin{vmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{vmatrix}}}(modp) = g^{\begin{vmatrix} x_{11} & 1 \\ x_{21} & 1 \end{vmatrix}}(modp) = g^{(x_{11}-x_{21})}(modp)$$

So any member can get a result $|D|$ with its decryption key and public encryption key material, the result is shown as following.

$$\begin{aligned} \sum_{j=1}^{2}(pk_j)^{x_{ij}} &= (pk_1)^{x_{i1}} + (pk_2)^{x_{i2}} \\ &= g^{\begin{vmatrix} 1 & x_{12} \\ 1 & x_{22} \end{vmatrix}_{x_{i1}} + \begin{vmatrix} x_{11} & 1 \\ x_{21} & 1 \end{vmatrix}_{x_{i2}}}(modp) \\ &= g^{\begin{vmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{vmatrix}}(modp) \end{aligned}$$

3.2 Three Parties Protocol

Three members $user_1$,$user_2$ and $user_3$ participate in protocol. Similar to the two parties protocol, Three-party protocol is composed of three phases including key agreement phase, encryption phase and decryption phase.

3.2.1 Key Agreement Phase

In this phase, similarly, all members $u_i, i \in \{1,2,3\}$ negotiate the public encryption key with the C, and each member sends its decryption key to the C.

Step 1: A member $u_i, i \in \{1,2,3\}$ selects the random value x_{i1},x_{i2} and x_{i3} $i \in \{1,2,3\}$ from the domain $(1, p-1)$ as its decryption key $skey_i =< x_{i1}, x_{i2}x_{i3} >$, and sends it to the C with a security channel, the C keeps it secretly;

Step 2: After the C gathers all legitimate members' decryption keys as the key set $\{< x_{i1}, x_{i2}, x_{i3} >, i = 1, 2, 3\}$, subsequently it uses those decryption keys to compute a public encryption key $pkey$, and issues the public encryption key on the bulletin board B.

$$\begin{aligned} &pkey = \\ &< pk_0 = g^{(x_{11}x_{22}x_{33}+x_{12}x_{23}x_{31}+x_{13}x_{21}x_{32})}, \\ &\qquad g^{(-x_{13}x_{22}x_{31}-x_{23}x_{32}x_{11}-x_{33}x_{12}x_{21})}, \\ &pk_1 = g^{(x_{22}x_{33}+x_{12}x_{23}+x_{32}x_{13}-x_{13}x_{22}-x_{23}x_{32}-x_{12}x_{33})}, \\ &pk_2 = g^{(x_{11}x_{33}+x_{21}x_{13}+x_{23}x_{31}-x_{13}x_{31}-x_{23}x_{11}-x_{21}x_{33})}, \\ &pk_3 = g^{(x_{11}x_{22}+x_{21}x_{32}+x_{12}x_{31}-x_{22}x_{31}-x_{12}x_{21}-x_{11}x_{32})} \\ &\qquad\qquad\qquad\qquad (\mod p) > \end{aligned}$$

3.2.2 Encryption Phase

In the encryption phase, a member gets an up-to-date public key from B. If the member need send a plaintext m to other members confidentially, it computes the ciphertext C of m with the public encryption and a random value r from $(1, p-1)$. The C is shown as following.

$$\begin{aligned} &C =< c_0 = \\ &mg^{r(x_{11}x_{22}x_{33}+x_{12}x_{23}x_{31}+x_{13}x_{21}x_{32}-x_{13}x_{22}x_{31})}, \\ &\qquad g^{-x_{23}x_{32}x_{11}-x_{33}x_{12}x_{21})}, \\ &c_1 = g^{r(x_{22}x_{33}+x_{12}x_{23}+x_{32}x_{13}-x_{13}x_{22}-x_{23}x_{32}-x_{12}x_{33})}, \\ &c_2 = g^{r(x_{11}x_{33}+x_{21}x_{13}+x_{23}x_{31}-x_{13}x_{31}-x_{23}x_{11}-x_{21}x_{33})}, \\ &c_3 = g^{r(x_{11}x_{22}+x_{21}x_{32}+x_{12}x_{31}-x_{22}x_{31}-x_{12}x_{21}-x_{11}x_{32})} \\ &(modp) > \end{aligned}$$

3.2.3 Decryption Phase

In the decryption phase, a legal member $u_i, i \in \{1, 2, 3\}$ receives a ciphertext C, it decrypts the ciphertext C with its decryption key $skey_i$. The user computes

$$g^{r(x_{22}x_{33}+x_{12}x_{23}+x_{32}x_{13}-x_{13}x_{22}-x_{23}x_{32}-x_{12}x_{33})x_{i1}}(modp)$$

with $g^{r(x_{22}x_{33}+x_{12}x_{23}+x_{32}x_{13}-x_{13}x_{22}-x_{23}x_{32}-x_{12}x_{33})}(modp)$ and x_{i1}, computes

$$g^{r(x_{11}x_{33}+x_{21}x_{13}+x_{23}x_{31}-x_{13}x_{31}-x_{23}x_{11}-x_{21}x_{33})x_{i2}}(modp)$$

with $g^{r(x_{11}x_{33}+x_{21}x_{13}+x_{23}x_{31}-x_{13}x_{31}-x_{23}x_{11}-x_{21}x_{33})}(modp)$ and x_{i2}, and computes

$$g^{r(x_{11}x_{22}+x_{21}x_{32}+x_{12}x_{31}-x_{22}x_{31}-x_{12}x_{21}-x_{11}x_{32})x_{i3}}(modp) >$$

with $g^{r(x_{11}x_{22}+x_{21}x_{32}+x_{12}x_{31}-x_{22}x_{31}-x_{12}x_{21}-x_{11}x_{32})}(modp) >$ and x_{i2}. So the decryption result is $m^{'}$ as shown as following.

$$m^{'} = \frac{C(modp)}{\sum_{j=1}^{2} g^{r(x_{22}x_{33}+x_{12}x_{23}+x_{32}x_{13}-x_{13}x_{22}-x_{23}x_{32}-x_{12}x_{33})x_{ij}}}$$

3.2.4 Key Structure

The decryption keys are described with a matrix D as shown as following, the matrix has three rows and three columns, and $|D| \neq 0$.

$$D = \begin{vmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{vmatrix}$$

So the public encryption key is shown as following.

$$\begin{aligned} pkey \quad = \quad &< pk_1 = g^{\begin{vmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{vmatrix}}(modp), \\ &pk_2 = g^{\begin{vmatrix} 1 & x_{12} & x_{13} \\ 1 & x_{22} & x_{23} \\ 1 & x_{32} & x_{33} \end{vmatrix}}(modp), \\ &pk_3 = g^{\begin{vmatrix} x_{11} & 1 & x_{13} \\ x_{21} & 1 & x_{23} \\ x_{31} & 1 & x_{33} \end{vmatrix}}(modp), \\ &pk_4 = g^{\begin{vmatrix} x_{11} & x_{12} & 1 \\ x_{21} & x_{22} & 1 \\ x_{31} & x_{32} & 1 \end{vmatrix}}(modp) > \end{aligned}$$

The value of following formula is equal to the second part pk_1 of public encryption key $pkey$.

$$g^{\frac{\begin{vmatrix} |D| & x_{12} & x_{13} \\ |D| & x_{22} & x_{23} \\ |D| & x_{32} & x_{33} \end{vmatrix}}{\begin{vmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{vmatrix}}}(modp) = g^{\begin{vmatrix} 1 & x_{12} & x_{13} \\ 1 & x_{22} & x_{23} \\ 1 & x_{32} & x_{33} \end{vmatrix}}(modp)$$

The second part pk_2 of public encryption key $pkey$ meets the following formula.

$$g^{\frac{\begin{vmatrix} x_{11} & |D| & x_{13} \\ x_{21} & |D| & x_{22} \\ x_{31} & |D| & x_{33} \end{vmatrix}}{\begin{vmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{vmatrix}}}(modp) = g^{\begin{vmatrix} x_{11} & 1 & x_{13} \\ x_{21} & 1 & x_{23} \\ x_{31} & 1 & x_{33} \end{vmatrix}}(modp)$$

The second part pk_3 of public encryption key $pkey$ meets the following formula.

$$g^{\frac{\begin{vmatrix} x_{11} & x_{12} & |D| \\ x_{21} & x_{22} & |D| \\ x_{31} & x_{32} & |D| \end{vmatrix}}{\begin{vmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{vmatrix}}}(modp) = g^{\begin{vmatrix} x_{11} & x_{12} & 1 \\ x_{21} & x_{22} & 1 \\ x_{31} & x_{32} & 1 \end{vmatrix}}(modp)$$

So any member can get a result $|D|$ with its decryption key and public encryption key material, the result is

shown as following.

$$\begin{aligned}
&\sum_{j=1}^{n}(pk_j)^{x_{ij}} \\
= \;& (pk_1)^{x_{i1}} + (pk_2)^{x_{i2}} + (pk_3)^{x_{i3}} \\
= \;& g^{\begin{vmatrix}1 & x_{12} & x_{13}\\ 1 & x_{22} & x_{23}\\ 1 & x_{32} & x_{33}\end{vmatrix}x_{i1}+\begin{vmatrix}x_{11} & 1 & x_{13}\\ x_{21} & 1 & x_{23}\\ x_{31} & 1 & x_{33}\end{vmatrix}x_{i2}+\begin{vmatrix}x_{11} & x_{12} & 1\\ x_{21} & x_{22} & 1\\ x_{31} & x_{32} & 1\end{vmatrix}x_{i3}} \\
= \;& g^{\begin{vmatrix}x_{11} & x_{12} & x_{13}\\ x_{21} & x_{22} & x_{23}\\ x_{31} & x_{32} & x_{33}\end{vmatrix}}(modp)
\end{aligned}$$

On the basis of above analysis, the definition is given.
Definition 1 Key Matrix, all legitimate members' decryption keys are composed of a matrix, the row of matrix represents the decryption key of each member and the columns of matrix represents a component of decryption key, the matrix is called a key matrix in which the scale of decryption key is same. For example, the following key matrix D has n rows and n columns, so n decryption keys are from n members.

$$D = \begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} \\ x_{21} & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & x_{nn} \end{vmatrix}$$

3.3 Multi Parties Protocol

In multi parties protocol,n users participate in the scheme, and we can use matrix structure to describe their decryption key and encryption key. The multi-party protocol composed of five phases including key agreement phase, encryption phase, decryption phase, joining key operation phase and leaving key operation phase.

3.3.1 Key Agreement Phase

In this phase, a number of members $u_i, i \in \{1, 2, ..., n\}$ negotiate the public encryption key and their secret decryption key with the C.

Step 1: A member $u_i, i \in \{1, 2, ..., n\}$ selects some random values,$x_{i1}, x_{i2} \ldots, x_{in} i \in \{1, 2, ..., n\}$ from the domain $(1, p-1)$ as its decryption key $< x_{i1}, x_{i2} \ldots, x_{in} >$, and send those values to C with a security channel, the C keeps it secretly, so the decryption key is described with a matrix D as shown as following, the matrix has n rows and n columns;

$$D = \begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} \\ x_{21} & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & x_{nn} \end{vmatrix}$$

Step 2: After the C gathers all legitimate members decryption keys as a key set $\{< x_{i1}, x_{i2} \ldots, x_{in} >\}$, subsequently it uses those decryption keys to compute a public encryption key $pkey$, and issues the public encryption key on bullet board B.

$$\begin{aligned}
pkey \;=\; & < pk_0 = g^{\begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} \\ x_{21} & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & x_{nn} \end{vmatrix}}(modp), \\
& pk_1 = g^{\begin{vmatrix} 1 & x_{12} & ... & x_{1n} \\ 1 & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ 1 & x_{n2} & ... & x_{nn} \end{vmatrix}}(modp), \\
& pk_2 = g^{\begin{vmatrix} x_{11} & 1 & ... & x_{1n} \\ x_{21} & 1 & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & 1 & ... & x_{nn} \end{vmatrix}}(modp), ..., \\
& pk_n = g^{\begin{vmatrix} x_{11} & x_{12} & ... & 1 \\ x_{21} & x_{22} & ... & 1 \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & 1 \end{vmatrix}}(modp) >
\end{aligned}$$

3.3.2 Encryption Phase

In the encryption phase, a member gets an up-to-date public key from B. If the member need send a plaintext m to other members confidentially, it computes the ciphertext C of m with the public encryption and a random value r from $(1, p-1)$. The C is shown as following.

$$\begin{aligned}
C \;=\; & < c_0 = mg^{r\begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} \\ x_{21} & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & x_{nn} \end{vmatrix}}(modp), \\
& c_1 = g^{r\begin{vmatrix} 1 & x_{12} & ... & x_{1n} \\ 1 & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ 1 & x_{n2} & ... & x_{nn} \end{vmatrix}}(modp), \\
& c_2 = g^{r\begin{vmatrix} x_{11} & 1 & ... & x_{1n} \\ x_{21} & 1 & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & 1 & ... & x_{nn} \end{vmatrix}}(modp), ..., \\
& c_n = g^{r\begin{vmatrix} x_{11} & x_{12} & ... & 1 \\ x_{21} & x_{22} & ... & 1 \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & 1 \end{vmatrix}}(modp) >
\end{aligned}$$

3.3.3 Decryption Phase

A legal member $user_i$ uses the public key material $< pk_1, pk_2, ..., pk_n >$ and its decryption key $< x_{i1}, x_{i2}, ..., x_{in} >$ to compute the following values.

$$< g^{\begin{vmatrix} 1 & x_{12} & ... & x_{1n} \\ 1 & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ 1 & x_{n2} & ... & x_{nn} \end{vmatrix}x_{i1}r}(modp), g^{r\begin{vmatrix} x_{11} & 1 & ... & x_{1n} \\ x_{21} & 1 & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & 1 & ... & x_{nn} \end{vmatrix}x_{i2}r}(modp),$$

$..., g^{\begin{vmatrix} x_{11} & x_{12} & ... & 1 \\ x_{21} & x_{22} & ... & 1 \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & 1 \end{vmatrix}_{x_{in}r}} (modp) >$ After that, the member computes plaintext $m^{'}$ with the following formula.

$$m^{'} = \frac{C}{\prod_{j=1}^{n} g^{\begin{vmatrix} 1 & x_{12} & ... & x_{1n} \\ 1 & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ 1 & x_{n2} & ... & x_{nn} \end{vmatrix}_{x_{ij}r}}} (modp)$$

3.3.4 Decryption Phase

When a new member $user_{n+1}$ joins network, joining key operation is implemented for rekeying.

Step 1: The new member selects a decryption key $< x_{n+11}, x_{n+12}, ..., x_{n+1n} >$ from $(1, p-1)$ and sends it to the key management center C via a secure channel.

Step 2: The C updates the key matrix D with the new decryption key as follows, the scale of new $D^{'}$ increase to $n+1$ rows and $n+1$ columns;

$$D^{'} = \begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} & x_{1n+1} \\ x_{21} & x_{22} & ... & x_{2n} & x_{2n+1} \\ ... & ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & x_{nn} & x_{nn+1} \\ x_{n+11} & x_{n+12} & ... & x_{n+1n} & x_{n+1n+1} \end{vmatrix} = \begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} & H(x_{11}, x_{12}, .., x_{1n}) \\ x_{21} & x_{22} & ... & x_{2n} & H(x_{21}, x_{22}, .., x_{2n}) \\ ... & ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & x_{nn} & H(x_{n1}, x_{n2}, .., x_{nn}) \\ x_{n+11} & x_{n+12} & ... & x_{n+1n} & x_{n+1n+1} \end{vmatrix}$$

Step 3: Every member except the new member computes a new decryption key $< x_{i1}, x_{i2}, ..., x_{in}, H(x_{i1}, x_{i2}, .., x_{in}) >$, the scale of decryption key increase to $n+1$, the new component is $H(x_{i1}, x_{i2}, .., x_{in})$ with the hash function$H(\cdot)$;

Step 4: The key management center computes the new public encryption key and issues it on B.

$$pkey^{'} =< pk_0 = g^{\begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} & x_{1n+1} \\ x_{21} & x_{22} & ... & x_{2n} & x_{2n+1} \\ ... & ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & x_{nn} & x_{nn+1} \\ x_{n+11} & x_{n+12} & ... & x_{n+1n} & x_{n+1n+1} \end{vmatrix}} (modp),$$

$$pk_1 = g^{\begin{vmatrix} 1 & x_{12} & ... & x_{1n} & x_{1n+1} \\ 1 & x_{22} & ... & x_{2n} & x_{2n+1} \\ ... & ... & ... & ... & ... \\ 1 & x_{n2} & ... & x_{nn} & x_{nn+1} \\ x_{n+11} & x_{n+12} & ... & x_{n+1n} & x_{n+1n+1} \end{vmatrix}} (modp),$$

$$pk_2 = g^{\begin{vmatrix} x_{11} & 1 & ... & x_{1n} & x_{1n+1} \\ x_{21} & 1 & ... & x_{2n} & x_{2n+1} \\ ... & ... & ... & ... & ... \\ x_{n1} & 1 & ... & x_{nn} & x_{nn+1} \\ x_{n+11} & 1 & ... & x_{n+1n} & x_{n+1n+1} \end{vmatrix}} (modp), ...,$$

$$pk_{n+1} = g^{\begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} & 1 \\ x_{21} & x_{22} & ... & x_{2n} & 1 \\ ... & ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & x_{nn} & 1 \\ x_{n+11} & x_{n+12} & ... & x_{n+1n} & 1 \end{vmatrix}} (modp) >$$

3.3.5 Leaving Key Operation

When a member $user_n$ leaves network, leaving key operation is implemented for rekeying.

Step 1: The member sends a leaving message to other members and the key management center;

Step 2: The c updates the key matrix $D^{'}$, the last column is deleted from the matrix D.

$$D^{'} = \begin{vmatrix} x_{11} & x_{12} & ... & x_{1n-1} \\ x_{21} & x_{22} & ... & x_{2n-1} \\ ... & ... & ... & ... \\ x_{n-11} & x_{n-12} & ... & x_{n-1n-1} \end{vmatrix}$$

Step 3: Remainder legal members $user_i, i \in \{1, 2, ..., n-1\}$ update their new decryption keys $< x_{i1}, x_{i2}, .., x_{in-1}, >$;

Step 4: The C computes a new encryption key and issue it on the B;

$$pkey^{'} =< pk_0 = g^{\begin{vmatrix} x_{11} & x_{12} & ... & x_{1n-1} \\ x_{21} & x_{22} & ... & x_{2n-1} \\ ... & ... & ... & ... \\ x_{n-11} & x_{n-12} & ... & x_{n-1n-1} \end{vmatrix}} (modp),$$

$$pk_1 = g^{\begin{vmatrix} 1 & x_{12} & ... & x_{1n-1} \\ 1 & x_{22} & ... & x_{2n-1} \\ ... & ... & ... & ... \\ 1 & x_{n-12} & ... & x_{n-1n-1} \end{vmatrix}} (modp),$$

$$pk_2 = g^{\begin{vmatrix} x_{11} & 1 & ... & x_{1n-1} \\ x_{21} & 1 & ... & x_{2n-1} \\ ... & ... & ... & ... \\ x_{n-11} & 1 & ... & x_{n-1n-1} \end{vmatrix}} (modp), ...,$$

$$pk_{n-1} = g^{\begin{vmatrix} x_{11} & x_{12} & ... & 1 \\ x_{21} & x_{22} & ... & 1 \\ ... & ... & ... & ... \\ x_{n-11} & x_{n-12} & ... & 1 \end{vmatrix}} (modp) >$$

4 Security Analysis

4.1 Key Independence

Key Independence is an important security quality in group key management, and it means that the probability of compromising other legal decryptions is negligible for a member having a legal decryption key. Firstly, the member's decryption key is selected from field $(1, p)$, and they are different each other, so it is difficult to guess a decryption key. Secondly, even if a member has a legal decryption key and gets a public key, if it compromises other member's decryption key successfully, it must break DH problem.

For an attacker, it has a legal decryption key$< x_{j1}, x_{j2}, .., x_{jn} >$, and its decryption key meets the formula as shown as following.

$$\prod_{k=1}^{n} (pk_k)^{x_{jk}} = g^{\begin{vmatrix} 1 & x_{12} & ... & x_{1n} \\ 1 & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ 1 & x_{n2} & ... & x_{nn} \end{vmatrix}_{x_{j1}}} + g^{\begin{vmatrix} x_{11} & 1 & ... & x_{1n} \\ x_{21} & 1 & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & 1 & ... & x_{nn} \end{vmatrix}_{x_{j2}}}$$

$$+...+g^{\begin{vmatrix} x_{11} & x_{12} & ... & 1 \\ x_{21} & x_{22} & ... & 1 \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & 1 \end{vmatrix}_{x_{jn}}} = g^{\begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} \\ x_{21} & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & x_{nn} \end{vmatrix}}$$

If the attacker want to get another legal decryption key $< x_{i1}, x_{i2}, .., x_{in} >$ to meets the below formula as showing

$$g^{\begin{vmatrix} 1 & x_{12} & ... & x_{1n} \\ 1 & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ 1 & x_{n2} & ... & x_{nn} \end{vmatrix}_{x_{i1}}} + g^{\begin{vmatrix} x_{11} & 1 & ... & x_{1n} \\ x_{21} & 1 & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & 1 & ... & x_{nn} \end{vmatrix}_{x_{i2}}} + ...+$$

$$g^{\begin{vmatrix} x_{11} & x_{12} & ... & 1 \\ x_{21} & x_{22} & ... & 1 \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & 1 \end{vmatrix}_{x_{in}}} = g^{\begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} \\ x_{21} & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & x_{nn} \end{vmatrix}}$$

However, those values $< pk_2, pk_3, .., pk_n >$ come from the public material key $pkey$ from bulletin board. Even if the attacker can get the public material key $pkey$. According to the DH hard problem, the probability of compromising $< d_1, d_2, .., d_n >$ is negligible.

Therefore, the probability of compromising of an decryption key is $\frac{1}{|P|^n - 1}$, so the probability of compromising of decryption key is $\frac{n-1}{|P|^n - 1}$ for the attacker.

4.2 Forward Security

A member cannot decrypt a ciphertext successfully after it leaves network, in other words its decryption key is not validity. The matrix of decryption key is shown as following.

$$D = \begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} \\ x_{21} & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & x_{nn} \end{vmatrix}$$

After the member $user_n$ leaved network, so the matrix of decryption key is updated as following.

$$D^{'} = \begin{vmatrix} x_{11} & x_{12} & ... & x_{1n-1} \\ x_{21} & x_{22} & ... & x_{2n-2} \\ ... & ... & ... & ... \\ x_{n-11} & x_{n-12} & ... & x_{n-1n-1} \end{vmatrix}$$

And the encryption key is updated as shown as following

$$pk^{'} =< pk_0 = g^{\begin{vmatrix} x_{11} & x_{12} & ... & x_{1n-1} \\ x_{21} & x_{22} & ... & x_{2n-1} \\ ... & ... & ... & ... \\ x_{n-11} & x_{n-12} & ... & x_{n-1n-1} \end{vmatrix}}(modp),$$

$$pk_1 = g^{\begin{vmatrix} 1 & x_{12} & ... & x_{1n-1} \\ 1 & x_{22} & ... & x_{2n-1} \\ ... & ... & ... & ... \\ 1 & x_{n-12} & ... & x_{n-1n-1} \end{vmatrix}}(modp),$$

$$pk_2 = g^{\begin{vmatrix} x_{11} & 1 & ... & x_{1n-1} \\ x_{21} & 1 & ... & x_{2n-1} \\ ... & ... & ... & ... \\ x_{n-11} & 1 & ... & x_{n-1n-1} \end{vmatrix}}(modp), ...,$$

$$pk_{n-1} = g^{\begin{vmatrix} x_{11} & x_{12} & ... & 1 \\ x_{21} & x_{22} & ... & 1 \\ ... & ... & ... & ... \\ x_{n-11} & x_{n-12} & ... & 1 \end{vmatrix}}(modp) >$$

If the leaving member $user_n$ want to decrypt a cipher text successfully generated with the new public key $pkey$, it need choose $< x^{'}_{n1}, x^{'}_{n2}, , .., x^{'}_{nn-1} >$ to meet the following formula.

$$\begin{vmatrix} 1 & x_{12} & ... & x_{1n-1} \\ 1 & x_{22} & ... & x_{2n-1} \\ ... & ... & ... & ... \\ 1 & x_{n-12} & ... & x_{n-1n-1} \end{vmatrix} x^{'}_{n1} +$$

$$\begin{vmatrix} x_{11} & 1 & ... & x_{1n-1} \\ x_{21} & 1 & ... & x_{2n-1} \\ ... & ... & ... & ... \\ x_{n-11} & 1 & ... & x_{n-1n-1} \end{vmatrix} x^{'}_{n2} + ... +$$

$$\begin{vmatrix} x_{11} & x_{12} & ... & 1 \\ x_{21} & x_{22} & ... & 1 \\ ... & ... & ... & ... \\ x_{n-11} & x_{n-12} & ... & 1 \end{vmatrix} x^{'}_{nn-1}$$

$$= \begin{vmatrix} x_{11} & x_{12} & ... & x_{1n-1} \\ x_{21} & x_{22} & ... & x_{2n-2} \\ ... & ... & ... & ... \\ x_{n-11} & x_{n-12} & ... & x_{n-1n-1} \end{vmatrix} >$$

Even if the member can get encryption key material $< pk_1, pk_2, .., pk_n >$ from the bulletin board, but the powers of $< pk_1, pk_2, .., pk_n >$ is difficult to break according to the discrete logarithm hard problem. So if the cipher text is generated after the member leaves network, the probability of breaking a cipher is $\frac{n-1}{|P|^{n-1}}$, And the probability of breaking a cipher is negligible for the leaving member.

4.3 Backward Security

A new member cannot decrypt a cipher text successfully that is generated before the new member joins network. The matrix of decryption key is shown as below.

$$D = \begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} \\ x_{21} & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & x_{nn} \end{vmatrix}$$

After the new member $user_{n+1}$ joins network, the matrix of decryption key is updated as below.

$$D^{'} = \begin{vmatrix} x_{11} & x_{12} & ... & x_{1n+1} \\ x_{21} & x_{22} & ... & x_{2n+2} \\ ... & ... & ... & ... \\ x_{n+11} & x_{n+12} & ... & x_{n+1n+1} \end{vmatrix}$$

The C computes a new public encryption key.

$$pk^{'} =< g^{\begin{vmatrix} x_{11} & x_{12} & ... & x_{1n+1} \\ x_{21} & x_{22} & ... & x_{2n+2} \\ ... & ... & ... & ... \\ x_{n+11} & x_{n+12} & ... & x_{n+1n+1} \end{vmatrix}}(modp),$$

$$g^{\begin{vmatrix} 1 & x_{12} & ... & x_{1n+1} \\ 1 & x_{22} & ... & x_{2n+2} \\ ... & ... & ... & ... \\ 1 & x_{n+12} & ... & x_{n+1n+1} \end{vmatrix}}(modp), g^{\begin{vmatrix} x_{11} & 1 & ... & x_{1n+1} \\ x_{21} & 1 & ... & x_{2n+2} \\ ... & ... & ... & ... \\ x_{n+11} & 1 & ... & x_{n+1n+1} \end{vmatrix}}$$

$$(modp), ..., g^{\begin{vmatrix} x_{11} & x_{12} & ... & 1 \\ x_{21} & x_{22} & ... & 1 \\ ... & ... & ... & ... \\ x_{n+11} & x_{n+12} & ... & 1 \end{vmatrix}}(modp) >$$

If the new member can break the cipher text decrypted with $pkey$, it must choose values $< x_{n1}^{'}, x_{n2}^{'}, .., x_{nn}^{'} >$ to meet the below formula.

$$\begin{vmatrix} 1 & x_{12} & ... & x_{1n} \\ 1 & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ 1 & x_{n-12} & ... & x_{nn} \end{vmatrix} x_{n1}^{'} + \begin{vmatrix} x_{11} & 1 & ... & x_{1n} \\ x_{21} & 1 & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n} & 1 & ... & x_{nn} \end{vmatrix} x_{n2}^{'} + ... + \begin{vmatrix} x_{11} & x_{12} & ... & 1 \\ x_{21} & x_{22} & ... & 1 \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & 1 \end{vmatrix} x_{nn}^{'} = \begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} \\ x_{21} & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & x_{nn} \end{vmatrix}$$

However, although the new member can get $< pk_1, pk_2, ..., pk_n >$from public encryption key, but the powers of $< pk_1, pk_2, ..., pk_n >$ is unknown and is hardly broken for the new member according to discrete logarithm hard problem, The probability of breaking a cipher is $\frac{n}{|P|^n}$ and negligible for the new member, so the probability of breaking a cipher is negligible for the new member.

4.4 Decryption Correctness

The decryption correctness means that a legal member can decrypt a ciphertext successfully with its correct decryption key, a legal decryption key is a row of the matrix D.

$$D = \begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} \\ x_{21} & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & x_{nn} \end{vmatrix}$$

Any correct decryption key meets the following Formula (1), $< pk_1, pk_2, ..., pk_n >$ is public encryption key material.

So the decryption process is formula.

$$\frac{mg^{r\begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} \\ x_{21} & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & x_{nn} \end{vmatrix}}(modp)}{g^{\sum_{j=1}^{n} x_{ij} r \begin{vmatrix} 1 & x_{12} & ... & x_{1n} \\ 1 & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ 1 & x_{n2} & ... & x_{nn} \end{vmatrix}}} = \frac{mg^{r\begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} \\ x_{21} & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & x_{nn} \end{vmatrix}}(modp)}{g^{r\begin{vmatrix} x_{11} & x_{12} & ... & x_{1n} \\ x_{21} & x_{22} & ... & x_{2n} \\ ... & ... & ... & ... \\ x_{n1} & x_{n2} & ... & x_{nn} \end{vmatrix}}} = m$$

So a member having a legal decryption key can decrypt a cipher text successfully.

5 Efficient Analysis

The efficient of multi parties protocol is analyzed in aspect of computation cost, message cost, network overload and storage cost.

5.1 Computation Cost

The suggested protocol is based on Discrete Logarithm Problem(DLP), the most complex operation is modular exponentiation computation, so the number of modular exponentiation operations is counted to evaluated the computation cost of protocol. In key agreement phase, the C selects n^2 random values, computes $n+1$ modular exponentiations to compute the public encryption key $pkey$. In the encryption phase, an encrypter implements $n+1$ modular exponentiation operations and a modular multiplication operation. In the decryption phase, a decrypter implements $n+1$ modular exponentiation operations and a modular multiplication operation. In the joining key operation, all members except the new member carry on a hash function once, the C implements $n+2$ modular exponentiation operations and n hash function computation to update the public encryption key. In the leaving key operation, the C implements n modular exponentiation operations to update the public encryption key. So the computation cost is related to the network scale.

5.2 Message Cost

In the key agreement phase, every member sends its decryption key to the C via a secure channel. The C sends a message about encryption key to the B after rekeying. In the joining key operation phase and the leaving key operation phase, only a joining or leaving message is sent by the joining member or the leaving member to all members. Except the joining or leaving member other members don't participate in rekeying to provide key material, so there aren't interactions among those remainder members. Therefore the message cost is not related to the scale of network.

5.3 Network Overload

We assume that the size of message block is L. a decryption key $skey_i$ compose of n parts, so it's size is nL. A public encryption key compose of n parts, so it's size is

$$g^{x_{i1}\begin{vmatrix}1 & x_{12} & ... & x_{1n}\\ 1 & x_{22} & ... & x_{2n}\\ ... & ... & ... & ...\\ 1 & x_{n2} & ... & x_{nn}\end{vmatrix}}(modp)+g^{x_{i2}\begin{vmatrix}x_{11} & 1 & ... & x_{1n}\\ x_{21} & 1 & ... & x_{2n}\\ ... & ... & ... & ...\\ x_{n1} & 1 & ... & x_{nn}\end{vmatrix}}(modp)+...+g^{x_{in}\begin{vmatrix}x_{11} & x_{12} & ... & 1\\ x_{21} & x_{22} & ... & 1\\ ... & ... & ... & ...\\ x_{n1} & x_{n2} & ... & 1\end{vmatrix}}(modp)=$$
$$g^{x_{i1}\begin{vmatrix}1 & x_{12} & ... & x_{1n}\\ 1 & x_{22} & ... & x_{2n}\\ ... & ... & ... & ...\\ 1 & x_{n2} & ... & x_{nn}\end{vmatrix}+x_{i2}\begin{vmatrix}x_{11} & 1 & ... & x_{1n}\\ x_{21} & 1 & ... & x_{2n}\\ ... & ... & ... & ...\\ x_{n1} & 1 & ... & x_{nn}\end{vmatrix}+...+x_{in}\begin{vmatrix}x_{11} & x_{12} & ... & 1\\ x_{21} & x_{22} & ... & 1\\ ... & ... & ... & ...\\ x_{n1} & x_{n2} & ... & 1\end{vmatrix}}(modp)=g^{x_{i1}\begin{vmatrix}x_{11} & x_{12} & ... & x_{1n}\\ x_{21} & x_{22} & ... & x_{2n}\\ ... & ... & ... & ...\\ x_{n1} & x_{n2} & ... & x_{nn}\end{vmatrix}}(modp) \quad (1)$$

$(n+1)L$. The overload of sending the public key encryption key by the C is $(n+1)L$, the overload of encryption is $(n+1)L$, the overload that a member joins or leaves network is L. Therefore, the network overload of issuing encryption key is related to the network scale, the network overload of rekeying is not related to the network size.

5.4 Storage Cost

All entities must have enough storage cost to keep their decryption keys, encryption keys and cipher text at least. As the size of decryption key is nL, the size of public encryption key is $(n+1)L$, the size of ciphertext is $(n+1)L$,the size of plaintext is L. Therefore, every member should has nL units at least to keep decryption keys,$(n+1)L$ units to accept cipher text,L units to hold plaintext, so every member needs $3nL$+$3L$ units. The C should have $(n^2+n+1)L$ units to preserve all decryption keys and encryption key. The B must use $(n+1)L$ units to issue a public encryption key. So the storage cost is related to the network scale.

6 Schemes Comparison

Our suggested scheme is compares with several typical exited group key management schemes RPKM, IGKM, OMEDP, AGKA, AOGKM, AKMSN, NRLGKM and OMKAP for non-reliable end-to-end link network from security and efficiency aspects.

6.1 Security Comparison

Key independence, forward/backward security, the relationship between decryption key and encryption key, collusion attack and cryptographic technology are selected as security valuation criteria. The scheme RPKM is based on symmetric cryptography and its relationship between decryption key and encryption key is 1-to-1 that means a decryption key corresponds to an encryption key, the scheme cannot guarantee key independence, forward security and backward security since a key could be shared by some members from a key pool, part of keys from the pool could be compromised with collusion attack method as every key could be used by different members. The Scheme IGKM is based on identity-based cryptography, and every member's decryption key is band to the primary key with its identity, so the key independence cannot be guaranteed so that an adversary can fabricate a legitimate decryption key with a primary key and a legitimate identity, the primary key must be updated when a member joins or leaves network otherwise the forward/backward security cannot be guaranteed. OMEDP, AGKA, AOGKM, AKMSN, OMKAP and our suggested scheme are based on multi-decryption-key single-encryption-key key protocol, so their relationship between encryption key and decryption key is 1-to-n that means an encryption key corresponds to n decryption keys, only the decryption key of joining or leaving member need be revocation or cancelled with the merit of multi-decryption-key single-encryption-key key protocol, thus they guarantee key independence, those schemes ensure that forward security and backward security as the encryption key is updated, however OMEDP and OMKAP are not against the collusion attack as they are designed with threshold cryptography technology. Therefore, our suggested scheme is suitable to the security requirements of non-reliable end-to-end link network.

6.2 Efficiency Comparison

The efficiency of group key management focus on the cost of rekeying, which include computation cost, message cost, network overload and storage cost. Moreover, those criterions including equipment and rekeying scale are also compared among those typical schemes. In the table 1 the parameters n and L are network scale and the message length of unit.

All schemes except AGKM take advantage of an off-line center who takes on the initial phase, the center generates all decryption key for all members and their corresponding encryption key in key agreement phase, the interaction is not exist between a joining or leaving member and the off-line center after the member joins or leaves network, so a member participate in rekeying without the support from the off-line center. The PRKM scheme usually generates a key pool and distributes part of keys for every member from the pool based on symmetric cryptography, so the computation cost is zero whether a joining or leaving event. the joining or leaving member only broadcasts a joining or leaving message in rekeying, nevertheless the ownership of key from a leaving or joining member may not be determined accurately since a key is shared by a few of members and it is spread in a large scale network, the scale of rekeying is related to the scale

Table 1: Several typical schemes comparison in security aspect

Scheme	Key independence	Forward security	Backward security	Relationship	Collusion Attack	Cryptography
RPKM	No	No	No	1-to-1	YES	Symmetric Cryptography
IGKM	No	No	YES	1-to-1	YES	Bilinear Pairing
OMEDP	YES	YES	YES	1-to-n	YES	Threshold Cryptography
AGKA	YES	YES	YES	1-to-n	NO	Bilinear Pairing
AOGKM	YES	YES	YES	1-to-n	NO	Discrete Logarithm Algorithm
AKMSN	YES	YES	YES	1-to-n	NO	Discrete Logarithm Algorithm
OMKAP	YES	YES	YES	1-to-n	NO	Bilinear Pairing, Threshold Cryptography
NRLGKM	YES	YES	YES	1-to-n	YES	Bilinear Pairing, Threshold Cryptography
Suggested scheme	YES	YES	YES	1-to-n	NO	Discrete Logarithm Algorithm

of every member's keys and the distribution of those keys. In the IGKM scheme, every member conserves its identity and decryption key at cost of two units in storage cost at least, when a joining member joins network the off-line center generates its decryption key with a modular multiplication in bilinear pairing, however the scheme IGKM doesn't support rekeying in a leaving event due to all members cannot participate in rekeying to update the primary key generated by the off-line center to against the expose of decryption key. The scheme AGKA need implement itself again for rekeying, so every member perform a modular multiplication operation and a modular exponentiation operation, and send a message of key material, the total message cost is $n+1$ and $n-1$ for a joining or leaving event, a member keep its decryption key with 3 units, the cost of rekeying is related to the network scale. The scheme AOGKM is improved in basis of the scheme AKMSN with a tree structure, the message cost is not related to the network scale in a leaving event but the message cost is related to the network scale in a joining event, the message cost is reduced at price of raising computation cost. Those schemes OMEDP and NRLGKM are based on threshold cryptography (n,t), every member preserve threshold number of key fragments, the parameters x and y are produced by the schemes and their values are less than t,but their sum is more than t, an encryption key has x key fragments and a decryption key has y key fragments, so those values x and y decide the cost of rekeying. The scheme OMKAP is presented for target that two sub-groups merge into a new group or a group is divided into two groups at short time delay, but its computation cost is related to the two subgroups' scale n and m, the message cost is high in a joining event while the cost of leaving event is suitable in OMKAP, the storage cost of every member's key fragments is related to the network scale.

Our suggested scheme' message cost is not related to the network scale in rekeying, it implements key management in short time, the dependence of reliable end-to-end link is reduced and it computation cost is more suitable than other schemes, the off-line center issues a new public decryption key at cost of $n+2$ modulate modular exponentiation operations in joining event and n modulate modular exponentiation operations in leaving event, every member carries on two hash function operations to update the key matrix in joining event.

7 Conclusion

In this paper, a key independence group key management scheme is presented with discrete logarithm. Our proposed key management has the merit that an encryption key is corresponding to multiple decryption keys, thus those decryption keys meet key independence, so the binding relationship is released between decryption key and encryption key. Only the joining or leaving member must participate in rekeying, the message cost is not related to the network scale, other members keep their decryption keys legitimate. In security aspect, the suggested scheme guarantees the forward/backward security. In efficiency aspect, the message cost is less in rekeying and the dependence on reliable end-to-end link is reduced since the rekeying cost is not related to the networks scale. Therefore our suggested scheme is suitable for the non-reliable end-to-end link and long-time-delay networks.

Table 2: Comparison in efficiency

Scheme	Computation Cost		Message Cost		Network Overload		Storage Cost	Equipm.	Rekeying Scale
	Joining	Leaving	Joining	Leaving	Joining	Leaving			
RPKM	0	0	1	1	L	L	Part of Key Pool	Off-line Center	Part of Key Pool
IGKM	1	No	1	No	L	No	2	Off-line Center	n
OMEDP	x+(n+1)y	x+(n-1)y	n+1	n-1	(n+1)yL	(n-1)yL	n	Off-line Center	n
AGKA	Member:1	Member:1	n+1	n-1	(n+1)L	(n-1)L	3	No	n
AOGKM	2n-2	3n-lo_2n-4	log_2n	1	2(n-2)L	(N+2)L	(2n-1)L	Off-line Center	Joining Leaving
AKMSN	4n+7	4n-1	n+2	1	(n+2)L	L	n+2	Off-line Center	1
OMKAP	$n+m+\sum_{i=1}^{m}\sum_{i=1}^{m} C_n^{i-k}C_m^k + \sum_{i=m}^{n}\sum_{k=1}^{m} C_n^{i-k}C_m^k + \sum_{i=n}^{m+n}\sum_{k=1}^{m} C_n^{i-k}C_m^k - 1$	2^n	$(2^m +2^n +4)n$	0	1	0	2^n+2	Off-line Center	0
NRLGKM	x+(n+1)y	x+(n-1)y	0	0	0	0	n	Off-line Center	1
Suggested scheme	n+2	n	1	1	L	L	3n+3	Off-line Center	1

Acknowledgment

This work is supported by the National Science Foundation Project of P.R. China (No. 61402001),the University Natural Science Foundation of Anhui (KJ2020A0013,ACKY22002),Jian Zhou et al. are very grateful to the National Science Foundation of China (NSFC) for the support.

References

[1] N.-T. Zhang, H. Li, and Q.-Y. Zhang, "Thought and developing trend in deep space exploration and communication," *Journal of Astronautics*, vol. 28, no. 4, pp. 786–793, 2007.

[2] G. Xu and Z. Song, "Effects of solar scintillation on deep space communications: challenges and prediction techniques," *IEEE Wireless Communications*, vol. 26, no. 2, pp. 10–16, 2019.

[3] I. Bekmezci, O. K. Sahingoz, and Ş. Temel, "Flying ad-hoc networks (fanets): A survey," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1254–1270, 2013.

[4] D. H. Lyon, "A military perspective on small unmanned aerial vehicles," *IEEE Instrumentation & Measurement Magazine*, vol. 7, no. 3, pp. 27–31, 2004.

[5] R. Singh and G. Asutkar, "Survey on various wireless sensor network techniques for monitoring activities of wild animals," in *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*. IEEE, 2015, pp. 1–5.

[6] R. Mittal and M. S. Bhatia, "Wireless sensor networks for monitoring the environmental activities," in *2010 IEEE International Conference on Computational Intelligence and Computing Research*. IEEE, 2010, pp. 1–5.

[7] D. R. Jackson, D. Rouseff, W. L. Fox, C. D. Jones, J. A. Ritcey, and D. R. Dowling, "Underwater acoustic communication by passive phase conjugation: Theory and experiment," *The Journal of the Acoustical Society of America*, vol. 108, no. 5_Supplement, pp. 2607–2607, 2000.

[8] C. Kunz, C. Murphy, R. Camilli, H. Singh, J. Bailey, R. Eustice, M. Jakuba, K.-i. Nakamura, C. Roman, T. Sato *et al.*, "Deep sea underwater robotic exploration in the ice-covered arctic ocean with auvs," in *2008 IEEE/RSJ International Conference on Intelligent Robots and Systems*. IEEE, 2008, pp. 3654–3660.

[9] F. He, L. Yao, and Q. Liu, "Research of buddle protocol of deep space sensor network based on dtn," in *2012 Fourth International Conference on Multimedia Information Networking and Security*. IEEE, 2012, pp. 604–607.

[10] Q. Yu, X. Sun, R. Wang, Q. Zhang, J. Hu, and Z. Wei, "The effect of dtn custody transfer in deep-space communications," *IEEE Wireless Communications*, vol. 20, no. 5, pp. 169–176, 2013.

[11] D. W. Dunham, R. W. Farquhar, N. Eismont, and E. Chumachenko, "New approaches for human deep-space exploration," *The Journal of the astronautical sciences*, vol. 60, pp. 149–166, 2013.

[12] O. K. Sahingoz, "Networking models in flying ad-hoc networks (fanets): Concepts and challenges," *Journal of Intelligent & Robotic Systems*, vol. 74, pp. 513–527, 2014.

[13] R. J. Cesarone, D. S. Abraham, and L. J. Deutsch, "Prospects for a next-generation deep-space network," *Proceedings of the IEEE*, vol. 95, no. 10, pp. 1902–1915, 2007.

[14] A. C. Singer, J. K. Nelson, and S. S. Kozat, "Signal processing for underwater acoustic communications," *IEEE Communications Magazine*, vol. 47, no. 1, pp. 90–96, 2009.

[15] S. Jiang, "On securing underwater acoustic networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 729–752, 2018.

[16] M. G. Rubinstein, I. M. Moraes, M. E. M. Campista, L. H. M. Costa, and O. C. M. Duarte, "A survey on wireless ad hoc networks," in *IFIP International Conference on Mobile and Wireless Communication Networks*. Springer, 2006, pp. 1–33.

[17] H. Harney and C. Muckenhirn, "Rfc2093: Group key management protocol (gkmp) specification," 1997.

[18] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *IEEE wireless communications*, vol. 11, no. 1, pp. 38–47, 2004.

[19] A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, and P. Spilling, "A survey of key management in ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 3, pp. 48–66, 2006.

[20] I. Ingemarsson, D. Tang, and C. Wong, "A conference key distribution system," *IEEE Transactions on Information theory*, vol. 28, no. 5, pp. 714–720, 1982.

[21] R. Dutta and R. Barua, "Overview of key agreement protocols," *Cryptology ePrint Archive*, 2005.

[22] J. Zhou, M. Song, J. Song, X.-w. Zhou, and L. Sun, "Autonomic group key management in deep space dtn," *Wireless personal communications*, vol. 77, pp. 269–287, 2014.

[23] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 41–47.

[24] J. Hwang and Y. Kim, "Revisiting random key predistribution schemes for wireless sensor networks," in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, 2004, pp. 43–52.

[25] M. Kendall and K. M. Martin, "Graph-theoretic design and analysis of key predistribution schemes," *Designs, Codes and Cryptography*, vol. 81, pp. 11–34, 2016.

[26] M. Klonowski and P. Syga, "Enhancing privacy for ad hoc systems with predeployment key distribution," *Ad Hoc Networks*, vol. 59, pp. 35–47, 2017.

[27] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology: Proceedings of CRYPTO 84 4*. Springer, 1985, pp. 47–53.

[28] H. Tanaka, "A realization scheme for the identity-based cryptosystem," *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, vol. 73, no. 5, pp. 1–7, 1990.

[29] M. Gupta, "Group key exchange management in delay tolerant network," *Int. J. Comput. Appl*, vol. 144, pp. 16–19, 2016.

[30] K. Kurosawa, "Multi-recipient public-key encryption with shortened ciphertext," in *Public Key Cryptography: 5th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2002 Paris, France, February 12–14, 2002 Proceedings 5*. Springer, 2002, pp. 48–63.

[31] A. A. Kamal, "Cryptanalysis of a polynomial-based key management scheme for secure group communication." *Int. J. Netw. Secur.*, vol. 15, no. 1, pp. 68–70, 2013.

[32] G.-H. Chiou and W.-T. Chen, "Secure broadcasting using the secure lock," *IEEE Transactions on Software Engineering*, vol. 15, no. 8, pp. 929–934, 1989.

[33] J. Liao, X. Hui, Q. Qing, L. Yi, and M. Yu, "A public key encryption scheme with one-encryption and multi-decryption," *Chinese Journal of Computers*, vol. 35, no. 5, pp. 1059–1067, 2012.

[34] Q. Wu, Y. Mu, W. Susilo, B. Qin, and J. Domingo-Ferrer, "Asymmetric group key agreement," in *Advances in Cryptology-EUROCRYPT 2009: 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings 28*. Springer, 2009, pp. 153–170.

[35] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, and Ú. González-Nicolás, "Asymmetric group key agreement protocol for open networks and its application to broadcast encryption," *Computer Networks*, vol. 55, no. 15, pp. 3246–3255, 2011.

[36] J. Zhou and X.-w. Zhou, "Autonomous shared key management scheme for space networks," *Wireless personal communications*, vol. 72, no. 4, pp. 2425–2443, 2013.

[37] J. Zhou, L. Sun, X. Zhou, and J. Song, "High performance group merging/splitting scheme for group key management," *Wireless personal communications*, vol. 75, pp. 1529–1545, 2014.

[38] J. Zhou, L. Sun, and J. Song, "Efficient group key management for non-reliable link networks," *Wireless Personal Communications*, vol. 98, pp. 1955–1973, 2018.

Biography

Jian Zhou, born in 1979. He is a post-doctoral researcher at Beijing University of Post and Telecommunications, and an professor and M.S. supervisor at Anhui University of Finance and Economics. His research interests

include key management, security and privacy of mobile systems, cognitive radio networks and secure protocol design in wireless networks, etc.

Liyan Sun,born in 1976. She received M.S. degree in Compute Application from the University of Inter Mongolia University, P. R. China in 2005. At present, she is associate professor in Anhui University of Finance and Economics. Her research interests include key management, security and privacy of mobile systems, ad hoc networks and secure protocol design in wireless networks.

Shi-hua Huang, born in 1999, master's degree, her main research directions are data mining, business intelligence, etc.

Security Encryption Analysis of Economic Big Data Based on Homomorphic Encryption and Attribute Base

Limin Chen

(Corresponding author: Limin Chen)

School of Finance and Economics, Zhengzhou University of Science and Technology
Zhengzhou 450064, China
Email: chenwwencww@163.com

(Received July 15, 2023; Revised and Accepted Jan. 17, 2024; First Online Feb. 23, 2024)

The Special Issue on Data Fusion, Deep Learning and Optimization Algorithms for Data Privacy Protection

Special Editor: Prof. Shoulin Yin (Harbin Institute of Technology)

Abstract

Traditional data encryption technology neglects the secondary deletion of cloud data, leading to serious redundancy of economic big data, and poor ability to resist various attacks. Therefore, in this paper, we propose a novel security encryption model based on homomorphic encryption and attribute base for economic big data. Fourier transform high-order cumulant algorithm is used to detect the duplicate data in cloud storage economy big data, and a 4-order cumulant post-processing method is selected to delete the duplicate data in the detection results. The homomorphic encryption combined with attribute-based encryption technology is used to construct an encryption scheme to complete the encryption of economy big data in cloud storage. Through theoretical analysis and experimental simulation, it is proved that the new scheme can support the access policy with rich expression ability, realize the dynamic policy update for the data in the cloud, and has advantages in storage and computing cost.

Keywords: 4-order Cumulant Post-processing Method; Attribute Base; Economic Big Data Encryption; Homomorphic Encryption

1 Introduction

At present, cloud computing services are gradually applied to various fields, and with the continuous expansion of cloud computing fields, corresponding cloud storage services appear [19]. At present, the amount of data to be stored is increasing in many fields [9], and the cloud storage mode capable of storing massive data is gradually attracting attention. Users can access the data in the cloud storage system through various forms at will. However, data loss and other phenomena may occur during the cloud storage process, and users can encrypt their own data. A layer of security service [21,23,25] is provided for data and then placed in the cloud storage server, but this method cannot fully guarantee the security of cloud storage data.

Cloud computing, the Internet of Things and the traditional industrial control system (ICS) integration, forming the industrial cloud system [11]. It connects products, factories, systems, machines, and users, and provides advanced analytics to harness the vast amounts of data generated in the network for efficiency gains and cost reductions. For a long time, enterprises pay more attention to production security and equipment security, but do not pay attention to information security and network security. This is because traditional ICS systems are proprietary, independent, and isolated from external networks [14]. In order to meet the requirements of continuous and stable production, industrial communication protocols pay more attention to the requirements of real-time, and lack the security protection of transmitted data to avoid additional costs. However, in the industrial cloud environment, the user identity is complex and diverse, and enterprises are faced with various dangers from various sources, especially the logic executed in the industrial system has a direct impact on the physical world, and the maliciously attacked system will cause serious damage and loss to human health and safety, the environment and equipment, that is, information security problems will lead to production security problems [18]. In addition, the public cloud is a semi-trusted environment, and after hosting data into a cloud storage system, enterprises cannot be sure that the storage of data is indeed protected. Therefore, it is necessary to study the confidentiality protection method in the process of data transmission, storage and sharing in the industrial cloud environment, and meet the real-time and availability requirements of indus-

trial production control.

For this reason, many scholars have studied data encryption. For example, Andola *et al.* [1] designed an encryption scheme for large data sets. For users with large data sets in the cloud storage environment, the block storage structure was used to optimize the data structure of the security index. Deng *et al.* [4] proposed a data encryption scheme capable of updating user attributes. By constructing attribute and user version key in ciphertext policy attribute encryption, the attribute version key needed to be updated when system attribute was revoked to realize the replaceable update of some components of ciphertext key. However, the encryption time of the above encryption methods is too long, and the ability to resist data attacks is weak.

In order to avoid industrial data leakage, reference [12] adopted RSA and DES encryption algorithms to prevent data from being eavesdropped during transmission and protect the security of data communication, aiming at the security of data collection in smart power plants. Aiming at the problem of secure data transmission between iot devices, reference [13] used chaotic mapping to generate AES keys and encrypt communication data, thus building a secure communication channel. In reference [26], the Paillier homomorphic encryption method was adopted to realize the secure data transmission between the field device and the controller. However, a large number of encryption and decryption operations are deployed on field sensors or actuators, which increases the computing overhead of field devices and puts forward higher requirements on network throughput. It can be seen that for ICS system, symmetric encryption scheme has low computation cost and good real-time performance, but how to manage its key is a problem that must be considered. Asymmetric encryption scheme is more secure, but the calculation cost is high, which affects the actual use. In addition, in the actual industrial cloud environment, there are many users with diverse identities, and how to ensure that users get the data within the scope of their authority and achieve fine-grained access control is also an urgent problem to be solved.

Attribute based encryption (ABE) is one of the methods for data protection and access control in cloud environment. Ciphertext-policy attribute-based encryption (CPABE) encrypts data according to the access policy and distributes the corresponding private key according to the user attributes [17]. Only the user attributes meet the requirements of the access policy. This is conceptually similar to traditional access control models such as role-based access control. Therefore, researchers are also applying CP-ABE to the industrial field to achieve data confidentiality protection and access control. References [6, 24] used CP-ABE to encrypt data and authenticate users for smart grid, medical cloud and intelligent transportation systems respectively, and only users who met the access policies in ciphertext could obtain plaintext.

Therefore, this paper studies econom big data encryption technology that supports complete outsourcing of cloud storagey. Through the improved fractional Fourier transform, duplicate data in cloud storage data was deleted to reduce the burden of data outsourcing encryption. Then, the data was outsourced to cloud storage server for attribute base and homomorphic encryption through the encryption form of complete outsourcing to the server, so as to realize data encryption and save the time of data encryption.

2 Proposed Encryption Technology

2.1 Attribute Base Encryption

When constructing the cloud storage data encryption scheme in this paper, the CP-ABE scheme under the prime-order group is taken as the basis of this research, and the theory of traditional outsourcing encryption algorithm is combined to study the verifiable fully outsourced attribute-based encryption scheme [2,5,7]. In this scheme, the following algorithms are mainly included.

1) $Setup(U) \rightarrow (pk, msk)$: The algorithm is started by AA, set the attribute set U composed of the output Y_k^M of eliminating duplicate data as the input, select the multiplicative cyclic group G, and the order of G is prime p. Let one of the generators of G be g, and randomly select $h_1, \cdots, h_U \in G$, and the exponent $a, a \in Z_p$, from which the public parameters can be obtained and expressed by Formula (1).

$$pk = (g, g^a, e(g,g)^a, h_1, \cdots, h_U). \tag{1}$$

Set $msk = g^a$ as the primary key of the cloud storage system. Where h is a random selection index. $e(g,g)$ represents the unit of G. a indicates a randomly selected integer. Z stands for bilinear set.

2) $KeyGen_{KG-CSP}(pk, S) \rightarrow (ISK_1, ISK_2)$: The algorithm is generated by two $KG - CSP$. The input of the algorithm is all attribute set S and public parameter pk. If $KG - CSP1$ starts to execute, it is necessary to select random numbers $a_1, t_1 \in Z_p$, and calculate $K' = g^{a_1} g^{at_1}$, $L' = g^{t_1}$, $\forall x \in S, K'_x = h_x^{t_1}$ to obtain the intermediate key $ISK_1 = (S, a_1, K', L', K'_{x x \in S})$ of $KG - CSP1$, the intermediate key $ISK_2 = (S, a_2, K'', L'', K''_{x x \in S})$ of $KG - CSP2$ can be obtained at the same time.

3) $KeyGen_{AA}(pk, msk, ISK_1, ISK_2) \rightarrow SK$: The algorithm is started by AA, and the inputs are set as public parameter pk, system main key msk, and intermediate key ISK_1, ISK_2. The following formulas are calculated.

$$K_1 = K' \times K'' = g^{a'} g^{at}. \tag{2}$$

$$L = L' \times L'' = g^t. \tag{3}$$

$$K_x = K'_x \times K''_x = h^t_x. \quad (4)$$

Here, $a' = a_1 + a_2$, $t = t_1 + t_2$. After calculation, the user key $SK = (S, K_1, L, K_{xx\in S}, K_2)$ is obtained, and $K_2 = g^{a-a'}$, where SK represents the user key.

4) $Encrypt(pk, msk, (M, \rho), m) \to CT$: The algorithm is executed interactively by DO and $E - CSP$. Within the access structure (M, ρ), DO encrypts the message m. Where M represents the matrix of the size of $l \times n$, and the mapping associated with each row of matrix M to the attribute is the function ρ, and ρ is the injective form. DO can randomly select the secret index $s \in Z_p$, and select the random vector $v = (s, v_2, \cdots, v_n)^T$ to make the sharing of the encryption index s more perfect. $\lambda_i = M_i v$ is calculated, where the $i - th$ row of matrix M is described by M_i; After that, DO performs operations on ciphertext $CT = ((M, \rho), C, \bar{C}, C_{ii\in[1,l]})$, in which $C = m \cdot e(g, g)^{as}, \bar{C} = g^s$. And Do algorithm for local calculation, can know $C_i = g^{a\lambda_i} h^{-s} \rho(i)$, after E-CSP cooperation calculation, can obtain C_i calculation process can be expressed by Formula (5).

$$Exp(\lambda_i, -s; g^a, h_{\rho(i)}) \to g^{a\lambda_i} h^{-s} \rho(i). \quad (5)$$

In Formula (5), λ represents the security parameter, CT represents the ciphertext, and C represents the encryption attribute.

Perform $Rand$ algorithm through DO to obtain random values (γ_1, g^{γ_1}), (γ_2, g^{γ_2}), (β, g^{β}), (a_1, g^{a_1}), (a_2, g^{a_2}), (a_3, g^{a_3}); $g^{a\lambda_i} h^{-s} \rho(i)$ is then disassembled into Formula (6).

$$g^{a\lambda_i} h^{-s} \rho(i) = g^{\gamma_1 \lambda_i - \gamma_2 s} \varpi_1^{\lambda_i} \varpi_i^{-s}. \quad (6)$$

In Formula (6), ϖ represents the outsourcing query index and γ represents the outsourcing decryption random value.

In order to ensure that the associated information will not be lost during $\varpi_1^{\lambda_i} \varpi_i^{-s}$ query, $\varpi_1^{\lambda_i} \varpi_i^{-s}$ will continue to be split and expressed by Formula (7).

$$\varpi_1^{\lambda_i} \varpi_i^{-s} = \varpi_1^{c_1,i}, \varpi_i^{c_2,i} (\varpi_1 \varpi_i^{-1})^{d_i x}. \quad (7)$$

Where d is a prime number, after the splitting is completed, the random value g^{β} is used to continue the next step of the splitting, and is expressed by Formula (8).

$$g^{a\lambda_i} h^{-s} \rho(i) = g^{\beta} g^{a_1 \zeta_1} \varpi_1^{c_1,i} \varpi_1^{c_2,i} (\varpi_1 \varpi_i^{-1})^{d_i x}. \quad (8)$$

Where $\varpi_1 = g^a / g^{\gamma_1}$, $\varpi_i = h_{\rho(i)} / g^{\gamma_2}$, $c_{1,i} = \lambda_i - d_i x$, $c_{2,i} = -s + d_i x$, $\zeta_i = (\gamma_1 \lambda_i - \gamma_2 s - \beta)$, and select $\eta_i = (a_3 - a_1 \zeta_i)/a_2$ for the next step, where β represents the random value and ζ and η represent the association information after splitting.

5) $Audit(CT^{RK}_{part}, \bar{C}, msk) \to 0/1$: The validation process is initiated by the AA authority. The algorithm input is the user decrypted value CT^{RK}_{part}, the system master key msk and the ciphertext $\bar{C}$. Analyze the size of $e(msk, \bar{C})$ and CT^{RK}_{part}, if they are equal, output "1"; If not, output "0".

2.2 Homomorphic Encryption

Assuming that the model parameter matrix of the $u - th$ $(1 \le u \le n)$ data owner is W_u, the scheme in this paper uses the Paillier algorithm to encrypt the model parameter matrix and perform homomorphism operations [3, 10, 15, 22, 27].

1) Generate public and private key pairs for encryption. First, two large prime numbers p and q are randomly selected. Note that p and q must be equal in length, and pq, $(p-1)$, $(q-1)$ are mutual primes. Second, calculate $r = pq$ and $\lambda = lcm(p-1, q-1)$, where, lcm represents the least common multiple, let $g = r + 1$. Third, let the function $L(x) = (x-1)/r$, then calculate $\mu = (L(g^{\lambda} mod(r^2)))^{-1}$. At this point, it can get the public key (r, q) and the private key (λ, μ).

2) Encrypt W_u and calculate the model parameter ciphertext c_u of the $u - th$ $(1 \le u \le n)$ data owner. First, select the random number s, where s must meet the condition $0 \le s < r$; Second, let the plaintext information corresponding to c_u be m_u, and calculate the ciphertext information $c_u = (g^{m_u} s^r) mod(r^2)$. Since $g = r + 1$, then

$$g^{m_u} = m_u r + 1 mod(r^2). \quad (9)$$

3) According to step 1 and step 2, n data owner model parameter ciphertext can be obtained, that is, $c_1, c_2, \cdots, c_n$, and the model parameter ciphertext c of the joint model computer can be obtained by performing operations in the ciphertext field, where $c = c_1 c_2 \cdots c_n$.

The joint model computer obtains the ciphertext c of the model parameter calculated in the encryption domain and decrypts it. When the ciphertext is c, $d(c)$ indicates that the ciphertext c is decrypted, that is, $d(c) = m_c$. Then the plaintext can be obtained according to Formula (6):

$$d(c) = m_c = L(c^{\lambda} mod r^2) \mu mod r. \quad (10)$$

In this paper, the homomorphism of Paillier algorithm is used to prove the feasibility of the proposed scheme. As shown in Formula (11):

$$d(c) = m_1 + m_2 + \cdots + m_n. \quad (11)$$

Table 1: Comparison of storage overhead

Method	Encryption key	Decryption key	Ciphertext of the client
HEMA	$2\|g\| + \|K_a\|$	$2\|S\|\|G\| + \|K_a\|$	$2\|G\|$
AAHE	$4\|G\| + \|K_a\|$	$(2\|S\| + 6)\|G\| + \|K_a\|$	$2\|G\| + \|Z_p\|$
HEB	$4\|U\|\|G\| + \|K_a\|$	$(2\|S\| + 3)\|G\| + \|K_a\|$	$2\|G\| + \|K_a\|$
Proposed	$\|K_a\|$	$\|Z_p\| + \|K_a\|$	$2\|G\|$

Table 2: Comparison of computing overhead

Method	Device encryption cost	Client decryption overhead
HEMA	$(2\|I\| + 1)(exp + exp_T) + \|HE\|$	$exp_T + \|HE\|\|$
AAHE	$exp_T + \|HE\|$	$exp_T + \|HE\|$
HEB	$3exp + 2exp_T + \|HE\|$	$2exp_T + e + \|HE\|$
Proposed	$\|HE\|$	$exp_T + \|HE\|$

3 Scheme Analysis

The scheme adopts a hybrid encryption method, that is, the homomorphic encryption algorithm (HE) is combined with the attribute-based algorithm (AB). The plaintext data is encrypted by HE algorithm first, and then the symmetric key K_a is encrypted by AB algorithm. Therefore, the security of symmetric key K_a determines the confidentiality of plaintext data. In this scheme, the data owner divides K_a into two sub-keys and sends them to two different fog nodes respectively. Each fog node encrypts AB algorithm independently, so each fog node does not know the symmetric key K_a of the data owner. Based on the fact that there is no collusion between different fog nodes, the fog node cannot obtain the symmetric key K_a. In addition, the symmetric key is generated by Logistic mapping in this scheme, and the key is updated after each communication between the field device and the user. Therefore, a symmetric key is only applicable to the one-time communication between the two parties. Based on the chaos of Logistic mapping, even if the attacker successfully cracks the symmetric key of a certain communication, Nor can all other keys be cracked with a non-negligible probability. In the decryption phase, the secret value s can be recovered only when the user attribute set meets the access policy, and the converted ciphertext $e(g,g)^{\frac{\alpha s}{z}}$ can be successfully decrypted. Otherwise, the decryption will be failed.

In the access policy update phase, although this part of the calculation is outsourced to the cloud, the cloud only has its selected secret value $\tilde{s}$, not the secret value s of the original file, so it cannot calculate the new secret value s' by $s' = \tilde{s} + s$. The new secret value s' is obtained by the exponential operation on the group and is hidden in the component $K_a e(g,g)^{a^{s'}}$. Because of the difficulty of calculating the discrete logarithm problem, the attacker cannot calculate s' according to the inverse operation, so the symmetric key K_a is secure.

This section compares this scheme with schemes HEMA [16], AAHE [20], and HEB [8] in terms of storage overhead and computing overhead to evaluate the performance of the scheme. The storage costs required by different schemes on the device and the client are compared, and the results are listed in Table 1. Where, $|G|$, $|G_T|$ and $|Z_p|$ represent the length of each element in G, G_T and Z_p respectively. In the symmetric bilinear pair construction, we have $|G| = |G_T|$, $|U|$ represents the number of all attributes, $|S|$ represents the number of user attributes, $|l|$ represents the number of attributes contained in the access structure, m represents the maximum number of users, and $|K_a|$ represents the length of the symmetry density.

In Table 1, the storage overhead on the device side comes primarily from encryption keys. The encryption keys of HEMA, AAHE, and HEB are composed of public key PK and symmetric key K_a, and this scheme outsources the encryption calculation of HE to the cloud and fog, so the device side of this scheme only needs to store symmetric key K_a, and the storage cost is much lower than the other three schemes.

The calculation costs of different schemes on the device and the client are compared, and the results are listed in Table 2. Let $|I|$ represent the number of user attributes matching the access policy, exp, exp_T represent the exponential operation on the group G, G_T. e represents the bilinear pair operation, and $|HE|$ represents the homomorphic encryption operation.

In the encryption process, this scheme completely outsources the encryption operation of the HE part to the cloud node [8], and only needs to perform homomorphic encryption operation on the device side, while other schemes need to complete HE and AB encryption on the device side. Therefore, the encryption cost of this scheme is small, and it is suitable for devices with limited re-

sources.

4 Conclusion

This paper studies the economy big data encryption technology of cloud storage that supports complete outsourcing, and provides perfect data for cloud storage data encryption through data deduplication algorithm. According to data homomorphic encryption technology, a data encryption scheme is constructed to realize the encryption of cloud storage data. Simulation is used to verify the effectiveness of the proposed technology, and it is proved that the encryption time and anti-attack performance of the technology are higher than other technologies.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] N. Andola, S. Prakash, V. K. Yadav, S. Venkatesan, et al, "A secure searchable encryption scheme for cloud using hash-based indexing," *Journal of Computer and System Sciences*, vol. 126, pp. 119-137, 2022.

[2] Z. Cao and O. Markowitch, "Comment on "Circuit Ciphertext-Policy Attribute-Based Hybrid Encryption With Verifiable Delegation in Cloud Computing"," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 2, pp. 392-393, 2021.

[3] S. Das, S. Namasudra, "MACPABE: Multi-Authority-based CP-ABE with efficient attribute revocation for IoT-enabled healthcare infrastructure," *International Journal of Network Management*, vol. 33, no. 3, pp. e2200, 2023.

[4] S. Deng, G. Yang, W. Dong, *et al.* "Flexible revocation in ciphertext-policy attribute-based encryption with verifiable ciphertext delegation," *Multimedia Tools and Applications*, vol. 82, no. 14, pp. 22251-22274, 2023.

[5] J. Gao, H. Yu, X. Zhu and X. Li, "Blockchain-Based Digital Rights Management Scheme via Multiauthority Ciphertext-Policy Attribute-Based Encryption and Proxy Re-Encryption," *IEEE Systems Journal*, vol. 15, no. 4, pp. 5233-5244, 2021.

[6] S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, X. Tang, "EFR-CSTP: Encryption for face recognition based on the chaos and semi-tensor product theory," *Information Sciences*, vol. 621, pp. 766-781, 2023.

[7] B. Ghosh, P. Parimi and R. R. Rout, "Improved Attribute-Based Encryption Scheme in Fog Computing Environment for Healthcare Systems," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India*, pp. 1-6, 2020, doi: 10.1109/ICCCNT49239.2020.9225606.

[8] D. Han, J. Chen, L. Zhang, Y. Shen, X. Wang and Y. Gao, "Access control of blockchain based on dual-policy attribute-based encryption," in *2020 IEEE 22nd International Conference on High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Yanuca Island, Cuvu, Fiji*, pp. 1282-1290, 2020, doi: 10.1109/HPCC-SmartCity-DSS50907.2020.00200.

[9] J. Hasenburg, M. Grambow and D. Bermbach, "MockFog 2.0: Automated Execution of Fog Application Experiments in the Cloud," *IEEE Transactions on Cloud Computing*, vol. 11, no. 1, pp. 58-70, 2023.

[10] J. Kim and A. Yun, "Secure Fully Homomorphic Authenticated Encryption," *IEEE Access*, vol. 9, pp. 107279-107297, 2021.

[11] S. Maesschalck, V. Giotsas, B. Green, N. Race, "Don't get stung, cover your ICS in honey: How do honeypots fit within industrial control system security," *Computers & Security*, vol. 114, pp. 102598, 2022.

[12] D. O. Orucho, F. M. Awuor, R. Makiya, C. Oduor, "Review of Algorithms for Securing Data Transmission in Mobile Banking," *Modern Economy*, vol. 14, no. 9, pp. 1192-1217, 2023.

[13] Z. Rahman, X. Yi, M. Billah, M. Sumi, A. Anwar, "Enhancing AES using chaos and logistic map-based key generation technique for securing IoT-based smart home," *Electronics*, vol. 11, no. 7, pp. 1083, 2023.

[14] Y. Su, M. Zhao, C. Wei, X. Chen, "PT-TODIM method for probabilistic linguistic MAGDM and application to industrial control system security supplier selection," *International Journal of Fuzzy Systems*, pp. 1-14, 2022.

[15] L. Teng, H. Li, J. Liu, S. Yin, "An efficient and secure cipher-text retrieval scheme based on mixed homomorphic encryption and multi-attribute sorting method under cloud environment," *International Journal of Network Security*, vol. 20, no. 5, pp. 872-878, 2018.

[16] R. Thenmozhi, S. Shridevi, S. N. Mohanty, V. Garcìa-Dìaz, D. Gupta, P. Tiwari, M. Shorfuzzaman, "Attribute-based adaptive homomorphic encryption for big data security," *Big Data*, 2021. ahead of print, http://doi.org/10.1089/big.2021.0176

[17] H. Wang, J. Liang, Y. Ding, S. Tang, Y. Wang, "Ciphertext-policy attribute-based encryption supporting policy-hiding and cloud auditing in smart health," *Computer Standards & Interfaces*, vol. 84, pp. 103696, 2023.

[18] X. Wang, Y. Sun, D. Ding, "Adaptive dynamic programming for networked control systems under communication constraints: a survey of trends and tech-

niques," *International Journal of Network Dynamics and Intelligence*, pp. 85-98, 2022.

[19] C. Wu, A. N. Toosi, R. Buyya and K. Ramamohanarao, "Hedonic Pricing of Cloud Computing Services," *IEEE Transactions on Cloud Computing*, vol. 9, no. 1, pp. 182-196, 2021.

[20] Z. Xu, S. Cao, "Multi-Source Data Privacy ProtectionMethod Based on Homomorphic Encryption and Blockchain," *CMES-Computer Modeling in Engineering & Sciences*, vol. 136, no. 1, 2023.

[21] M. M. Yang, I. Tjuawinata, K. Y. Lam, "K-Means Clustering With Local d_x-Privacy for Privacy-Preserving Data Analysis," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2524-2537, 2022.

[22] X. Yang, S. Zheng, T. Zhou, Y. Liu and X. Che, "Optimized relinearization algorithm of the multikey homomorphic encryption scheme," *Tsinghua Science and Technology*, vol. 27, no. 3, pp. 642-652, 2022.

[23] S. Yin, H. Li, S. Karim, and Y. Sun, "ECID: Elliptic Curve Identity-based Blind Signature Scheme," *International Journal of Network Security*, vol. 23, no. 1, pp. 9-13, 2021.

[24] S. Yin, H. Li, L. Teng, A. A. Laghari, V. V. Estrela, "Attribute-based Multiparty Searchable encryption model for Privacy Protection of Text Data," *Multimedia Tools and Applications*, 2023. ttps://doi.org/10.1007/s11042-023-16818-4.

[25] S. Yin, J. Liu and L. Teng, "Improved Elliptic Curve Cryptography with Homomorphic Encryption for Medical Image Encryption," *International Journal of Network Security*, vol. 22, no. 3, pp. 419-424, 2020.

[26] Z. P. Yuan, P. Li, Z. -L. Li, J. Xia, "A Fully Distributed Privacy-Preserving Energy Management System for Networked Microgrid Cluster Based on Homomorphic Encryption," *IEEE Transactions on Smart Grid*, 2023. doi: 10.1109/TSG.2023.3309405.

[27] C. Zhou and N. Ansari, "Securing Federated Learning Enabled NWDAF Architecture with Partial Homomorphic Encryption," *IEEE Networking Letters*, 2023. doi: 10.1109/LNET.2023.3294497.

Biography

Limin Chen biography. Limin Chen is with School of Finance and Economics, Zhengzhou University of Science and Technology, Zhengzhou City, Henan Province, 450064, China. Her research interests are economic data security and business management.

Research on Information Dissemination Security Based on Generative Adversarial Network in Internet of Vehicle Environment

Junting Zhang

(Corresponding author: Junting Zhang)

School of Automobile, Henan College of transportation

Zhengzhou 450000 China

Email: byoungholee@qq.com

(Received July 20, 2023; Revised and Accepted Jan. 17, 2024; First Online Feb. 23, 2024)

The Special Issue on Data Fusion, Deep Learning and Optimization Algorithms for Data Privacy Protection

Special Editor: Prof. Shoulin Yin (Harbin Institute of Technology)

Abstract

Information security transmission is very important in the Internet of Vehicles. In the traditional methods, the remote node storage operation is not cooperative. In addition, the data block with low service evaluation is not effectively processed, and the duplicate redundancy is persistent, resulting in increased bandwidth pressure. Hence, we propose an information dissemination security model based on a generative adversarial network in the Internet vehicle environment. The data is enhanced with generative adversarial networks. Based on the enhanced data, practical features can be extracted to analyze the transmitted data effectively. Experimental results show that the proposed method enhances system security, information transmission security, and network performance compared with other methods.

Keywords: Data Enhancement; Generative Adversarial Network; Information Dissemination Security; Internet of Vehicle

1 Introduction

CACC (cooperative adaptive cruise control) [18,20] based on Internet of vehicle (IoV) means that the vehicle equipped with adaptive cruise control system uses mobile wireless communication technology such as DSRC (dedicated short range communications) [1, 14] to exchange information with roads, people and cloud to solve practical problems such as traffic accidents and traffic congestion. However, with the application and deployment of IoV and vehicle-road collaboration technologies, due to the openness of mobile communication and application information [7, 15, 21], they not only meet the requirements of vehicle information interaction, but also provide opportunities for virus intrusion. The intrusion of malicious code can be accompanied by the transmission of information between CACC vehicles, which can steal user privacy or interfere with the normal running of vehicles, resulting in serious security threats.

At present, the classical method to analyze the information transmission in the environment of IoV is to use simulation method. Yao *et al.* [22] reviewed the simulation methods in detail and analyzed the nonlinear relationship between traffic flow, information flow and vehicle-vehicle communication events. Based on the existing micro-traffic simulation model, Gupta *et al.* [8] built an information transmission simulation framework in the environment of the IoV and simulated the information transmission between vehicles on the expressway. In references [4,13,16], traffic flow was simplified as static traffic flow, and by analyzing the statistical distribution of traffic parameters, the constraints faced by information flow propagation were discussed. However, these simulation methods lack strict theoretical model support. Zhou *et al.* [24] considered communication constraints, analyzed the relationship between information propagation and traffic flow mechanics, established an information flow propagation model, and described the dynamic behavior of information flow propagation. Du *et al.* [6] divided the road into multiple cell units and constructed an information-coupled cell transport model (IT-CTM) to capture the flow of information within and between cells. Adaptive CruiseControl (ACC) is a widely used driver assistance system, and it is also the first step to realize automatic driving. ACC technology mainly collects the distance between the vehicle and the forward vehicle through on-board sensors such as radar, and automatically adjusts the speed of the vehicle to maintain a reasonable safety distance with the front vehicle. Collaborative adaptive cruise control technology is the sec-

ond step to realize autonomous driving, which means that vehicles equipped with adaptive cruise control system realize vehicle-to-vehicle interconnection communication through vehicle-to-vehicle networking technology. That is, the vehicle can not only sense the environment ahead through radar sensors, but also obtain information between the vehicle in front and other vehicles through wireless communication technologies such as DSRC, so that the connected vehicles can cooperate to complete the control and manipulation. Compared with ACC, CACC technology enables vehicles to obtain more information about surrounding vehicles, such as speed, acceleration, etc., and can react in real time according to the running status of other vehicles. Therefore, it can shorten the safety distance between vehicles, reduce the speed fluctuation of the road fleet, improve the operating efficiency of road traffic flow, reduce the incidence of road traffic accidents, and improve the driving comfort.

To sum up, most of the studies conducted by experts and scholars on the information dissemination of the Internet of vehicles aimed at the well-intentioned information, without considering the intrusion of malicious virus information. In addition, most of the current information dissemination models do not consider the interaction between different types of traffic flows. Based on this, aiming at the realistic road traffic environment in which CACC vehicles and ordinary vehicles are driving together, this paper constructs a dynamic model of virus transmission in the vehicle-connected environment, aiming to provide a theoretical basis for studying the virus transmission law in the vehicle-connected environment, and provide an effective method for suppressing the transmission of virus information, so as to ensure the safety of CACC vehicle information transmission.

2 Proposed Information Dissemination Security Model

Generative adversarial network (GAN) is a generative model based on zero-sum game idea [12, 19], which has been applied in many fields such as image generation, traffic sign recognition and traffic accident detection. GAN is mainly composed of generator and discriminator. The main function of the generator is to learn the distribution of real data, and the discriminator determines whether the data is real data or the data generated by the generator based on the input data. According to the discriminant results, the generator G and discriminator D continue to optimize and finally reach a Nash equilibrium, that is, the discriminator D cannot determine whether the input data is real or generated data.

The objective function of GAN optimization process is:

$$min_G max_D L(G,D) = A + B. \tag{1}$$

Where $A = E_{x-P_{data(x)}} log(D(x))$, $B = E_{z-P_{z(z)}} log(1-D(G(z)))$, E is the mathematical expectation of the distribution specified in the subscript. $P_{data(x)}$ is the distribution of the real data x. $P_{z(z)}$ is the distribution of generated data. $D(x)$ is the discriminant function of the discriminator. $G(z)$ is the data generated by the generator.

In this paper, both the generator and discriminator of GAN are fully connected neural networks, and the active function is the rectified linear unit (ReLU) [3,9] function, which can effectively alleviate the gradient disappearance problem. The generator and discriminator are optimized using the Adam optimizer [11], which has the advantages of high computational efficiency and is suitable for unstable objective functions.

The learning rate of generator and discriminator is set to 0.01, and the number of neurons in the hidden layer of generator and discriminator is set to 128. After 10^4 rounds of iterative training, GAN extended data set containing 8058 on-board data and 12060 normal operation data is obtained. In order to test the performance of the GAN proposed in this paper, a normalization method is used to process the extended and original GAN data sets to eliminate the dimensional effects and facilitate the comparison of data distribution between the two types of data sets. The normalization processing formula is as follows:

$$y_i = \frac{x_i - \min\limits_{1\le j\le n}}{\max\limits_{1\le j\le n} - \min\limits_{1\le j\le n}} \tag{2}$$

Where, x_i and y_i are the data before and after normalization processing respectively.

In order to analyze the communication probability of CACC vehicles, this paper first automatically divides the road into several cells of equal length based on cells, and each car occupies one cell [2]. To make the simulated traffic flow more consistent with the real situation, the safe distance model was introduced to further improve the simulation accuracy. The model evolution process includes constant velocity, acceleration, deceleration and position updating. Kim *et al.* [11] believed that if CACC vehicles wanted to complete the communication function, there should be at least one CACC vehicle in a communication range on the road network. However, considering that the transmission of wireless signal between vehicles will be affected by other uncertain factors such as driving speed, channel quality and environmental changes, the wireless signal will be dynamically attenuated during transmission. Therefore, if the CACC vehicle wants to complete the communication function, it must ensure the reliability of signal transmission in the communication range while ensuring that there is at least one CACC vehicle in the communication range. Based on this, this paper proposes a calculation method for the communication probability of CACC vehicles in the networked vehicle environment, and the communication success probability P_{com} is:

$$P_{com} = [1 - (P1 + P2)^m] P_{suc}. \tag{3}$$

Where m is the total number of cells discretized into roads within the communication range; $P1$ is the proba-

bility that the cell is not occupied by the vehicle; $P2$ is the probability that the cell is occupied by ordinary vehicles. P_{suc} is the probability that the signal will be reliably received.

$$P1 = 1 - \frac{N(t)}{N}. \tag{4}$$

$$P2 = \frac{(1-q)N(t)}{N}. \tag{5}$$

Where $N(t)$ is the total number of vehicles at time t of simulation; N is the total number of discrete cells of the entire lane. q is the ratio of CACC vehicles on road.

The bidirectional generative adversarial network adopts the adversarial tuple strategy, which can not only generate the same data distribution as the training sample, but also output the hidden space feature representation of the training sample. The bidirectional generation adversarial network can capture the hidden space feature representation of training sample data through multiple iterative adversarial networks. Therefore, by making full use of the image semantic feature abstraction ability of the bidirectional generation network and generating the feature sequence with the image essential feature description ability, the perceptual hash code with stronger image content representation ability can be constructed and the image content forensics performance can be improved. In this study, a perception hash image content forensics algorithm based on BiGAN is proposed. By optimizing and enhancing the bidirectional generative adversarial network structure, the bidirectional generative adversarial network can improve its ability to learn complex data distribution, and generate data distribution consistent with complex training samples (such as natural images). At the same time, the learning performance of the potential features of the sample data is enhanced, the hidden space feature representation of the sample image is output and the perceptual hash code is quantitatively generated, which realizes the image content authentication and copyright protection based on the perceptual hash.

The basic model of the image perception hash generation network based on BiGAN consists of four subnetworks, namely as shown in Figure 1, encoding network E, generation network G, joint discriminant network D and jump-layer network S. Where, the encoding network E implements mapping $E : x \to E(x)$ from the original image data x to the potential feature representation $E(x)$. The input is the normalized training image, and the output is the image hidden space feature encoding. The generation network G maps the preset noise distribution z to a data distribution $G(z)$ that is consistent with the target image sample, $G : z \to G(z)$. Joint discriminant D network to distinguish the input data tuples from encoding or generate network $D : ((x, E(x)), (G(z), z)) \to 0, 1$. Aiming at the problems of low quality of generated image and insufficient ability of output feature code representation in bidirectional generative adversarial network, a jump layer network S is added between encoding network E and generating network G to realize the transmission of different dimension feature information between coding network E and generating network G, and the mean square error (MSE) loss is added to the network optimization loss. The content representation ability of the images generated by the generation network G is enhanced, so that the generation network G can output high-quality images with complex texture distribution. At the same time, based on the counter loss of the joint discrimination network D, the reverse excitation coding network E outputs more representative image hidden space feature coding, and improves the quality of the generated image perceptual hash code.

Where, E represents the coding network, G represents the generation network, D represents the joint discriminant network, S represents the added jump-layer network, RealImage represents the training sample Image, and Generated Image represents the generated image.

The perceptual hash generation algorithm based on BiGAN makes full use of the self-learning ability of the bidirectional generative adversarial network, and generates the image perceptual hash code by encoding the hidden space features output by the coding network E. Through the iterative confrontation between the generation network G, coding network E and joint discriminant network D, as well as the optimization and enhancement of the jump-layer network S and the mean square error loss MSE, the hidden space feature representation capability of the image perception hash code is continuously improved, and the effective balance between the authentication robustness and discrimination sensitivity of the perception hash code is achieved.

In the perception hash generation network based on BiGAN, the role of coding network E is to extract the hidden space feature information from the original image and generate the image perception hash sequence. The encoding network designed in this study consists of 10 layers of convolutional neural network, each layer of convolutional neural network includes three data operation processing: image $Conv2d$, $BatchNorm$ and activation ($LeakRelu$). The initial input of the coding network is the normalized training sample image. At the same time, in order to improve the hidden space feature representation ability of the output feature coding, the convolutional layer output of the fifth, sixth and seventh layers of the encoding network E is transmitted to the same dimensional network layer of the generating network G through the jump-layer network S as an input, and the image feature information of different dimensions extracted by the coding network E is linked to the generating network G to improve the visual quality of the generated image and the network convergence speed. The convolutional output of the last layer of the coding network E is used as the image hidden space feature representation sequence to generate the image perception hash code. The detailed parameter information of coding network E in Bigan-based perceptive hash generation network is shown in Table 1. Among them, the parameters in the first column of the config-

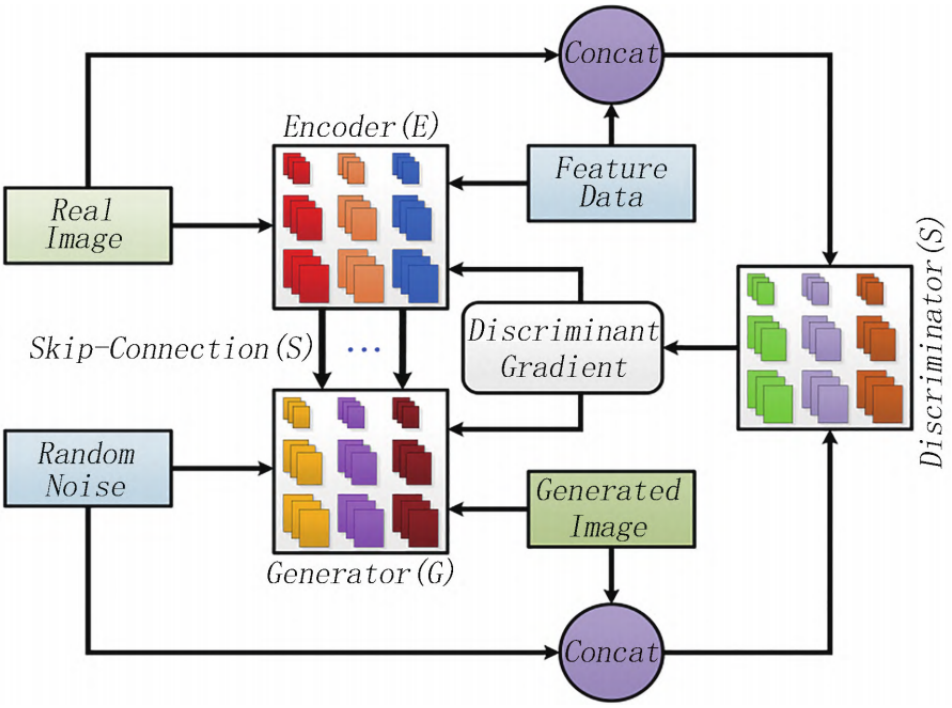


Figure 1: The structure of perceptive hash image forensics algorithm based on BiGAN

uration column represent the number of filters. It can be seen that the coding network E adopts the multiplication method to increase the number of filters, and finally forms an image perception hash code with good hidden space feature representation ability. The parameters in the second column are the size of the sensitivity field of the convolutional operation, the length of the convolutional step, and the number of rows/columns added to the input side. The third column parameter is the slope of LeakRelu activation function adopted. In addition to the last convolution layer, BatchNorm operation is applied after every convolution operation in the experiment to ensure that the training sample data is distributed in the sensitive region of the activation function, so as to avoid the disappearance of gradient and speed up the convergence of the model. In the experiment, a self-learning coding network structure model with 10-layer network structure, including 10 convolutional layers, 9 batch normalization layers and 9 activation layers, is selected to ensure that the network output hidden space feature coding with strong representation ability, considering the influence of the number of convolutional layers on the network operation efficiency and the ability to generate sensing hash code feature representation.

Table 1: Detailed parameter design in encoding network

Layer	Function	value
1	Conv2d, BatchNorm2d, LeakyRelu	32,[3,1,1],0.01
2	Conv2d, BatchNorm2d, LeakyRelu	64,[4,2,1],0.01
3	Conv2d, BatchNorm2d, LeakyRelu	128,[4,2,1],0.01
4	Conv2d, BatchNorm2d, LeakyRelu	256,[5,1,0],0.01
5	Conv2d, BatchNorm2d, LeakyRelu	512,[4,2,0],0.01
6	Conv2d, BatchNorm2d, LeakyRelu	512,[4,1,0],0.01
7	Conv2d, BatchNorm2d, LeakyRelu	512,[4,2,0],0.01
8	Conv2d, BatchNorm2d, LeakyRelu	1024,[4,1,0],0.01
9	Conv2d, BatchNorm2d, LeakyRelu	2048,[1,1,0],0.01
10	Conv2d, BatchNorm2d, LeakyRelu	1024,[1,1,0]

3 Simulation Experiment

Due to the participation of a large number of users, each user may set a different local policy II, which will affect the stability of the P2P network, so the local policy should be given by the designer according to the security prin-

Table 2: Service evaluation analysis

0-0.3	0.3-0.5	0.5-0.8	0.8-1
danger information	low information	lower information	trust information

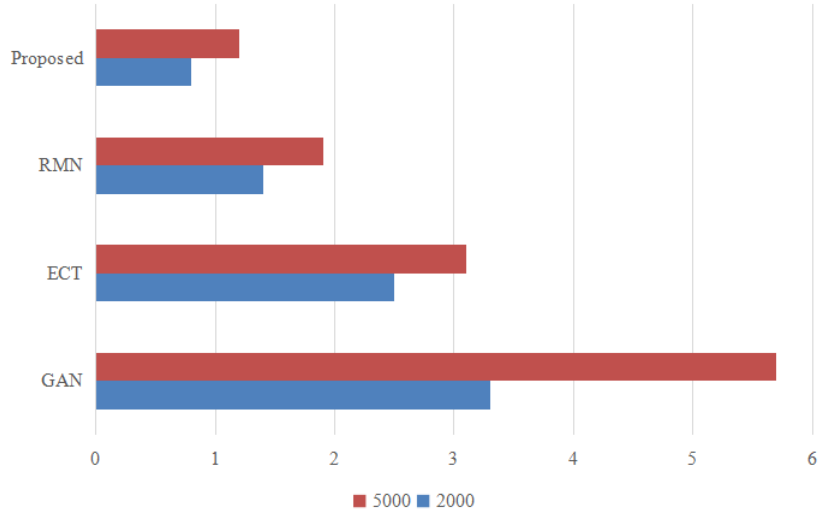


Figure 2: Visual result

ciple of the default value, common users use the default value. In order to explain the value range of local policy II, according to the general safety principle, the analysis diagram is given, the designer can determine the specific value according to the weighted result.

This model takes 4 language variables y, k, w and z to analyze service evaluation, and their weights are all 25%, as shown in Table 2.

When the information is published, it is first divided into several data blocks, and distributed agents store it in neighboring nodes. In this case, subsequent nodes need to search for data blocks when accessing them. Since the local resource list stores a large amount of data block information, the subsequent node only needs to search for one data block, which is a constant less than the total number of data blocks. Its value size is restricted by the amount of information stored in the local resource list, and its search efficiency is comprehensively affected by data block availability, reliability k, optimal search, and data integrity w, etc. Their thresholds are generally set at 0.5, 0.6, 0.5, 0.3. When they are lower than this value, the data service evaluation value is lower than 0.5, then the data is cached or cleared; Otherwise, the data is safely available.

Because the higher the activity of nodes, the more times the nodes are evaluated, the greater the sharing degree of the stored data blocks, the more reliable the comprehensive service evaluation, the effective supervision of data security, and the enhanced stability of the system. You can modify the threshold if you need to search for as much information as possible but the information is not widely shared.

Between any two nodes in the cluster, because of the uniqueness of its coding, there must be different bits of coding, so the probability of establishing a communication link between any two nodes is 100%. The comparison of the communication cost simulation experiment data between the random key model and the information transmission model in the process of key establishment is shown in Table 3 and Figure 2.

Table 3: Comparison of communication overhead with different nodes/s

Model	2000	5000
GAN [25]	3.3	5.7
ECT [26]	2.5	3.1
RMN [5]	1.4	1.9
Proposed	0.8	1.2

As can be seen from Table 1, when the number of nodes is relatively small, the communication cost of the transmission model is less than that of the random key model, because the key path establishment between nodes in the transmission model only needs one communication. In order to improve the security performance, the random key model does not create paths at one time, but generates new keys through mutual random numbers. In the first communication between nodes in the cluster [10, 17, 23], two more times of communication will be carried out. Rel-

ative to the improvement of its security performance, a small increase in the communication overhead between nodes in the cluster is acceptable. When the number of nodes increases sharply, the communication cost of the random key model is less than that of the transmission model, because with the increase of the number of nodes, the intercluster communication greatly increases, and the probability of the direct first path establishment of the random key model in the intercluster communication is increased.

4 Conclusions

Based on the dual key building algorithm based on GAN model, a new random key building algorithm based on dual coding is proposed. Theoretical analysis and simulation results show that the new algorithm can effectively improve the probability and security performance of direct dual key establishment between any two nodes, and also save the communication cost in the communication between nodes. Therefore, it can be considered that this is a better performance IoV key establishment algorithm.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] E. Abuhdima *et al.*, "Impact of Dust and Sand on 5G Communications for Connected Vehicles Applications," *IEEE Journal of Radio Frequency Identification*, vol. 6, pp. 229-239, 2022.

[2] I. Ahmed, E. Balestrieri, P. Daponte and F. Lamonaca, "A Method Based on Ellipse Fitting for Automatic Morphometric Parameter Measurements of Fish Blood Cells," in *2023 IEEE International Symposium on Medical Measurements and Applications (MeMeA), Jeju, Korea, Republic of*, pp. 1-6, 2023, doi: 10.1109/MeMeA57477.2023.10171881.

[3] T. Devi and N. Deepa, "A novel intervention method for aspect-based emotion Using Exponential Linear Unit (ELU) activation function in a Deep Neural Network," in *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India*, pp. 1671-1675, 2021, doi: 10.1109/ICICCS51141.2021.9432223.

[4] Z. Ding, J. Xiang, "Overview of intelligent vehicle infrastructure cooperative simulation technology for IoV and automatic driving," *World Electric Vehicle Journal*, vol. 12, no. 4, pp. 222, 2021.

[5] Z. Dou, J. Tian, Q. Yang, L. Yang, "Design and analysis of cooperative broadcast scheme based on reliability in mesh network," *Mobile Information Systems*, vol. 2021, pp. 1-18, 2021.

[6] L. Du, S. Gong, L. Wang, X. Y. Li, "Information-traffic coupled cell transmission model for information spreading dynamics over vehicular ad hoc network on road segments," *Transportation Research Part C: Emerging Technologies*, vol. 73, pp. 30-48, 2016.

[7] T. M. Ghazal, R. A. Said, N. Taleb, "Internet of vehicles and autonomous systems with AI for medical things," *Soft Computing*, pp. 1-13, 2021.

[8] M. Gupta, R. B. Patel, S. Jain, H. Garg, B. Sharma, "Lightweight branched blockchain security framework for Internet of Vehicles," *Transactions on Emerging Telecommunications Technologies*, 2022. https://doi.org/10.1002/ett.4520.

[9] I. Jahan, M. F. Ahmed, M. O. Ali, Y. M. Jang, "Self-gated rectified linear unit for performance improvement of deep neural networks," *ICT Express*, vol. 9, pp. 3, pp. 320-325, 2023.

[10] S. U. Jan, I. A. Abbasi and M. A. Alqarni, "LMAS-SHS: A Lightweight Mutual Authentication Scheme for Smart Home Surveillance," *IEEE Access*, vol. 10, pp. 52791-52803, 2022.

[11] D. J. Kim, H. I. Kim, S. H. Lee, C. C. Chung, "Adaptive Feedforward Compensator Based on Approximated Causal Transfer Function for CACC with Communication Delay," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 15192-15197, 2020.

[12] P. Li, A. A. Laghari, M. Rashid, J. Gao, T. R. Gadekallu, A. R. Javed, S. Yin, "A Deep Multimodal Adversarial Cycle-Consistent Network for Smart Enterprise System," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 693-702, 2023.

[13] J. Liu, L. Zhang, C. Li, J. Bai, H. Lv and Z. Lv, "Blockchain-Based Secure Communication of Intelligent Transportation Digital Twins System," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 11, pp. 22630-22640, 2022.

[14] Q. Pan, J. Wu, J. Nebhen, A. K. Bashir, Y. Su and J. Li, "Artificial Intelligence-Based Energy Efficient Communication System for Intelligent Reflecting Surface-Driven VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 19714-19726, 2022.

[15] Y. Ren, F. Zhu, J. Wang, P. K. Sharma and U. Ghosh, "Novel Vote Scheme for Decision-Making Feedback Based on Blockchain in Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 2, pp. 1639-1648, 2022.

[16] P. Sharma and H. Liu, "A Machine-Learning-Based Data-Centric Misbehavior Detection Model for Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4991-4999, 2021.

[17] Y. Sun, S. Yin, J. Liu, L. Teng, "A Certificateless Group Authenticated Key Agreement Protocol Based on Dynamic Binary Tree," *International Journal of Network Security*, vol. 21, no. 5, pp. 843-849, 2019.

[18] T. Tapli and M. Akar, "Cooperative Adaptive Cruise Control Algorithms for Vehicular Platoons Based

on Distributed Model Predictive Control," in *2020 IEEE 16th International Workshop on Advanced Motion Control (AMC), Kristiansand, Norway*, pp. 305-310, 2020, doi: 10.1109/AMC44022.2020.9244429.

[19] L. Wang, S. Yin, H. Alyami, *et al.*, "A novel deep learning-based single shot multibox detector model for object detection in optical remote sensing images," *Geoscience Data Journal*, 2022. https://doi.org/10.1002/gdj3.162.

[20] P. Wang, C. Jiang, X. Deng, L. Wang, H. Deng and Z. He, "A multi-mode cooperative adaptive cruise switching control model for connected vehicles considering abnormal communication," in *2017 6th Data Driven Control and Learning Systems (DDCLS), Chongqing, China*, pp. 739-744, 2017, doi: 10.1109/DDCLS.2017.8068165.

[21] L. Yang, A. Moubayed and A. Shami, "MTH-IDS: A Multitiered Hybrid Intrusion Detection System for Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 616-632, 2022.

[22] Z. Yao, Y. Wu, Y. Wang, B. Zhao, Y. Jiang, "Analysis of the impact of maximum platoon size of CAVs on mixed traffic flow: An analytical and simulation method," *Transportation Research Part C: Emerging Technologies*, vol. 147, pp. 103989, 2023.

[23] S. Yin, H. Li, L. Teng, A. A. Laghari, V. V. Estrela, "Attribute-based Multiparty Searchable encryption model for Privacy Protection of Text Data," *Multimedia Tools and Applications*, 2023. ttps://doi.org/10.1007/s11042-023-16818-4.

[24] L. Zhou, T. Ruan, K. Ma, C. Dong, H. Wang, "Impact of CAV platoon management on traffic flow considering degradation of control mode," *Physica A: Statistical Mechanics and Its Applications*, vol. 581, pp. 126193, 2021.

[25] J. Zhang and Y. Zhao, "Research on Intrusion Detection Method Based on Generative Adversarial Network," in *2021 International Conference on Big Data Analysis and Computer Science (BDACS), Kunming, China*, pp. 264-268, 2021, doi: 10.1109/BDACS53596.2021.00065.

[26] Y. X. Zhang, L. Zou, "Research on information dissemination on social networks based on edge-based compartmental theory," *International Journal of Modern Physics B*, vol. 35, no. 24, pp. 2150249, 2021.

Biography

Junting Zhang biography. Junting Zhang is with School of Automobile, Henan College of transportation. Research interests are Information security, Computing networks, Internet of vehicles security.

Data Privacy Protection Based on Unsupervised Learning and Blockchain Technology

Jian'E Zhao and Jianjun Zhu
(Corresponding author: Jianjun Zhu)
School of Electronics and Electrical Engineering, Zhengzhou University of Science and Technology
Zhengzhou 450000, China
Email: xdwangxd@163.com

(Received Oct. 21, 2023; Revised and Accepted Feb. 7, 2024; First Online Feb. 23, 2024)
The Special Issue on Data Fusion, Deep Learning and Optimization Algorithms for Data Privacy Protection
Special Editor: Prof. Shoulin Yin (Harbin Institute of Technology)

Abstract

In order to ensure the reliability and privacy security of perceptual data, this paper proposes data privacy protection based on unsupervised learning and blockchain technology. In this scheme, audit nodes are set up for user screening and performing tasks, mixing nodes for dispute processing and reward distribution, and differential privacy technology under the mixing model is used to noise user data. The method uses boundary-extended local sensitive hashing to calculate the similarity between the instances. It weights the instances according to the similarity to realize the federated transfer learning based on the instance. In this process, the instance itself does not need to be disclosed to other parties, preventing direct disclosure of privacy. At the same time, in order to reduce the indirect privacy leakage in the process of knowledge transfer, the unsupervised learning mechanism is introduced in the process of knowledge transfer to disturb the gradient data that needs to be transmitted between the parties to realize privacy protection in the process of knowledge transfer. In addition, the additional secret sharing technology is also used to divide the data into r mixers to prevent the mapping relationship between the user and the data. Finally, the feasibility of the scheme is verified by experiments. Compared with the relevant algorithms, the data obtained by the scheme is more accurate.

Keywords: Blockchain Technology; Boundary-Extended Local Sensitive Hashing; Data Privacy Protection; Unsupervised Learning

1 Introduction

With the development of Internet of Things technology, 5G technology and big data analysis technology, the collection and transaction of personal perception data is becoming increasingly common. In perceptual data trading, individual users can obtain rewards by selling their perceptual data. Buyers can use the perception data for research, product development and training of intelligent systems. However, personal perception data involves personal privacy information, so it is necessary to ensure the security of data [10,15,22]. Traditional privacy protection methods such as encryption and desensitization, while effective, are still subject to attack and cracking in some cases. Therefore, it becomes more and more important to design a more efficient and secure privacy protection scheme.

Differential privacy (DP) is a new definition of privacy, which is used to protect the privacy information of individuals in the database when releasing statistical information [11]. DP generally refers to central differential privacy (CDP), where a central server collects data about users, adds noise to the aggregated results, and then publishes the results. However, the central server may leak private data, so local differential privacy (LDP) is proposed. LDP differs from CDP in that each user adds random noise before sending the data to a central server. Therefore, the user does not need to trust the server. However, local differential privacy adds a lot of noise, which will reduce the availability of data. For this reason, in 2017 Bittau *et al.* [1] proposed ESA (encode-shuffle-analyze) framework, which mainly consisted of encoder, shuffler and analyzer. The encoder runs on the client side to locally encode, segment, and perturb user data. The mixer runs on a semi-trustworthy third party that can safely shuffle data with the help of existing secure shuffle protocols. The analyzer runs on the data collector side to correct and analyze the collected data. In this framework, the mixer completes the complete anonymity of user data, so that users can obtain more privacy protection while making less disturbance to the data itself. Subsequently, Tang *et al.* [18] introduced differential privacy under the mix-up model according to this framework, and conducted a rigorous mathematical proof of the privacy

amplification theory. Privacy amplification theory refers to that the user perturbs the data through localized differential privacy method on the client side, so that the disturbed data can be close to the statistical data obtained by the centralized method after mixing. A middle ground between CDP and LDP in terms of privacy and utility can be achieved by introducing an additional party, namely the shuffle model.

In addition, blockchain as a new technology [16], blockchain-based perceptual data transactions can achieve decentralized data storage and management, avoiding the risk of single point of failure and improving the security of data. In addition, the smart contract function of blockchain can realize the automation and programmability of data transactions, increasing the transparency and credibility of data transactions. However, blockchain-based perceptual data transactions still face some challenges and privacy protection needs. For example, how to protect the privacy of the perceived data while ensuring the immutability of the transaction, how to realize the anonymized transaction process, and how to ensure the controllability and compliance of the data. Therefore, it is necessary to carry out in-depth research and propose innovative blockchain-based perceptual data privacy protection schemes to provide effective technical support for the security and reliability of perceptual data transactions.

2 Related Works

Most traditional machine learning methods need to centralize scattered data for training [9]. With the in-depth development of the era of big data, the harm caused by data privacy leakage is becoming more and more serious, and the state and society pay more attention to data security and privacy protection. Information processors shall take technical measures and other necessary measures to ensure the security of the personal information they collect and store, and prevent information disclosure, alteration and loss. Fragmented data cannot be easily aggregated to train machine learning models, forming "data island".

Although federated learning can solve the problem of data silos and direct privacy disclosure in multi-party distributed training, when the data sets of each party have large differences in sample space and feature space, the prediction accuracy and stability of federated model will inevitably decline. Aiming at this limitation of federated learning, Liu *et al.* [13] proposed federated transfer learning in 2020 to improve the prediction accuracy of federated models. Saha *et al.* [17] divided federated transfer learning into model-based federated transfer learning, feature-based federated transfer learning and case-based federated transfer learning according to different knowledge transfer objects. Among them, the basic principle of case-based federated transfer learning is that participants select or weight training samples selectively according to certain knowledge transfer strategies to reduce distribution differences, so as to minimize the target loss function and improve the model prediction accuracy. Some federative transfer learning studies focus only on model performance and ignore privacy protection. For example, Hu *et al.* [7] proposed a federated transfer learning method for gradient lifting tree models. Although the paper claimed that this method satisfied the privacy protection, in fact, its work only satisfied the simple privacy protection viewpoint. This paper believed that privacy protection could be achieved as long as the original data of participants did not go out of the local area, and only the direct privacy disclosure was considered, without considering the privacy disclosure that could be caused by the capture of model parameters or gradient information. Such privacy disclosure is indirect disclosure, especially gradient data disclosure, which may lead to label inference attacks and member inference attacks [25].

Reference [6] proposed a profit-driven data acquisition framework for crowd perception data market, which realized the determination of group perception data transaction patterns, profit maximization of polynomial computational complexity, and payment minimization in strategic environments. Reference [2] designed a mobile crowdsense data market architecture and proposed a crowdsense data pricing mechanism based on online query to determine the transaction price of crowdsense data, which was superior to the most advanced pricing mechanism, achieving about 90% of the best revenue, and distributing rewards among data providers in a fair way to encourage data providers to contribute data. However, centralized data storage and management models may have risks of single points of failure and data abuse, and some security issues cannot be guaranteed.

On the other hand, the privacy protection scheme combined with DP and blockchain is also a relatively cutting-edge research direction. For example, Gai *et al.* [5] used DP to build a blockchain-based privacy protection architecture for the Industrial Internet of Things. The proposed architecture relied on a centralized entity called an "optimization server" that assigned tasks, collected data, and added "noise" to the data using DP. This solution provided privacy protection, but once a trusted centralized entity was attacked, all data was compromised. Li *et al.* [12] proposed a secure power data transaction blockchain scheme based on differential privacy, which utilized zero-knowledge proof and blockchain to achieve data availability and reliability of data transactions without data leakage, and proposed a differential privacy protection scheme to protect private information in power data. However, this scheme used CDP, the data noise process was implemented in the centralized server, once attacked, all the data would be leaked. It used LDP to protect the privacy of data providers from data consumers and system operators, Jia *et al.* [8] built a blockchain-based solution to ensure fair exchange and immutable data logs. However, this scheme added a lot of noise, which affected the availability of data, and the RAPPOR method required

a lot of communication overhead.

Therefore, additional privacy protection policies must be introduced. Park *et al.* [14] proposed a secure federated transfer learning framework for neural network models, which used homomorphic encryption and secret sharing to protect privacy and was a feature-based federated transfer learning. It used an independent neural network model to map the source features of the participant dataset into a common feature subspace in which knowledge transfer between participants was realized. Zhang *et al.* [26] proposed a differential privacy federated transfer learning method based on voting strategy for neural network models, which was model-based federated transfer learning. Each party used the local model to predict the public data set from the central server to obtain false labels, and the central server voted according to the false labels and the majority rule to generate global labels to realize knowledge transfer. Chiu *et al.* [4] proposed a heterogeneous federated transfer learning method for logistic regression and support vector machine models, which used homomorphic encryption and secret sharing to protect privacy and was a feature-based federated transfer learning. It used domain adaptation and feature mapping to map the participant's data to a homogeneous common feature space in which knowledge transfer was achieved.

3 Proposed Data Privacy Protection

The data privacy protection model proposed in this paper contains two main design goals: a) to realize the case-based knowledge transfer between parties, and to realize the privacy protection in the process of knowledge transfer; b) The unsupervised learning model with higher prediction accuracy can be trained by all parties through knowledge transfer.

3.1 Basic Assumption

Suppose there are M parties, each party is represented by P_m, $m = 1, 2, \cdots, M$ is the serial number of the participant. $I_m = (x_i^m, y_i^m)|i = 1, 2, \cdots, N_m$ represents the data set for party P_m. I_m contains N_m instances. $x_i^m \in R^d$ is an instance attribute. $y_i^m \in R$ is the instance tag. The total number of instances for all participants is $N = \sum_{m=1}^{M} N_m$. Assuming that each instance has an unique global ID, the global ID of the $i-th$ instance x_i^m of P_m represents a number of pairs of $ID_{m,i} = (m, i)$. Global ID is allocated and maintained independently by each party and stored in the local hash table. During the exchange of local hash tables during the preprocessing phase, each party can obtain the global ID of all the participating party instances. The global ID does not reveal the instance data itself because it does not contain any attribute characteristics of the instance. The only information that global ID can divulge is almost the number of instances of the participant, which is outside the scope of this paper.

3.2 Pretreatment Stage

The final goal of each party in the preprocessing phase is to construct the similarity matrix S^* by finding a corresponding similar instance for each of its instances in the other parties based on the similarity determined by the hash table. Locally sensitive hashing (LSH) [20] is an algorithm that implements approximate nearest neighbor search. LSH uses the hash value as the bucket number. The core idea is that two adjacent data points (that is, two similar data points), their hash values have a high probability of being equal, will be mapped to the same bucket. The key of LSH is to find and generate hash conflicts as much as possible to realize nearest neighbor search. This is different from hashing in the cryptographic sense, where hashing algorithms require as little hash conflict as possible. LSH will map multiple inputs to the same hash value output, an input can be mapped to a hash value vector output by calculating the hash value several times, and the value of the original input cannot be determined by the output, to achieve the effect of data privacy.

In this paper, the boundary-expanding LSH (BELSH) [21] is used to calculate the hash value of the instance and construct the hash table, taking into account the similarity of instances at the boundary of the hash bucket. According to the hash conflict and unidirectional characteristics of BELSH, BELSH is used to calculate the hash value of the instance and map the global ID of the instance to the corresponding bucket. The hash value (bucket number) can display the mapped instance features without revealing the real attribute characteristics of the instance.

First, the initiator coordinates and sends parameters and policies to other participants. Then, in order to obtain similarity information between instances, each party uses BELSH to build L local hash tables, each consisting of a differentially numbered bucket and a global ID that is mapped to the bucket. Then, the parties exchange local hash tables to build L identical global hash tables, and count the number of identical hash values between instances on multiple global hash tables. The greater the number value, the higher the similarity between instances. Finally, each party P_m builds a similar matrix $S^m \in R^{N_m \times M}$. Where each row of S^m corresponds to a similar instance of an instance in I_m, and each column corresponds to a similar instance between a participant (including P_m) and P_m. Therefore, the element S_{ij}^m in row i and column j of S^m represents that for instance x_i^m of P_m, the global ID of the instance that is most similar to it in P_j.

Algorithm 1 describes the process of each party in the preprocessing stage from calculating hash values to building a similar matrix S^*. In algorithm 1, P_m represents each player in turn. Given L BELSH hash functions, each party calculates their instance hash values separately

and builds L local hash tables separately. Then, the parties exchange local hash tables to create the same L global hash tables (each global hash table consists of M local hash tables). Finally, each party computes the similarity matrix S^m from the global hash table.

Algorithm 1 Each party P_m builds a hash table separately and calculates the similar matrix S^m

Input: L BELSH hash functions $H_{kk=1,2,\cdots,L}$, Data set I_m.
Output: Similarity matrix S^m.
for $m \leftarrow 1$ to M paralleled do
  for $i \leftarrow 1$ to N_m do
    Compute hash value $hash_i^{mk} | hash_i^{mk} \leftarrow H_k(x_i^m)$
  end for
end for
Parties exchange local hash tables to create global hash tables.
for $m \leftarrow 1$ to M paralleled do
  for $i \leftarrow 1$ to N_m do
    for $j \leftarrow 1$ to M do
      Call algorithm 2, which returns the global ID of the instance with the highest count value.
      $S_{ij}^m \leftarrow ID_j$
    end for
  end for
end for

Algorithm 2 is a sub-procedure of algorithm 1, called by algorithm 1, and describes the process of finding the global ID of similar instances when calculating the similar matrix S^m. Record the global hash table number as $k = 1, 2, \cdots, L$. For instance x_i^m of P_m, the hash value in the $k-th$ global hash table is denoted as a $hash_i^{mk}$. Suppose P_m wants to find similar instances of x_i^m in P_j, then P_m uses an array of capacity N_j to record the similarity between x_i^m and the instances that P_j belongs to. P_m adds one to the similarity of the instance of P_j whose hash value is equal to the $hash_i^{mk}$, and so on, in each global hash table, P_m performs the above record operation. In this way, P_m gets N_j count values as similarity information. The instance with the highest count is the similar instance of x_i^m in P_j, and the global ID of the similar instance is returned to algorithm 1 as S_{ij}^m into the similar matrix S^m. If there are multiple instances that have the highest count, the instance that has the highest count for the first time is selected as a similar instance.

Algorithm 2 Find the instance ID in P_j that is most similar to instance x_i^m

Input: L global hash tables; The hash value $hash_i^{mk}$ of instance x_i^m in a different global hash table.
Output: Global $ID = ID_{j,*}$ of similar instances in P_j.
$sim[N_j] \leftarrow 0$.
indictor
for $k \leftarrow 1$ to L do
  if $hash_q^{jk} = hash_i^{mk}$ then
    $sim[q] \leftarrow sim[q] + 1$
    the element with the highest current count
  end if
end for
return $ID_{j,*}$

3.3 Data Feature Extraction Based on Unsupervised Learning

In the whole process of collaborative positioning, the data quality of nodes cannot be in a stable state. Due to some unexpected situations, the node may not be able to provide high-quality data for a period of time; Or, some malicious nodes deliberately provide poor quality data to interfere with the performance of the positioning system. Therefore, on the basis of dynamic observation of node data quality, this paper proposes an anomaly detection algorithm based on unsupervised learning [19,24] to eliminate some unqualified node data in time to ensure the stability of the overall performance of the positioning system.

It is obviously unreasonable to judge whether a node is abnormal only according to the data quality of the node in one iteration. Therefore, record the historical positioning data provided by the node, and use unsupervised learning to establish the Reputation evaluation system of the node on this basis, so as to determine whether there are abnormal nodes. In general, a person's reputation in society is often gradually built up by a series of reliable actions, and can be quickly "destroyed" after a few dishonest actions. Therefore, the design of reputation function needs to meet the following characteristics: (1) When the node contributes higher quality data, the reputation of the node will be slightly improved; When the data provided by a node is of poor quality, the reputation value will decrease significantly. Based on the above analysis, this paper uses logical functions to model the reputation of nodes, because the value growth rate of logical functions is the fastest in the left and right sides and the slowest in the middle part. Specifically, using the Richard growth curve, the expression is:

$$R(t) = A(1 - Be^{-at})^{1/(1-b)}. \tag{1}$$

Where A is the saturation value of cumulative growth. B is the growth initial parameter. a is the growth rate parameter. b is the allometric growth function.

In order to describe the performance of node data in the long term, the historical data of nodes is summarized. At the same time, in order to distinguish the importance of historical data in different periods, exponential factors are used to weight the data in each iteration. Therefore, when node i is iterated in round t, the input parameters of the reputation estimation function are designed as follows:

$$q_{i,t} = \sum_{n=1}^{t} \varpi_i^{t-n} \Omega_i^t. \tag{2}$$

Where ϖ represents the historical data proportion of nodes in different stages. ϖ is a value of different sizes in the value space N, and $0 < \varpi < 1$.

Below, DQN (Deep Q-network) will be used to get the weight of the current data of the node in each round of iteration. The kernel of DQN is Q-learning machine Learning algorithm, assuming that the Q function adopted is denoted as:

$$\phi(s_t) \rightarrow Q(\varphi(s_t), a_t; \vartheta). \tag{3}$$

This function is used to calculate the expected cumulative reward for taking action a_t given input $\phi(s_t)$. Where ϑ is the behavioral value function that maps the input to the output decision. $\varphi(s_t)$ indicates state reconstruction. In each round of learning, the possible behavior is selected using greedy strategy, that is, the value of weight ϖ is selected. In each round of input-output mapping, the Q-network generates a tuple consisting of the current state $\varphi(s_k)$, the current action a_k, the immediate reward r_{k+1}, and the next moment state $\varphi(s_{k+1})$. Store these results in hard disk memory D. At each learning time, a Mini-batch is randomly sampled from D, combined with the target network $\hat{Q}(\vartheta')$, the loss is calculated and the Q-network is trained. Specifically, the loss function can be designed as:

$$L(\vartheta) = E[(y_k - Q(\varphi(s), a; \vartheta_k))^2]. \tag{4}$$

Where $E[*]$ indicates the expected value. y_k is the value of the objective function, and the expression is:

$$y_k = r_{k+1} + \gamma max_a \hat{Q}(\varphi(s_{k+1}), a; \vartheta'). \tag{5}$$

Where r_{k+1} represents a Reward and γ is a normal amount.

After learning the weight ϖ_i^t of node data in different periods, the reputation value of node i in the round t iteration can be obtained by calculating the value of $R(q_{i,t}(\varpi_i^t))$. Finally, the reputation value of the node at the current moment is compared with the fixed threshold R_{Thre}. If it is lower than the threshold, the current data of the node is judged to be abnormal, and the data of the node will not be used in the calculation of collaborative positioning.

3.4 Addition Secret Sharing

Addition secret sharing means that users can split a secret value $v \in 0, 1, 2, \cdots, d-1$ into r parts. $r-1$ is randomly selected, it calculates the last a_r to make $(a_1 + a_2 + \cdots + a_{r-1} + a_r) mod d = v$. These are then sent to r participants, each with only one random value. In this technique, v can only be recovered if all r parties cooperate.

Let $M = R \circ S$, each user u_i perturbs $v_i : y_i = R(v_i)$ by using the localized differential privacy algorithm $R : V \rightarrow Y$ satisfying ε_l on the local client, and $y_1, y_2, \cdots, y_n$ is the perturbed result of n users. $S : Y^n \rightarrow Y^n$ performs random mixing operations on the output results of n users for the mixer. When for any adjacent data sets D and D' (only one of n users with different data), any output set $y' \in Y^n$ satisfies the following formula, then M satisfies (ε_c, δ)-shuffle differential privacy:

$$Pr[M(D) \in y'] \leq e^{\varepsilon_c} Pr[M(D') \in y'] + \sigma. \tag{6}$$

Where ε represents the privacy budget and $\delta \in (0, 1]$ is the risk probability of privacy disclosure.

3.5 Generalized Randomized Response (GRR)

The basic mechanism is called random response [5], which is introduced for binary states ($D = 0, 1$), but can be easily extended. In a generalized randomized response (GRR), each user with a private value $v \in D$ sends $GRR(v)$ to the server, where $GRR(v)$ outputs the true value v with probability P. With probability $1-P$, $v \in D$ is randomly selected to replace the true value v and $v' \neq v$, the size of the field is expressed as $d = |D|$, that is, the following formula:

$$Pr[GRR(v) = y] = \left\{ \begin{array}{l} p = \frac{e^{\varepsilon}}{e^{\varepsilon}+d-1} \text{ if } y = v \\ q = \frac{1}{e^{\varepsilon}+d-1} \text{ otherwise} \end{array} \right\} \tag{7}$$

4 Security Analysis

4.1 Privacy Protection Analysis

Compared with existing schemes, the proposed scheme can not only protect the identity privacy of participants, but also ensure data privacy. First, in terms of identity privacy, in the registration stage, the identities of various entity participants will be strictly reviewed by AN through the blockchain, avoiding malicious users, ensuring that all participants are legitimate, and then the blockchain will generate a pseudonym for each participant. The privacy of participants will be protected because pseudonyms are used in the follow-up process instead of their real identities.

Secondly, in terms of data privacy, in the transaction stage, the original data of the user is added to the noise locally through (ε_l, δ) differential privacy, and the data is sent to r SN respectively through secret sharing. Ensure that the original data is owned only by yourself and not accessed by any participant. The mixer randomly arranges the data reported by the user, and after receiving the data, the DC cannot link the user to the data because the data is scrambled. During the transaction process, only the hash value of the transmitted data is uploaded to the blockchain, and the public transaction information is only used to verify whether the data is tampered with, and does not contain the transmitted data.

4.2 Protection Against Common Attacks

1) Conspiracy attack.

If a user colludes with the DC, the DC can get reports from all users except the attacked one. By subtracting each user's data from the final result, the DC can obtain the victim's LDP report. Therefore, the privacy also falls back to (ε_l, δ) localized differential privacy, which is protected by local differential privacy.

When SNs collude with each other, there is no amplification of privacy. When a server colludes with a secondary server, the privacy guarantee reverts to the original LDP model. When using the shuffle model, the possibility of such collusion needs to be reduced, for example, by introducing more secondary servers.

2) Denial of service attack.

To defend against denial-of-service attacks, system operators will initially charge a portion of the additional fee as a broadcast fee when a DC publishes a task. The minimum fee will be set by AN to ensure the proper operation of the contract code. Charging a DC when a task is published is done in part to keep the transaction running properly, and in part to prevent a malicious DC from consuming resources. Attackers get far less in return than they pay, so denial of service attacks can be defended against.

3) Tampering attacks.

Attackers can maliciously tamper with stored data. However, a transaction published on the blockchain cannot be tampered with, and if it is to be modified, it needs to be republished. Participants can check whether the data has been tampered with by verifying the hash value of the data on the blockchain. In addition, his data is encrypted by a key before it is sent to DC. Without the corresponding private key, neither internal nor external attackers can crack the ciphertext.

In addition, if the attacker is a malicious node in the system, the execution results may be deliberately falsified. In this case, AN is set up to perform random checks on each participant. If the malicious behavior is found, the malicious node will be severely punished and a certain credit value attribute will be deducted. In addition, if the DC is not satisfied with the result and disputes it, then the system will track the transaction and the malicious behavior will also be detected. Therefore, when the harm outweighs the good, the participants usually do not act maliciously.

4.3 Correlative System Characteristic Analysis

The scheme in this paper can ensure the robustness, non-repudiation and traceability of the system.

1) Robustness.

First, either party can try to interrupt the transaction process, but this is easily resolved. If the user refuses to upload the data, another user is found to upload the data. If the SN refuses the service, AN can find another SN to replace it from the previously applied node and reduce the credit value of the SN that refuses the service.

Second, the SN may deviate from the protocol, which will not perform the shuffle operation, so the DC gets the original LDP report. In this case, the DC can get more information, but the SN has no benefit other than saving some computing power. Malicious nodes may be randomly checked by AN, which will result in severe penalties, and the credit attribute will be reduced. Therefore, this paper assumes that SN will not deviate from the protocol operation. Since DC can only view and evaluate the final report, DC cannot get more information from the user.

2) Non-repudiation.

Data transactions are conducted through the blockchain, and the transparency of the blockchain ensures the non-repudiation of transactions. The allocation of rewards to the corresponding entities shall be executed by the smart contract if any entity has illegal operations, such as the user and SN obtaining improper benefits by falsifying or tampering with data. AN will conduct spot checks from time to time and accept complaints from participants, and if the user and SN are found, they will be severely punished. DC will also be held liable if it refuses to pay for the data it received after receiving it. Therefore, no entity can make illegal profits by rejecting transactions stored on the blockchain.

3) Traceability.

Due to the presence of certain disputed or malicious participants, AN has the right to track the identity of the participants. Transactions published on the blockchain can be traced back to specific details. This scheme takes advantage of the characteristics of the blockchain, the hash value of the transmitted data is stored on the blockchain, which allows AN to effectively track the transaction message, so as to determine responsibility.

5 Experiment Evaluation

5.1 Experiment Environment

Firstly, the data processing process is simulated to test the privacy effect and the influence of different parameters on the mean square error (MSE). The experiments were conducted on a system equipped with an Intel(R) Core(TM) i7-1065G7 CPU @ 1.30GHz with 16GB of RAM. The data privacy protection algorithm is written by python language running on Pycharm 2022.1.3, python version is Python 3.9, and is executed 10 times respectively, and the average value is taken for comparative analysis.

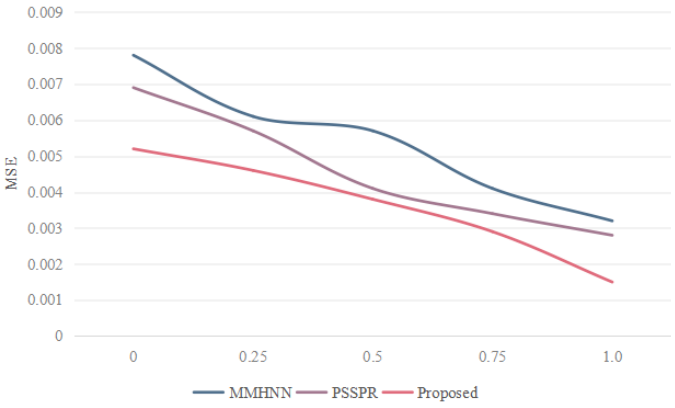


Figure 1: MSE value when ε_C changing

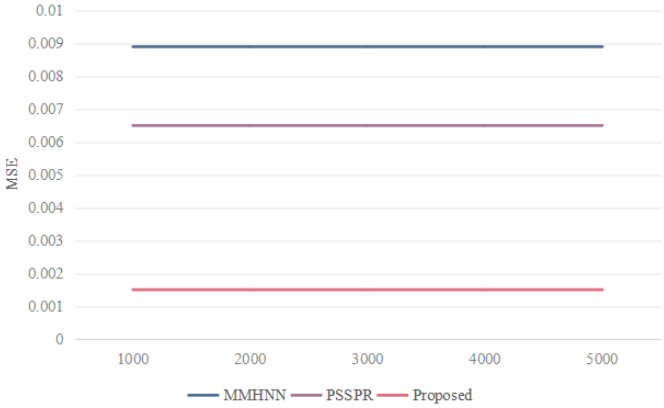


Figure 2: MSE value when k changing

The smart contract experiment is conducted on AMD R5 4600H @3.00GHz and 16GB of RAM running 64bit Ubuntu16.04. In this paper, a private chain in Ethereum is constructed to simulate the scheme, and the hash function SHA256 is used to test the gas consumption of the main function of the smart contract and the system time overhead of calling the function. It is carried out 20 times respectively, and the average value is taken for comparative analysis.

5.2 Experiment Result

Setting parameters $\varepsilon_C = 1.0$, $k = 3000$, $\delta = 10^{-6}$, randomly generating a normal distribution of $\mu = k/2$ and $\sigma = k/6$. This scheme is compared with MMHNN [23] and PSSPR [3]. MSE is calculated as follows:

$$MSE_{frea} = \frac{1}{k}\sum_{i\in[k]}(f_i - \tilde{f}_i)^2. \tag{8}$$

Where f_i is the frequency of the original data v_i. $\tilde{f}_i$ is the estimated frequency of the final v_i.

Figure 2 shows that MSE based on proposed approach is lower than MMHNN and PSSPR. Because the adopted k in the experiment is 3000, the new method in this paper can improve the availability of data in the case of a large range. It is also found that when the value of n increases, MSE decreases and the resulting data availability is higher.

To observe the change of frequency MSE with respect to k from 1000 to 5000, we set parameters $n = 1000000$, $\varepsilon_C = 1.0$, $\delta = 10^{-6}$. For the variable k, it randomly generates $\mu = k/2$ and $\sigma = k/6$.

Figure **??** shows that when the value of k changes from 1000 to 5000, the MSE of proposed method remains small. With the change of k value, the MSE of the method in this paper is almost unchanged, because the algorithm in this paper is suitable for large k value and relatively stable, so it is very necessary to select an appropriate algorithm according to the value range of the perceived data.

Table 1 shows the cost of deploying a smart contract and calling its functions, in gas. The cost per operation is not affected by the number of DS, nor by the range of values. The gas cost and time cost of calling contract function in this scheme are very small, and both belong to the normal consumption range. Although deploying a contract consumes a lot of gas, the contract only needs to be deployed once, so that time is acceptable.

Table 1: The cost and time spent deploying smart contracts and calling functions

Operation	Gas cost	time cost/s
Contract deployment	1164753	179
Create query	90169	71
User data hash upload	85045	82
Shuffle data hash value upload	85045	86

Table 2 shows the comparison between the original data upload efficiency before privacy protection and the data upload efficiency after privacy protection. It can be seen that in the comparison between the data upload before and after privacy protection processing, the consumption time and Gas consumption of smart contract data upload have increased due to the privacy protection.

Table 2: Comparison of original data upload efficiency after privacy protection

size	Gas cost	time cost/s
256	170099	167
512	252161	174
768	334513	179
1024	416868	217

6 Conclusions

This paper proposes a differential privacy approach based on unsupervised learning and blockchain technology. In this scheme, data demanders can assign tasks and purchase data via BTP broadcast. Use blockchain to ensure fairness and traceability of transactions, and use smart contracts to distribute rewards. When collecting data, the differential privacy under unsupervised learning and random response mechanism model is used to noise user data, and the corresponding processing algorithm can be selected according to different data characteristics, and the privacy protection effect close to CDP can be obtained without the need for a trusted third party. Finally, the feasibility of the scheme and the effect of privacy protection are verified by experiments, and several related algorithms are compared, and better results are obtained. Due to the efficiency of the blockchain system, the practical application deployment under the real data set is still a challenge. In the future work, we will continue to focus on how to reduce the efficiency of the blockchain hidden and private protection system, and conduct performance experimental tests on the real data set. In addition, research and design of the mixing node to make it more efficient and more private, and explore the application of the scheme to other application scenarios and improve it is also one of the future work directions.

References

[1] A. Bittau, U. Erlingsson, P. Maniatis, I. Mironov, "Prochlo: Strong privacy for analytics in the crowd," in *Proceedings of the 26th symposium on operating systems principles*, pp. 441-459, 2017.

[2] D. Chatzopoulos, S. Gujar, B. Faltings and P. Hui, "Privacy preserving and cost optimal mobile crowdsensing using smart contracts on blockchain," in *2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Chengdu, China*, pp. 442-450, 2018.

[3] Y. Chen, J. Sun, Y. Yang, T. Li, X. Niu, H. Zhou, "PSSPR: A source location privacy protection scheme based on sector phantom routing in WSNs," *International Journal of Intelligent Systems*, vol. 37, no. 2, pp. 1204-1221, 2022.

[4] H. -J. Chiu, T. -H. S. Li and P. -H. Kuo, "Breast cancer-detection system using PCA, multilayer perceptron, transfer learning, and support vector machine," *IEEE Access*, vol. 8, pp. 204309-204324, 2020.

[5] K. Gai, Y. Wu, L. Zhu, Z. Zhang and M. Qiu, "Differential privacy-based blockchain for industrial internet-of-things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4156-4165, 2020.

[6] J. Hu, K. Yang, K. Wang and K. Zhang, "A blockchain-based reward mechanism for mobile crowdsensing," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 1, pp. 178-191, 2020.

[7] K. Hu, Y. Li, M. Xia, J. Wu, M. Lu, S. Zhang, L. Weng, "Federated learning: a distributed shared machine learning method," *Complexity*, vol. 2021, pp. 1-20, 2021.

[8] B. Jia, X. Zhang, J. Liu, Y. Zhang, K. Huang and Y. Liang, "Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4049-4058, 2022.

[9] Y. Jiang, S. Yin, "Heterogenous-view occluded expression data recognition based on cycle-consistent adversarial network and K-SVD dictionary learning under intelligent cooperative robot environment," *Computer Science and Information Systems*, vol. 20, no. 4, 2023. https://doi.org/10.2298/CSIS221228034J

[10] T. T. Ke, K. Sudhir, "Privacy rights and data security: GDPR and personal data markets," *Management Science*, vol. 69, no. 8, pp. 4389-4412, 2023.

[11] Q. Li, Z. Wen, Z. Wu, S. Hu, N. Wang, Y. Li, X. Liu, B. He, "A survey on federated learning systems: Vision, hype and reality for data privacy and protection," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 4, pp. 3347-3366, 2023.

[12] Y. Li, N. Li and Y. Xia, "Research on a data desensitization algorithm of blockchain distributed energy transaction based on differential privacy," in *2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP), Xi'an, China*, pp. 980-985, 2019.

[13] Y. Liu, Y. Kang, C. Xing, T. Chen and Q. Yang, "A secure federated transfer learning framework," *IEEE Intelligent Systems*, vol. 35, no. 4, pp. 70-82, 2020. doi:10.1109/MIS.2020.2988525.

[14] J. Park, H. Lim, "Privacy-preserving federated learning using homomorphic encryption," *Applied Sciences*, vol. 12, no. 2, pp. 734, 2022.

[15] S. Quach, P. Thaichon, K. Martin, S. Weaven, R. Palmatier, "Digital technologies: Tensions in privacy and data," *Journal of the Academy of Marketing Science*, vol. 50, no. 6, pp. 1299-1323, 2022.

[16] S. U. Rehman, M. U. S. Khan and M. Ali, "Blockchain-based approach for proving the source of digital media," in *2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan*, pp. 1-6, 2020. doi: 10.1109/iCoMET48670.2020.9073820.

[17] S. Saha, T. Ahmad, "Federated transfer learning: Concept and applications," *Intelligenza Artificiale*, vol. 15, no. 1, pp. 35-44, 2021.

[18] Z. Tang, H. -S. Wong and Z. Yu, "Privacy-preserving federated learning with domain adaptation for multi-disease ocular disease recognition," *IEEE Journal of Biomedical and Health Informatics*, 2023. doi: 10.1109/JBHI.2023.3305685.

[19] L. Teng, Y. Qiao, M. Shafiq, G. Srivastava, A. Javed, T. Gadekallu, S. Yin, "FLPK-BiSeNet: Federated

learning based on priori knowledge and bilateral segmentation network for image edge extraction," *IEEE Transactions on Network and Service Management*, vol. 20, no. 2, pp. 1529-1542, 2023.

[20] Y. Tian, X. Zhao and X. Zhou, "DB-LSH 2.0: Locality-sensitive hashing with query-based dynamic bucketing," *IEEE Transactions on Knowledge and Data Engineering*, 2023. doi: 10.1109/TKDE.2023.3295831.

[21] Q. Wang, Z. Guo, G. Liu and J. Guo, "Boundary-expanding locality sensitive hashing," in *2012 8th International Symposium on Chinese Spoken Language Processing, Hong Kong, China*, pp. 358-362, 2012. doi: 10.1109/ISCSLP.2012.6423463.

[22] S. Yin, H. Li, L. Teng, A. A. Laghari, V. V. Estrela, "Attribute-based multiparty searchable encryption model for privacy protection of text data," *Multimedia Tools and Applications*, 2023. https://doi.org/10.1007/s11042-023-16818-4

[23] F. Yu, H. Shen, Q. Yu, X. Kong, P. K. Sharma and S. Cai, "Privacy protection of medical data based on multi-scroll Memristive hopfield neural network," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 2, pp. 845-858, 2023.

[24] D. Zhang, M. Shafiq, L. Wang, G. Srivastava, S. Yin, "Privacy-preserving remote sensing images recognition based on limited visual cryptography," *CAAI Transactions on Intelligence Technology*, 2023. https://doi.org/10.1049/cit2.12164

[25] G. Zhang, B. Liu, T. Zhu, M. Ding and W. Zhou, "Label-only membership inference attacks and defenses in semantic segmentation models," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 2, pp. 1435-1449, 2023.

[26] W. Zhang and X. Li, "Federated transfer learning for intelligent fault diagnostics using deep adversarial networks with data privacy," *IEEE/ASME Transactions on Mechatronics*, vol. 27, no. 1, pp. 430-439, 2022.

Biography

Jianjun Zhu biography. Jianjun Zhu is with School of Electronics and Electrical Engineering, Zhengzhou University of Science and Technology. His interests are deep learning, AI, image processing.

Jian'E Zhao biography. Jian'E Zhao is with School of Electronics and Electrical Engineering, Zhengzhou University of Science and Technology. His interests are deep learning, AI, image processing.

A Novel Capsule Network and Chaotic System Method for English Private Data Encryption

Yuqiang Wang
(Corresponding author: Yuqiang Wang)
School of Foreign Languages, Zhengzhou College of Finance and Economics
Zhengzhou 450000, China
Email: sarkozyteague@foxmail.com
(Received Oct. 22, 2023; Revised and Accepted Feb. 7, 2024; First Online Feb. 23, 2024)
The Special Issue on Data Fusion, Deep Learning and Optimization Algorithms for Data Privacy Protection
Special Editor: Prof. Shoulin Yin (Harbin Institute of Technology)

Abstract

Data encryption is a way of information transmission used to protect the security of data information. The using of data encryption technology can encrypt the data transmission process; it can suppress the attack of viruses or illegal personnel, and effectively protect data security. In order to ensure the security of English private data and avoid data leakage during the attack, this paper proposes a novel capsule network and chaotic system method for English private data encryption. The capsule network is used to incorporate the correlation and dependency between features into the data classification basis to realize multi-level feature extraction. After the encryption key of English private data is designed, feature clustering and encoding fusion are used to encrypt English private data automatically. Experimental results show that the data encryption method in this paper can effectively resist attacks.

Keywords: Capsule Network; Chaotic System; Data Encryption; Encoding Fusion; Feature Clustering

1 Introduction

Data masking, data subset, and data editing technologies are specifically designed to reduce the exposure of sensitive data in applications. These technologies play a vital role in meeting the related anonymization and pseudonymisation requirements of regulations such as the EU GDPR. The EU GDPR builds on widely accepted established privacy principles, such as purpose limitation, legality, transparency, integrity and confidentiality. This reinforces existing privacy and security requirements, including those related to notification and consent, technical and operational security measures, and cross-border data transfers. To adapt to the new digitization, globalization, and data-driven economy, the GDPR also formalizes new privacy principles, such as accountability and data minimization. Under the General Data Protection Regulation (GDPR), a data breach can result in a company facing a fine of up to 4% of its global annual turnover or 20 million (EURO), whichever is higher. Businesses that collect and process data in the EU region need to consider and manage their data processing practices, including the following requirements [1, 4, 9].

- Data security. Organizations need to implement appropriate levels of security controls, including the adoption of technical and organizational security controls to prevent data loss, information leakage, or other unauthorized data processing operations. The GDPR encourages organizations to incorporate encryption, event management, and network and system integrity, availability, and resilience requirements into their security plans.

- Extend personal rights. Individuals have a higher level of control over their data, and ultimately a higher level of ownership. They also have a range of extended data protection rights, including data portability and the right to be forgotten.

- Data breach notification. Upon becoming aware of a data breach, businesses need to notify their regulators and/or affected individuals immediately.

- Security audit. The company shall record and maintain records of its safety practices, audit the effectiveness of its safety programs, and take corrective actions where appropriate.

English data information is extremely important privacy data in universities, and its good security should be guaranteed. Data privacy protection is a measure used to protect all private data in universities, so as to avoid the leakage of private data.

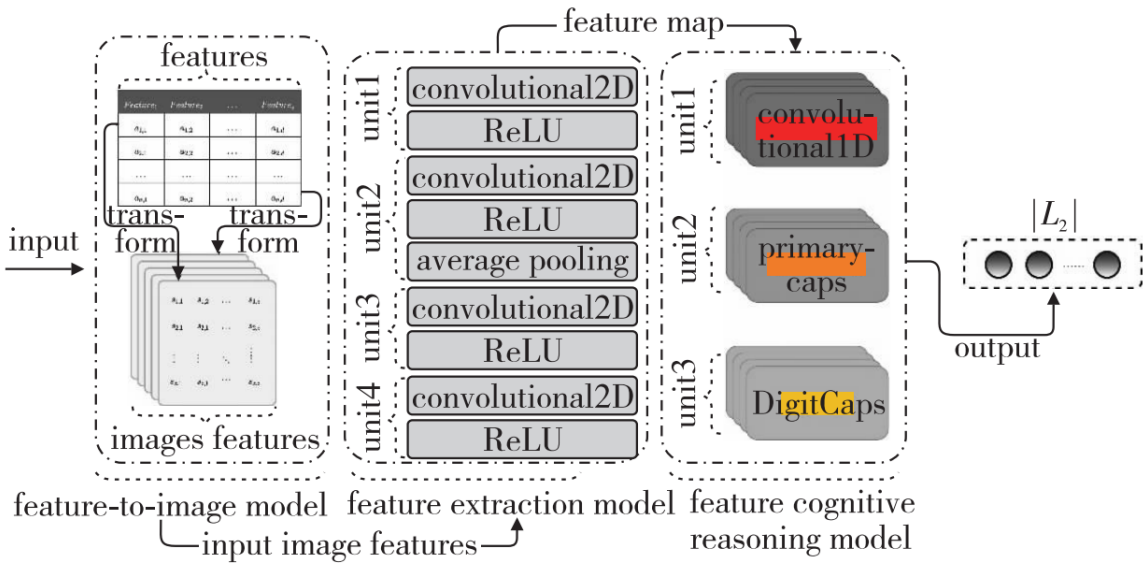


Figure 1: CapsMC model architecture

At present, English data needs to be transmitted between multiple related parties, and simply encrypting the communication equipment, path and other aspects can no longer meet the current data encryption requirements, and data leakage often occurs. After analyzing the encryption problem of private data, Jia *et al.* [3] studied the encryption scheme based on differential privacy in order to realize the decryption of private data. Zhang *et al.* [17] proposed a cloud-assisted encryption scheme after analyzing the encryption requirements of English data. When the above encryption methods face different attacks in the encryption process, the data leakage risk still needs to be further verified, and there are problems such as complicated calculation process and unsatisfactory results. Therefore, this paper studies the English privacy data encryption method based on capsule network and chaotic system, which makes full use of the classification advantages of capsule network, and introduces chaotic sequence algorithm to complete the English data privacy encryption.

2 Proposed English Privacy Data Encryption Method

2.1 English Data Classification Based on Capsule Network

English data contains various types of encrypted data with a large amount of data, among which there are some non-private data. In order to ensure the efficiency and effect of data encryption [5,10] and avoid the encryption of non-private data, English data should be classified first, and private data should be automatically encrypted after the division of private data and non-private data is completed.

The capsule network model (CapsMC) is a model capable of processing large data sets and extracting high-dimensional features. The model can realize interpretability classification. The basic structure of the CapsMC model is shown in Figure 1. CapsMC model mainly includes three parts, which are F2I transformation model, feature extraction model and feature cognitive reasoning model. F2I transformation model is mainly used to convert structured data into image data. Feature extraction model is mainly used for preliminary feature extraction. The feature cognitive reasoning model is mainly used to quantify the correlation of the feature mapping output of the feature extraction model, carry on the further feature extraction, feature combination, and realize the category explainable prediction through the cognitive reasoning mechanism.

The core idea of the F2I transformation model proposed in this paper is to combine the characteristics of the RGB images stored in the computer, convert the feature vector of each representation instance in the structured data set into a grayscale image matrix, and then use the image classification method to classify the instance.

Let the eigenmatrix $F(a_{ij}) \in R^{n\times d}$ represent a structured data set. Two-dimensional matrix $X(s_{ij}) \in R^{z\times z}$ represents a grayscale image matrix. Where F_i represents the $i-th$ eigenvector. d represents the dimension of the eigenvector. z represents the dimension required by the image matrix to store the feature vector. $z=\sqrt{d}$ represents the $j-th$ feature of the $i-th$ eigenvector. s_{ij} represents the gray value of the image, then

$$X = F2I(F_i, d). \tag{1}$$

The feature extraction model adopts 4 groups of convolution layers, 1 group of pooling layers and 2 groups of fully connected layers, as shown in Figure 2. Group 1 and 2 convolutional layers use $5\times5\times64$ convolutional

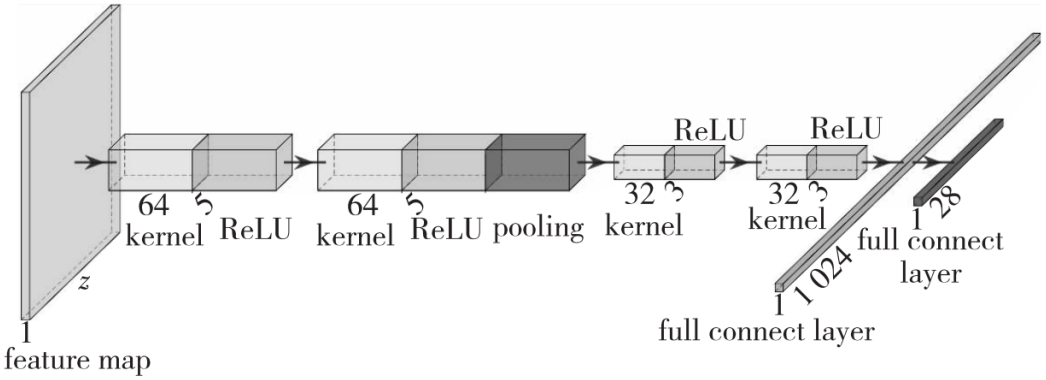


Figure 2: Feature extraction model

kernel and ReLU function as activation function [15]. For the third and fourth convolutional layers, $3 \times 3 \times 32$ convolutional kernels are used, ReLU functions are used as activation functions, average pooling is used for pooling layer to save more background information of image data, and the fully connected layer is used for feature fitting.

The convolutional layer extracts the features of the F2I model. Let the input layer l feature map be $\delta_i^l (i = 1, 2, \cdots, I)$, the output layer $l+1$ feature map be δ_i^{l+1}, the input convolution kernel be W_{ji}^{l+1}, and the size be $K \times K$, the output layer $1+1$ feature map be:

$$\delta_i^{l+1}(x, y) = \sigma(\sum_{i=1}^{I} W_{ji}^{l+1}(w, h) \times \delta_i^l(x - w, y - h)). \quad (2)$$

Where I is the depth of input feature mapping. J is the depth of the output feature mapping. (x, y) is the $x - th$ row $y - th$ column feature of the output feature map. (w, h) represents the features of row w and column h of the input feature map. $\sigma()$ is the activation function, and ReLU function is selected as the activation function in this paper.

Let the English data set be represented by Q, input it into the random forest algorithm, divide the data set by the regression number, and send it to the leaf node. To obtain the output y of the random forest regression model, the average value of the regression leaf nodes of l trees is selected. The detailed steps are as follows.

1) A subsample matrix is randomly selected in Q, represented by Q_z, which is defined as the training sample of the regression root node of the $v - th$ tree, and $v = 1, 2, \cdots, l$. The two samples Q and Q_z have the same size and are both matrices with dimension $m_d \times n_d$, where the number of variables is represented by na, and the number of data samples contained in any single variable is represented by n_d. The expression for Q and Q_z is:

$$Q = (x_1, x_2, \cdots, x_{n_d}). \quad (3)$$

$$Q_z = (x_{z1}, x_{z2}, \cdots, x_{zn_d}). \quad (4)$$

2) Q_z is treated by branching growth, where w variables are randomly obtained, and $w \ll n_d$; On this basis, the value of w with quantity e is randomly selected to get the cutting point matrix X_{cut}. Its expression is:

$$X_{cut} = (x_1, x_2, \cdots, x_w). \quad (5)$$

The dimension of matrix X_{cut} is $e \times w$. The elements of this matrix are represented by x_{kf}, $k = 1, 2, \cdots, e$, $f = 1, 2, \cdots, w$.

To solve the optimal cut $C(x_{kf})$ in the matrix X_{cut}, the formula is:

$$C(x_{kf}) = \frac{A + B}{M_1 + M_2}. \quad (6)$$

$$A = \sum_{y_n \in R_{left}(k,f)} (y_n - c_1)^2. \quad (7)$$

$$B = \sum_{y'_n \in R_{right}(k,f)} (y'_n - c_2)^2. \quad (8)$$

$$c_1 = \frac{1}{M_1} \sum_{y_n \in R_{left}(k,f)} y_n. \quad (9)$$

$$c_2 = \frac{1}{M_2} \sum_{y'_n \in R_{right}(k,f)} y'_n. \quad (10)$$

In the formula, after x_{kf} is cut, the left and right subtree sets are represented by $R_{left}(k, f)$ and $R_{right}(k, f)$ respectively. The number of samples contained in the two is expressed by M_1 and M_2. The calculation results of Formula (6) are filtered to obtain the x_{kf} point corresponding to the minimum value. If $Q_z(g, f) < x_{kf}$, which means that all invariants in line g of Q_z are divided into $R_{left}(k, f)$. If $Q_z(g, f) \geq x_{kf}$, it is divided into $R_{right}(k, f)$. After dividing the two subtree sets, the corresponding matrix Q_{left} and Q_{right} can be obtained respectively.

3) The node path length h_d and sample size s of Q_{left} and Q_{right} are recorded. If h_d of the two reaches the height of the tree or s is less than the set threshold, the branch growth of the node is stopped. Otherwise, it continues to grow.

4) Repeat the above steps to complete the construction of regression trees with a number of l trees, so as to complete the construction of random forest regression model.

2.2 Chaotic Key Encoding

After obtaining $x_1, x_2, \cdots, x_{M\times N}$, the binary optimization method is adopted to encode it, and the homogeneous distribution feature quantity of data encoding is obtained. The formula is:

$$m(c) = j + \frac{s(n) + h_i(t)}{s}. \tag{11}$$

Where, $h_i(t)$ represents the chaotic random sequence fusion operator of English private data. When $t = 2$, $s(n)$ represents a linearly extended key protocol for encoding English data. j represents the amplitude of the fluctuation. s stands for sequence distribution field.

The temporal feature distribution set of English data is analyzed to complete the establishment of English privacy data encryption identification bits. The formula is:

$$q = \sum_{c=1} m(c) + ||s_i + x_{n+1}|| + \psi. \tag{12}$$

Where, in the high-dimensional feature space, ψ represents the embedded dimension of English privacy data, so as to complete the chaotic key encoding of English data.

After the chaotic key encoding of English data, the key control method is used to complete the key design in the encryption process of English private data [12], and the automatic encryption of English private data is realized through feature clustering and coding fusion [14]. The encoding fusion formula is as follows.

$$b(u) = q^n + s_i + \psi. \tag{13}$$

In the formula, $\psi > 0$ represents the kernel function, and the value is encrypted to obtain the encoded chaos matrix, represented by A, G, θ, and its constant $\varepsilon > 0$. On this basis, the chaotic key encoding of English data in the encryption process [8] is analyzed, and the feature distribution of chaotic sequence is obtained, and the formula is as follows.

$$T = \sum_{u=1} b(u) + (A + G + \theta) + \varepsilon. \tag{14}$$

On the basis of formula (14), the chaotic sequence feature analysis model of English private data is established, and the deep fusion algorithm is adopted to solve it. The encoded positive multiple solution [2] is obtained, which is represented by $f :\to V$, and the α-order performance H_∞ of the solution is obtained. A encoding protocol is established, and a random linear encryption method is used to obtain the clustering distribution feature set X^t of α, whose formula is.

$$X^t = p_o^i + |N + T| + \psi. \tag{15}$$

Where p_o^i represents the constraint parameter of the private data of financial statements in the transmission process; N is the boundary coefficient.

On the basis of the above formula, the chaotic encryption control function U of financial statement privacy data is obtained, and the formula is:

$$U = \beta + X^t + N. \tag{16}$$

Among them, $\beta > 0$ represents the distribution function. The formula of decryption key $z(i)$ on the receiving end is:

$$E_t = z(i) + \sum(U) + k_{ij}. \tag{17}$$

Where $z(i)$ represents the spatial distribution dimension of privacy data in financial statements. k_{ij} indicates the characteristic quantity of key distribution.

2.3 Model Training

In order to make the model training effect significant, the loss function of CapsMC model adopts the edge loss function, limiting the upper boundary of the edge to m^+ and the lower boundary to m^-. Suppose that the probability sample obtained by CapsMC model is:

$$v_1, v_2, \cdots, v_j, \cdots, v_n. \tag{18}$$

Where $v_j \in R^c, j = 1, 2, \cdots, n$. v_j is a c-dimensional probability capsule. c is the number of categories. n is the number of samples. These probability samples are all linearly separable in c-dimensional space, i.e. there is hyperplane:

$$g(x) = x_1^2 + x_2^2 + \cdots, x_c^2 = m^2. \tag{19}$$

So that all probability samples can be separated without error. Where $x_i \in R^c$ is the coordinates of the probability capsule v_j in the c-dimensional space vector, and is also the probability value of predicting a certain class. m stands for boundary. If the class predicted by the probability sample exists, the predicted probability sample value is greater than or equal to m^+; if the class predicted by the probability sample does not exist, the predicted probability sample value is less than or equal to m^- Then the decision function is:

$$\left\{ \begin{array}{l} \sqrt{x_1^2 + x_2^2 + \cdots, x_c^2} \geq m^+ \\ \sqrt{x_1^2 + x_2^2 + \cdots, x_c^2} \leq m^- \end{array} \right\} \tag{20}$$

Where m^+ is the upper bound of the edge; m^- is the lower bound of the edge. c refers to the category of prediction probabilities.

According to the least square error criterion, the minimum square error loss from probability sample to edge is $|m - \sqrt{|g(x)|}|^2$.

For the edge lower bound, the loss that does not exist in the class predicted by the probability sample is calculated as:

$$\sum_j min(0, m^- - \sqrt{|g(x)|})^2. \tag{21}$$

It is equivalent to:

$$\sum_j max(0, \sqrt{|g(x)|} - m^-)^2. \tag{22}$$

For the edge upper bound, the loss of the existing probability sample is calculated as:

$$\sum_j min(0, \sqrt{|g(x)|} - m^+)^2. \tag{23}$$

It is equivalent to:

$$\sum_j max(0, m^+ - \sqrt{|g(x)|})^2. \tag{24}$$

In the process of model training, there will be a problem of class sample proportion imbalance, so a weight factor is added to adjust the proportion of class presence and class absence. The final loss function is:

$$CapsMC - loss = \sum_j I_j \cdot A + \lambda(1 - I_j) max(||v_j||). \tag{25}$$

Here, $A = max(0, m^+ - ||v_j||)^2$ The general learning process of CapsMC model is shown in Algorithm 1. In the process of model training, the model first converts the structured data set into image data set through F2I transformation model, and divides the data set according to the proportion that the training set accounts for 80% of the total sample and the test set accounts for 20% of the total sample. The segmented data set is input into the feature extraction model, and the output of the feature extraction model is the input of the feature cognitive inference model. The characteristic cognitive reasoning model outputs the possible probability of each category, and selects the one with high probability as the prediction category by comparing the probability, so as to realize the category prediction.

3 Testing Analysis

In order to test the effect of this method on the automatic encryption of English private data, it is applied to the automatic encryption of private data in a final English exam of a university. The data size is 40Gbit. Private data is 22Gbit and non-private data is 18Gbit. The two types of data are unbalanced. The data needs to be transferred between different departments, and the risk of data leakage is high.

Algorithm 1 CapsMC model training process

1: **Input:** Data set in row n and column d, training times *epochs*.
2: **Output:** Predicted category.
3: Initializing data set $\hat{X}$.
4: **while** $r \leftarrow 1, 2, \cdots, n$ **do**
5: The r row of data set is selected and converted into gray image matrix X by F2I model.
6: X is added into $\hat{X}$.
7: Dividing $\hat{X}$ into the training set and the test set.
8: **end while**
9: **while** $epoch \leftarrow 1, 2, \cdots, epochs$ **do**
10: Training CapsMC models using training sets.
11: Using CapsMC_Loss to calculate the model training loss and update the model parameters.
12: The model is validated using test sets.
13: **end while**
14: Comparing the probabilities of the output for each category and output the predicted results.
15: End

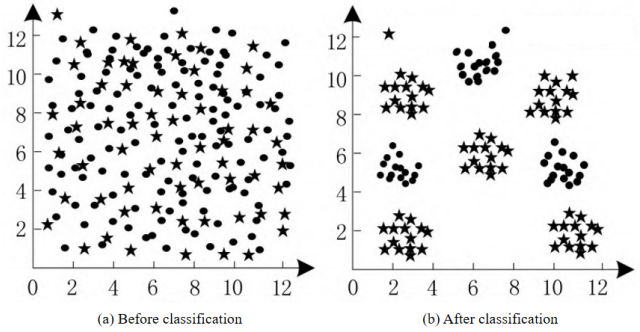


Figure 3: The results of English data distribution in two-dimensional space

English data contains non-private data, so before encrypting private data, it is necessary to classify it, and the classification effect directly affects the encryption efficiency of private data. In order to measure the classification effect of the proposed method on private data, the distribution results of data before and after classification in two-dimensional space are obtained, as shown in Figure 3.

According to the test results in Figure 3, the following results can be obtained: (1) Before the original English data is classified, the two kinds of data, private and non-private, are cross-mixed; (2) After classification, the two types of data are effectively divided, and there is no cross mixing between private data and non-private data after classification, and the classification effect is good.

In the process of implementing encryption, the method in this paper needs to generate random chaotic sequences, whose randomness directly affects the encryption effect of private data. Therefore, the randomness of chaotic sequences is used to measure the encryption performance of the method in this paper, and its chaos is described

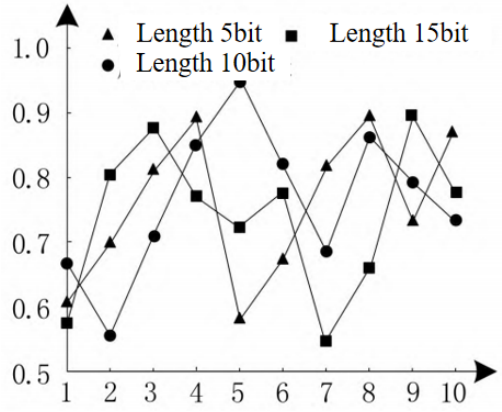


Figure 4: Lyapunov results

by Lyapunov index [13]. The index can effectively describe the randomness and chaos of chaotic sequences. If its value is greater than 0.01, the randomness is good. The privacy data was divided into 10 groups, and the Lyapunov index test results for each group of data were calculated, as shown in Figure 4.

According to the test results in Figure 4, under different chaotic sequence lengths, the Lyapunov index of 10 groups of privacy data is all above 0.52, among which the maximum Lyapunov index reaches 0.94, and the change of sequence length has no influence on the Lyapunov index. Therefore, the method in this paper has good application performance, can generate chaotic sequences randomly, and achieve a larger value range of chaotic sequences, can obtain more effective keys, and improve the encryption effect.

To test the encryption performance of the proposed method, the correlation coefficient is used as the measurement standard. The closer the value is to 0, the smaller the correlation between the leaked data, the lower the risk of data leakage, and the better the encryption effect. On the contrary, if the correlation coefficient is closer to 1, it means the greater the correlation between the leaked data, the greater the risk of data leakage, and the worse the encryption effect [6, 7]. The calculation formula is as follows:

$$\Upsilon = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}. \tag{26}$$

Where $cov(x,y)$ represents the covariance value between adjacent data. The variance values of the data x and y are represented by $\sqrt{D(x)}$ and $\sqrt{D(y)}$, respectively.

According to the above formula, the correlation coefficients of encrypted data under different chaotic random sequence lengths obtained by the proposed method are listed in Table 1.

According to the test results in Table 1, it can be concluded that under different chaotic random sequence lengths and with the gradual increase of data imbalance,

Table 1: The correlation coefficient between encrypted data sets

Unbalance degree/%	5bit	10bit	15bit
2	0.044	0.042	0.053
4	0.035	0.036	0.040
6	0.032	0.040	0.037
8	0.047	0.077	0.088
10	0.060	0.087	0.095
12	0.073	0.092	0.087
14	0.068	0.066	0.078
16	0.088	0.080	0.098

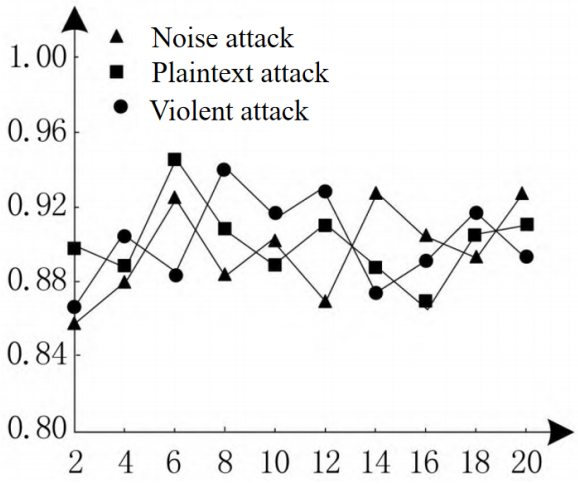


Figure 5: The anti-attack effect of proposed method

the correlation coefficients between private data after encryption by the method in this paper are all below 0.1, the highest correlation coefficient is 0.098, and the minimum correlation coefficient is 0.032. Because the linear extended key protocol is adopted in the encryption process, the correlation between all private data can be reduced to the greatest extent, and the encryption effect of English data can be better guaranteed.

In order to test the anti-attack effect of the proposed method in the encryption process, the user response value is used as the measurement standard. The value of this index ranges from 0 to 1. The closer the value is to 1, the better the anti-attack effect is. Figure 5 shows the results of user response values when the method in this paper is confronted with three kinds of attacks under different encrypted data quantities.

Further, we compare the time cost of the proposed method and the other two schemes (Reference [11] and Reference [16]) on mobile phones and sensors, as shown in Table 2 and Table 3 respectively. Since Reference [11] and Reference [16] schemes do not involve fog nodes, the encryption time of these two schemes on fog nodes is 0, while the encryption time of the scheme in this paper in-

creases with the increase of the number of attributes and the number of professional categories in the professional access policy. As shown in Table 2 and Table 3, the encryption time of the phone and sensor increases with the number of attributes. Among the three schemes, the encryption time of shared data is the least. At the same time, the encryption time of the proposed scheme is about 1/3 times that of the other two schemes under the same number of attributes. As we can see from the tables, sensor encryption takes longer than phone encryption. When 20 attributes are defined in the access policy, the data encryption on the sensor in Reference [16] is close to 45s, while at this time, the scheme in this paper only consumes 16s, which greatly reduces the calculation time.

Table 2: The encryption time of the phone/s

Attribute number	[11]	[16]	Proposed
5	6	4	2
10	9	5	3
15	13	7	4
20	19	10	5
25	24	14	7
30	31	19	12

Table 3: The encryption time of the sensors/s

Attribute number	[11]	[16]	Proposed
5	10	6	3
10	14	8	5
15	17	11	6
20	24	16	8
25	32	22	12
30	47	26	18

4 Conclusions

In order to realize the security of private data in English teaching, this paper studies the automatic encryption method of English private data based on capsule network, and tests the application performance and effect of this method. The results show that the encryption method studied in this paper can reliably divide private data and non-private data in English data, and provide a reliable basis for private data encryption. In addition, the method has excellent randomness and can generate chaotic sequences in a wider range to ensure the diversity of keys. Meanwhile, its encryption performance is good, and the correlation between private data can be greatly reduced after encryption. In the face of different attacks, it can quickly complete the encryption response, ensure the reliable encryption of English private data, and provide a reliable guarantee for the security management of the university.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] J. Domingo-Ferrer, O. Farras, J. Ribes-González, D. Sánchez, "Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges," *Computer Communications*, vol. 140, pp. 38-60, 2019.

[2] O. Dubrovsky, G. Levitin, M. Penn, "A genetic algorithm with a compact solution encoding for the container ship stowage problem," *Journal of Heuristics*, vol. 8, pp. 585-599, 2002.

[3] B. Jia, X. Zhang, J. Liu, Y. Zhang, K. Huang, Y. Liang, "Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4049-4058, 2021.

[4] K. Lee, Y. Lai, S. Chen, Y. Lin, M. Tsai, "The design of access control by using data dependency to reduce the inference of sensitive data," *2020 International Conference on Technologies and Applications of Artificial Intelligence (TAAI). IEEE*, pp. 68-72, 2020.

[5] H. Li, L. Teng and S. Yin, "A new bidirectional research chord method based on bacterial foraging algorithm," *Journal of Computers (Taiwan)*, vol. 29, no. 3, pp. 210-219, 2018.

[6] Z. Man, J. Li, X. Di, R. Zhang, X. Li, X. Sun, "Research on cloud data encryption algorithm based on bidirectional activation neural network," *Information Sciences*, vol. 622, pp. 629-651, 2023.

[7] K. Munjal, R. Bhatia, "A systematic review of homomorphic encryption and its contributions in healthcare industry," *Complex & Intelligent Systems*, vol. 9, no. 4, pp. 3759-3786, 2023.

[8] P. Naskar, S. Bhattacharyya, K. Mahatab, K. Dhal, A. Chaudhuri, "An efficient block-level image encryption scheme based on multi-chaotic maps with DNA encoding," *Nonlinear Dynamics*, vol. 105, pp. 4, pp. 3673-3698, 2021.

[9] J. Smedt, A. Yeshchenko, A. Polyvyanyy, J. D. Weerdt, J. Mendling, "Process model forecasting and change exploration using time series analysis of event sequence data," *Data & Knowledge Engineering*, vol. 145, 2023.

[10] L. Teng, H. Li, J. Liu, S. Yin, "An efficient and secure cipher-text retrieval scheme based on mixed homomorphic encryption and multi-attribute sorting method under cloud environment," *International*

Journal of Network Security, vol. 20, no. 5, pp. 872-878, 2018.

[11] S. Yadala, C. Pundru, V. Solanki, "A novel private encryption model in iot under cloud computing domain," in *The International Conference on Intelligent Systems & Networks. Singapore: Springer Nature Singapore*, pp. 263-270, 2023.

[12] X. Yan, X. Wang, Y. Xian, "Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation," *Multimedia Tools and Applications*, vol. 80, pp. 10949-10983, 2021.

[13] G, Ye, M, Liu, M. Wu, "Double image encryption algorithm based on compressive sensing and elliptic curve," *Alexandria engineering journal*, vol. 61, no. 9, pp. 6785-6795, 2022.

[14] M. Yildirim, "Optical color image encryption scheme with a novel DNA encoding algorithm based on a chaotic circuit," *Chaos, Solitons & Fractals*, vol. 155, 2022.

[15] S. Yin, L. Meng and J. Liu, "A new apple segmentation and recognition method based on modified fuzzy c-means and hough transform," *Journal of Applied Science and Engineering*, vol. 22, no. 2, pp. 349-354, 2019.

[16] M. Zhang, J. Liu, K. Feng, F. Beltran, Z. Zhang, "SmartAuction: A blockchain-based secure implementation of private data queries," *Future Generation Computer Systems*, vol. 138, pp. 198-211, 2023.

[17] Z. Zhang, L. Zhang, Q. Li, K. Wang, N. He, T. Gao, "Privacy-enhanced momentum federated learning via differential privacy and chaotic system in industrial Cyber-Physical systems," *ISA transactions*, vol. 128, pp. 17-31, 2022.

Biography

Yuqiang Wang biography. Yuqiang Wang is with the School of Foreign Languages, Zhengzhou College of Finance and Economics. Research interests: English data processing, English for Specific Purposes, English Education.

A Novel Nodes Data Security Communication Model of Internet of Vehicles Based on Mobile Edge Computing

Zengyong Xu

(Corresponding author: Zengyong Xu)

School of Automobile & Henan College of Transportation

No. 259 Tonghui Road, Baisha Vocational Education Park, Zhengdong New District, 451460 Zhengzhou, China

Email: zxcvfdsa5024@foxmail.com

(Received Oct. 24, 2023; Revised and Accepted Feb. 7, 2024; First Online Feb. 23, 2024)

The Special Issue on Data Fusion, Deep Learning and Optimization Algorithms for Data Privacy Protection

Special Editor: Prof. Shoulin Yin (Harbin Institute of Technology)

Abstract

Internet of Vehicles involves data acquisition, processing, and decision-making, requires a lot of computing and storage resources, and is extremely sensitive to delay. Although traditional cloud computing can compensate for the lack of computing resources of onboard equipment, due to the huge amount of data transmitted, there will be a large transmission delay from onboard equipment to the cloud, which cannot meet the delay requirements of onboard services. Therefore, mobile edge computing is introduced into the Internet of Vehicles as a general trend. By deploying mobile edge computing devices in roadside units and other locations, the problem of insufficient vehicle computing resources can be effectively solved, and the real-time processing of vehicle networking services can be realized. In order to solve the problems of excessive physical load and high data security risk in the central entity of vehicle networking communication architecture, this paper proposes a novel nodes data security communication model of the Internet of Vehicles based on mobile edge computing. The "vehicle-edge-cloud" collaborative network architecture based on 5G is built, in which various emerging technologies, such as software-defined networks, are integrated to achieve unified scheduling of vehicles, edge equipment, and cloud resources. Then, based on the practical Byzantine fault-tolerant consensus mechanism, an improved dynamic, practical Byzantine fault-tolerant mechanism is proposed. Finally, the data security communication model is evaluated, the characteristics of the data security communication model, the problems faced by vehicle nodes, and the solutions of the data security communication model are analyzed, and the model's effectiveness is proved with experiments.

Keywords: Byzantine Fault-Tolerant; Edge Computing; Internet of Vehicles; Nodes Data Security

1 Introduction

Internet of Vehicles (IoV) is one of the core technologies of intelligent networked vehicles. In IoV, vehicle nodes regularly broadcast information such as their current location, speed and acceleration to surrounding nodes, but this way poses a potential threat to vehicle data security. The existing IoV architecture is centralized, once the centralized entity is attacked, it will bring serious data security risks, resulting in identity, location and other privacy disclosure. With the rapid development of Internet of Things technology, the data volume of IoV nodes increases dramatically, and the central entity load is too large, facing the risk of single point failure. At the same time, the characteristics of high mobility and variability of IoV have brought great challenges to vehicle communication systems [6, 17, 19].

Blockchain technology is a completely distributed public database or ledger, with decentralization, transparency, tamper-proof and other characteristics, so domestic and foreign scholars proposed to introduce blockchain technology into the Internet of vehicles. For example, reference [20] designed independent blockchains with different functions according to the data type, and proposed a model for the outward transmission of vehicle blockchain data. Reference [1] proposed a permission-based blockchain model that managed the collected vehicle-related data. Reference [18] added a reward mechanism and proposed a semi-distributed peer-to-peer (P2P) network model. Reference [4] proposed a blockchain-based security data sharing model that encouraged vehicles to broadcast announcement messages and generate blocks. Based on the alliance chain, some scholars transfer the storage and computing of vehicles to the Road Side Unit (RSU). Reference [3] developed a P2P data sharing system to openly audit and store shared data and its shared records. Reference [16] proposed a

data security sharing and storage system based on alliance blockchain. Reference [8] realized the safe sharing of autonomous driving cloud control services and related data in an open environment. Some scholars divide blockchain networks into regions. Reference [14] divided the Internet of vehicles into several areas, each area set a public chain, and proposed a blockchain branch algorithm. Reference [15] designed vehicle networking as an alliance chain based on the city, and realized the data exchange among the alliance chains of vehicle networking in various cities.

This paper aims at problems such as difficult storage maintenance, low communication efficiency, and difficult real-time processing. A Date Security Communication Model (DSCM) based on mobile edge computing is proposed, which includes mobile edge computing design, node identity authentication, improved dynamic practical Byzantine fault-tolerant consensus algorithm, and vehicle security communication method. According to the urgency of the data, the data is divided into ordinary data and urgent data. Considering the motion of vehicle nodes, an improved and practical Byzantine fault-tolerant consensus algorithm is proposed.

This paper is organized as follows. In Section 2, we introduce the DSCM of IoV in detail. Simulation and result analysis is conducted in Section 3. There is a conclusion in Section 4.

2 DSCM of IoV

Based on IoV services, this paper designs a secure communication model with the help of mobile edge computing, including mobile edge computing design, node identity authentication, improved dynamic practical Byzantine fault-tolerant consensus algorithm and vehicle security communication method.

The whole link of the Internet of vehicles is composed of the Internet of vehicles alliance chain and a public chain. Considering the deployment of communication base stations, the entire IoV is divided into a cellular area. One blockchain is set for each region. These blockchains together form the Internet of Vehicles alliance chain. The IoV alliance chain is composed of all communication base stations and vehicle nodes in each region. At the same time, all communication base stations (5G) and roadside units and other edge side devices of IoV are collectively referred to as edge nodes [9]. All the edge nodes in the IoV constitute the public chain of the IoV as consensus nodes to realize the sharing of emergency data among various regions.

This paper divides IoV data into ordinary data and emergency data. Common data contains the basic safety data of the vehicle and is transmitted between the vehicles in the area. Emergency data, including special information such as traffic accidents and road congestion, is transmitted between regions and shared across the whole range through distributed broadcasting of vehicular communication and cloud computing. However, the following problems still need to be solved. First, how to design the block structure, data storage structure and node identity authentication mode of ordinary data and emergency data, and realize the verification of the authenticity and integrity of vehicle data; Second, how to realize the consensus of vehicle data effectively, eliminate malicious nodes, improve the consensus efficiency and shorten the consensus time; The third is how to realize the secure communication of data.

2.1 Mobile Edge Computing Design

Under the "vehicle-edge-cloud" cooperation architecture, it is assumed that vehicles share communication resources. The delay can be minimized by dividing tasks into multiple subtasks and uninstalling them in different locations.

When a new request arrives, the task is first divided into k subtasks, consisting of the k-dimensional vector $TA = (Tk_1, Tk_2, \cdots, Tk_k)^T$, where $Tk_i = \delta_i \cdot Tk$. Tk represents the total task data size in bits. δ_i indicates the proportion of subtasks in the total task. The number of CPU cycles required to compute Tk_i is $C_i = \rho \cdot Tk_i$. Where ρ is the complexity of the computational task. The unit of CPU cycles is *cycles*.

Based on this scheme, the total delay of unloading task mainly includes the time delay of data processing on the vehicle, MEC, cloud, and transmission queue delay during data upload. Since the time delay of the processed data back to the vehicle is small, it is ignored here.

1) Vehicle unloading delay. Vehicle unloading delay mainly includes unloading delay on source vehicle and V2V vehicle. IEEE802.11p protocol [11] in DSRC communication mode is used to communicate between vehicles in an independent co-distributed channel. Path loss can be defined as:

$$L_{V2V}^{dB} = 63.3 + 17.7log_{10}(d_{i,u_j}). \tag{1}$$

Where d_{i,u_j} represents the communication distance between vehicle u_i and vehicle u_j. When $i = j$, it indicates that the source vehicle is unloaded, and there is no path loss. We convert equation (1) into numerical form as follows:

$$L_{V2V} = 10^{-(L_{V2V}^{dB}/10)}. \tag{2}$$

Therefore, the data transfer rate between the two vehicles is:

$$r_{V2V} = B_{V2V}log_2(1 + \frac{p_i L_{V2V} h^2}{N_0}). \tag{3}$$

B_{V2V} represents the channel bandwidth allocated to V2V vehicles. p_i is the transmitting power of the vehicle equipment. p_i represents Gaussian white noise power. h indicates the channel fading factor of the upload link.

Then the delay in task i choosing to unload on the vehicle can be expressed as:

$$T_{i,u_j} = \frac{C_i}{C_{i,u_j}} + \frac{\mu \cdot Tk_i}{r_{V2V}} + \Delta T. \tag{4}$$

$\frac{C_i}{C_{i,u_j}}$ indicates the processing delay on the V2V. μ indicates the transmission cost factor of the upload link. ΔT indicates the queue waiting delay.

2) MEC unload delay. The vehicle communicates with the MEC device through the LTE-Advanced direct link [12]. If the upload link of the vehicle to the MEC(RSU) is set as the flat fast fading Rayleigh channel, the data transmission rate of the upload link is as follows:

$$r_{V2M} = B_{V2M} log_2(1 + \frac{p_i h^2 d_{i,e_j}^{-\varepsilon}}{N_0}). \tag{5}$$

B_{V2M} indicates the channel bandwidth allocated to the MEC. d_{i,e_j} is the distance between vehicle u_i and MEC device e_j. h represents the channel fading factor of the upload link. ε is the path loss factor. N_0 indicates Gaussian white noise power.

Then the unloading delay T_{i,e_j} on the MEC can be expressed as:

$$T_{i,e_j} = \frac{C_i}{C_{i,e_j}} + \frac{\mu \cdot Tk_i}{r_{V2V}} + \Delta T. \tag{6}$$

$\frac{C_i}{C_{i,e_j}}$ indicates the processing delay on the MEC. μ indicates the transmission cost factor of the upload link. ΔT indicates the queue waiting delay.

3) Cloud uninstallation delay. If the upload link is still set to a flat frequency fast fading Rayleigh channel, the data transmission rate of the upload link is:

$$r_{V2C} = B_{V2C} log_2(1 + \frac{p_i h^2 d_{i,0}^{-\varepsilon}}{N_0}). \tag{7}$$

Where, B_{V2C} represents the channel bandwidth allocated to the cloud. $d_{i,0}$ is the distance between vehicle u_i and the remote cloud.

Then the uninstallation delay $T_{i,0}$ on the remote cloud is:

$$T_{i,0} = \frac{C_i}{C_{i,0}} + \frac{\mu \cdot Tk_i}{r_{V2C}} + \Delta T. \tag{8}$$

$\frac{C_i}{C_{i,0}}$ indicates the processing delay on the cloud. μ indicates the transmission cost factor of the upload link. ΔT indicates the queue waiting delay. In summary, the uninstallation delay of subtask i can be expressed as:

$$t(Tk_i) = \alpha_i[\lambda_i T_{i,e_j} + (1-\lambda) T_{i,0}]. \tag{9}$$

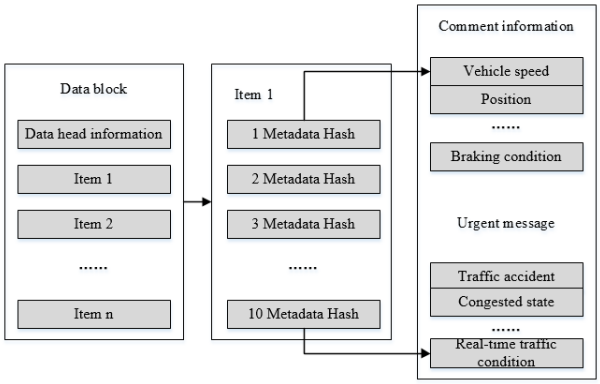


Figure 1: Data storage structure

Where α decides whether to unload the task onto the vehicle. λ_i decide whether to uninstall in MEC or in the cloud. The total task response delay is equal to the maximum value of the subtask unload delay, namely:

$$t(TA) = maxt(Tk_1), t(Tk_2), \cdots, t(Tk_k). \tag{10}$$

In order to keep the response delay as small as possible, equation (10) is modeled as the following optimization problem:

$$mint(TA), TA \in I. \tag{11}$$

Where, I is the search range of the feasible solution.

2.2 Data Storage Structure

As shown in Figure 1, in order to ensure that the recorded content is trustworthy and untampered, the model records the hash values of all data and stores them in a hierarchical structure. A Data Block consists of a header and multiple data entries. The header information contains the timestamp and hash value of the data block, which can reduce the computational cost of verification and facilitate the propagation of the data block in the blockchain network. Each data entry contains a timestamp t, the data owner's public key P_k, metadata, and a data Hash. Among them, metadata is common data or emergency data: common data includes the vehicle's position, speed, direction, braking state, effective time and other basic safety information; Emergency data includes special information such as traffic accidents, road congestion, real-time road conditions, and effective time. The size of each piece of data does not exceed 1 KB. According to the previous three information, calculate and store the hash value of this data to facilitate the hash check of other nodes, so as to speed up the node's check on the block and reduce the search space.

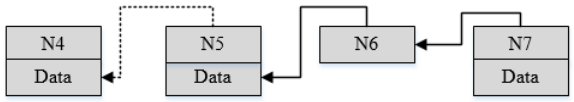


Figure 2: Node data update

2.3 Node Data Update

Due to the infinite redundancy of the blockchain, each node backs up all the information of the blockchain network, consuming a lot of power, which is difficult to operate and maintain in the network environment of the Internet of vehicles. In addition, a large amount of data is generated during vehicle communication, which requires a large data server to manage and store data for a long time. Therefore, according to the real-time and mobility of the Internet of vehicles, on each blockchain node, only the data of the blockchain network in the current area is backed up. When a vehicle node moves from one area to another, the blockchain information in the original area is deleted, and the blockchain information and data of the current regional network are updated and downloaded. When the vehicle node storage reaches the threshold, the validity period of the block is determined from the beginning. As shown in Figure 2, if a block in the blockchain expires, the entire block is deleted; If the block in the blockchain is not expired and the memory is insufficient, in order to protect the integrity and authenticity of the block, the data of the block is deleted first, and only the hash value of the block is retained.

2.4 Packet Format

The data sent by the vehicle includes the data owner's public key Q, metadata m, digital signature S, data hash value $h(m)$(SHA256), and timestamp t. As shown in Table 1, the packet that should be sent is $M_{sig}Q|S|t|m|h(m)$.

Table 1: Typical states of SEIR model

Content	Q	m	S	h(m)	t
Length	65	changeable	changeable	256	13

2.5 Node Identity Authentication

User authentication and privacy are two important issues in IoV. This paper adopts a node authentication scheme based on cloud server and blockchain. The IoV nodes (vehicle nodes and edge nodes) send registration requests to the Certificate Authority (CA) responsible for issuing certificates before starting to join the network. The cloud server is responsible for storing and managing node factory information and real identity, facilitating authentication during node registration, and managing node pseudonyms issued by the CA. When a node is registered in a system with a real identity, it gets a certificate issued by a CA that includes a pseudonym, a pair of public and private keys, and two hashes. In the certificate issued by the CA for the node, the real identity of the node is hidden, which can protect the privacy of the node, and the malicious node can be traced according to the hash value of the pseudonym+public key and the hash value of the real name+certificate.

In the blockchain network, the vehicle networking node will save the information of the nodes communicated within a certain period of time in its communication list, which is the trust list. If the node information in the list is out of the time range, it will be deleted. The trust list can be updated between edge nodes and between edge nodes and vehicle nodes. When a vehicle node moves to another zone, the zone in which the node is currently located sends a verification request on behalf of the node to the previous zone and its surrounding zone (excluding the current zone). Among them, as long as the information of the vehicle node can be queried in the communication list of 1 edge node or n vehicle nodes in the verification group, it is considered to pass the verification of the area. If the vehicle node passes the verification of the region where it is located before crossing the zone, and fails to pass in the surrounding zone (excluding the current zone and the previous zone), it indicates that the vehicle node has uniqueness, that is, it is considered that the identity verification of the vehicle node is successful, and it can participate in data communication. If the above conditions are not met, the right of the vehicle node to participate in the data communication is revoked, and after a period of time the above verification process is repeated until the authentication of the vehicle node is completed. When a vehicle node joins the network for the first time, the region in this region sends verification requests to the verification groups of other regions on behalf of the node. If the verification fails in each region, the uniqueness of the vehicle node is proved, that is, the authentication of the vehicle node is considered successful; otherwise, it cannot participate in data communication.

In short, through the identity authentication of the cloud server and the identity authentication between nodes, the network of vehicles nodes can be allowed to carry out effective data communication, thereby reducing the dependence on CA in the traditional authentication scheme, effectively detecting and preventing the entry of malicious nodes, and protecting the identity privacy of nodes.

2.6 Improved Dynamic Practical Byzantine Fault-tolerant Consensus Mechanism

The consistency protocol, view switching protocol and checkpoint protocol proposed by Practical Byzantine Fault Tolerance (PBFT) algorithm [2] can realize data update and fault-tolerant recovery, and make blocks reach

agreement in the whole network. Compared with the Proof of work (PoW) mechanism, this mechanism can not only meet the demand of short response time in terms of efficiency, but also solve the problem of historical message storage of each node, and can be fault-tolerant recovery when malicious nodes invade. However, because nodes in the network of vehicles can move quickly and generate more data in real time, consensus needs to be reached quickly. Therefore, based on PBFT consensus mechanism, a dynamic regional consensus mechanism composed of intra-regional consensus mechanism and multi-regional consensus mechanism is proposed.

Based on the partitioning strategy, the intra-region consensus mechanism randomly selects the regional representative node among the edge nodes, and selects the primary node among the regional representative nodes. The election method of the primary node is $p = v \cdot f(R)$, where p is the number of the primary node, v is the view number (the number of current blocks), R is the total number of edge nodes in the region, and f is the complementary function. The nodes represented by other regions serve as replica nodes. If the primary node has malicious behaviors, the primary node is selected from the replica node. According to the master node, the intra-region consensus mechanism uses the original consistency protocol of PBFT to complete the block consensus.

The multi-regional consensus mechanism also relies on the previous mechanisms. However, considering that under the multi-region consensus mechanism, the number of regional representative nodes participating in the block consensus far exceeds the number of nodes in the intra-region consensus mechanism, in order to improve the efficiency of the consensus mechanism and shorten the data update time, the consistency protocol and view switching protocol are simplified [13].

In the simplified consistency protocol, the primary nodes of each region form the primary node group, send the preparatory message to the representative nodes of other regions, the regional representative nodes receive and process the preparatory message, and send the acknowledgement message to the primary node group. If the number of acknowledgement messages received by the primary node group exceeds f_2 (f_2 is 1/3 of the number of regional representative nodes), the primary node group sends the acknowledgement messages to other regional representative nodes for verification. If the zone representative node is authenticated, the authentication message is sent to the primary node group. If the number of verification success messages received by the master node group exceeds, the consensus is reached and the block is written to the public chain of the Internet of vehicles. The simplified view switching protocol is mainly aimed at choosing one of the duplicate nodes to replace the current master node when the master node is a malicious node, and continuing to complete the current consensus. This method can not only avoid the risk of transaction delay caused by malicious nodes building blocks as master nodes, but also meet the needs of IoV.

2.7 Data Security Communication Implementation

Considering the existence of common data and emergency data in vehicle networking data, a secure communication method for different data is proposed. The exchange of vehicles' own routine data between vehicles is a common message, which is mainly realized through vehicle-vehicle communication in the region. When there is emergency data, the data needs to be broadcast to vehicles in other areas, which needs to be realized through vehicle and road communication, that is, the edge node can directly broadcast the emergency data to nearby vehicle nodes, and at the same time send the emergency data to the cloud server, which will coordinate and find the edge nodes in other areas of interest through big data. The edge node then sends emergency data to nearby vehicle nodes in its area. The flow of data security communication is shown in Figure 3.

3 Simulation and Result Analysis

In order to prove the superiority of the "vehicle-edge-cloud" cooperation architecture proposed in this paper and the offload strategy based on the proposed algorithm in terms of delay reduction, the delay performance of this architecture is simulated and compared with cloud and "edge-cloud" cooperation architecture, and the proposed algorithm is compared with BBM [10], SBO [5] and FLPA [7].

In a real IoV environment, the distance between each device and the bandwidth of the transmission link are time-varying, and the computing power of each MEC device and vehicle is not the same. The final simulation result is the average value obtained from multiple experiments.

Figure 4 and Figure 5 respectively simulate and compare the delay performance of the network architecture of "vehicle-side-cloud" collaboration, "edge-cloud" collaboration and cloud working alone based on the proposed algorithm under the influence of different task loads and different link bandwidths.

As can be seen from Figure 4, the task response delays of "vehicle-edge-cloud" collaboration, "edge-cloud" collaboration and cloud working alone in this paper all increase with the increase of task data. Among them, the "vehicle-side-cloud" collaboration has lower delay than the "edge-cloud" collaboration and cloud work alone. This is because the "vehicle-edge-to-cloud" collaboration comprehensively considers the computing capacity of the vehicle, MEC, and cloud, and realizes the effective regulation of each part of the resources. When the task data volume is 5Mb, the delay performance of "vehicle-edge-cloud" cooperation architecture is increased by 13.6% and 28.7% respectively compared with "edge-cloud" cooperation and cloud alone work. Therefore, the use of "vehicle-edge-cloud" collaborative architecture can effectively reduce the delay.

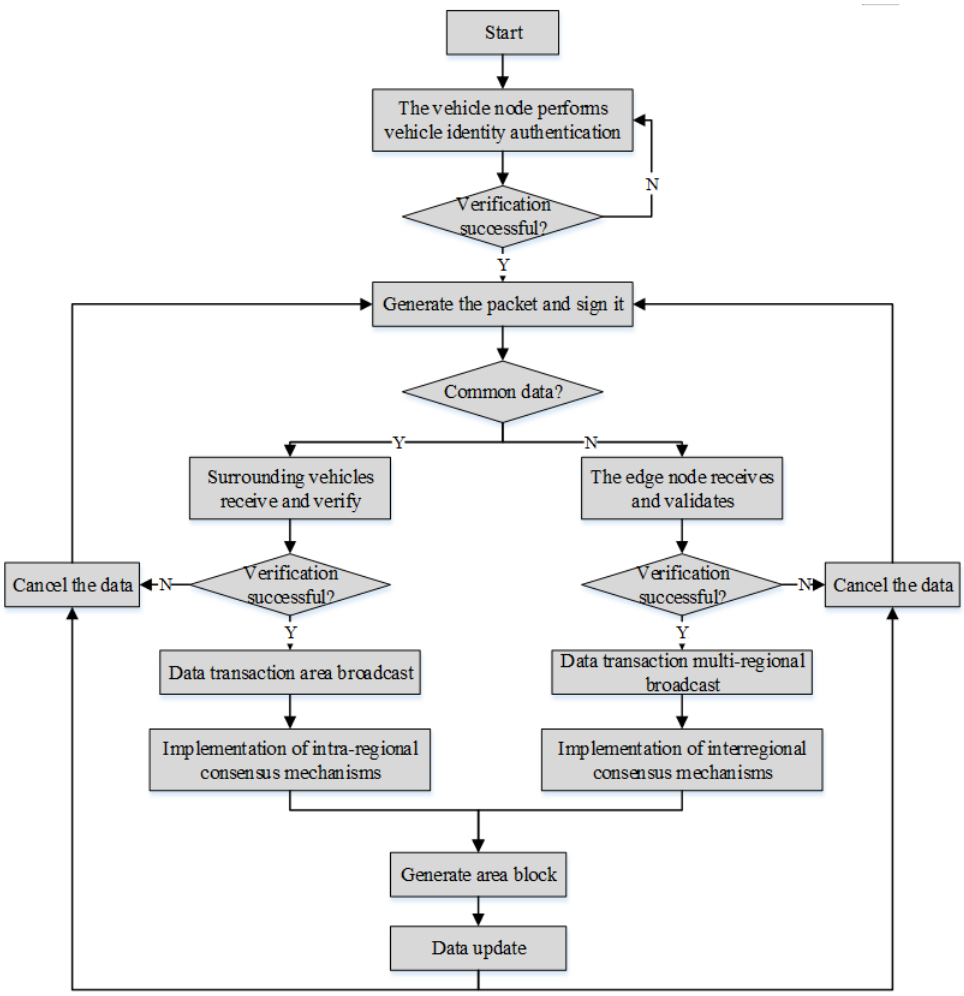


Figure 3: Processes for secure data communication

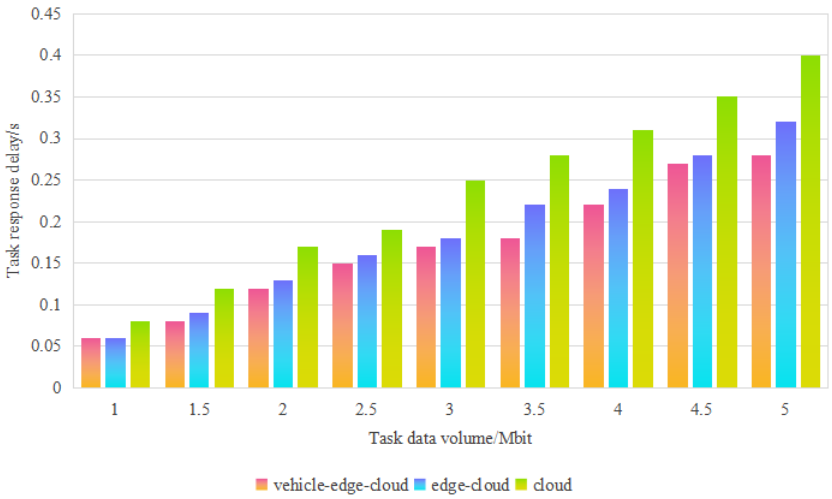


Figure 4: The effect of task volume on the performance of network architecture

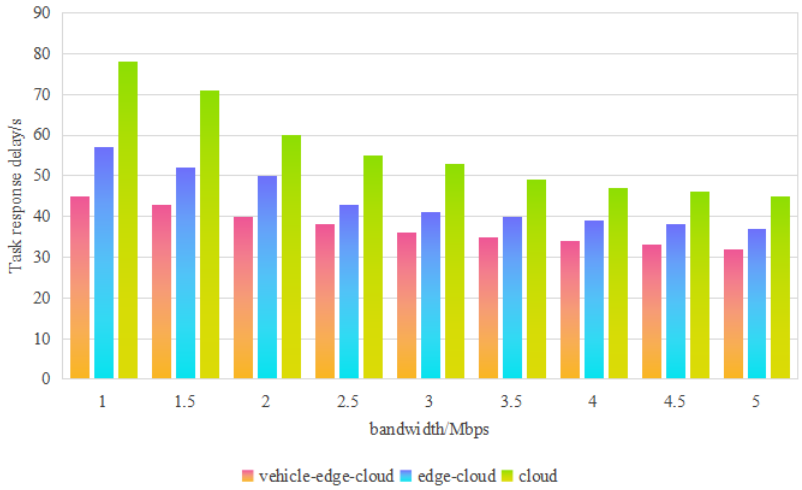


Figure 5: The performance impact of bandwidth on network architecture

Figure 5 is simulated when the bandwidth allocated to vehicle, MEC and cloud is the same, and the task volume is 1Mb. It can be seen that the response time of each architecture shows a decreasing trend when the bandwidth continues to increase, and the delay of cloud architecture is the most obvious. This is because in the cloud architecture, all data needs to be uploaded to the cloud for processing, and the transmission delay of the upload process will decrease significantly with the increase of bandwidth. However, in the other two architectures, due to the proximity of the vehicle and MEC devices to the data source, only a small amount of data transfer to the cloud does not result in a significant latency reduction. Moreover, compared with "edge-cloud" collaboration, the architecture proposed in this paper takes into account the computing power of the vehicle, MEC, and cloud, and the delay is lower. In summary, when the link bandwidth is limited, the "vehicle-edge-cloud" collaborative network architecture has obvious advantages in reducing delay.

In order to verify that in the "vehicle-edge-cloud" collaborative architecture, the proposed algorithm can effectively reduce the response delay, the simulation is compared with the delay performance of BBM, SBO and FLPA, and the simulation results are shown in Figure 6. As can be seen from Figure 6, as the amount of task data increases, the proposed algorithm has the most superior delay performance compared with the other three algorithms. This is because compared with algorithm BBM, this paper has a faster convergence speed. Compared with SBO and FLPA, the unloading strategy of this algorithm not only considers the unloading mode of V2V, but also schedules the computing resources of vehicle, MEC and cloud. When the task data volume is 5Mb, the delay performance of the proposed algorithm is improved by 10.9%,39.4% and 44.1%, respectively, compared with BBM, SBO and FLPA. Therefore, the application of this algorithm in the "vehicle-edge-cloud" collaborative architecture can effectively reduce the response delay of vehicle-connected services.

4 Conclusions

With the help of mobile edge technology, this paper solves the problems that the central entity load is too large and the data security risk is high in the existing vehicle networking architecture. Based on the mobile edge technology, the node data security communication model (DSCM) is proposed. The block structure of common data and emergency data is designed according to the real-time and mobility of vehicle networking, and the integrity and authenticity of data and block are verified by digital signature method. Secondly, a node authentication scheme based on cloud server and authentication group is adopted to solve user authentication and privacy problems. Then, on the basis of PBFT consensus mechanism, a dynamic and practical Byzantine fault-tolerant consensus algorithm is proposed to ensure the rapid consensus of the blockchain of the Internet of vehicles. Finally, by comparing with other communication models, the DSCM model has the characteristics of fast consensus, data security, privacy protection, lightweight storage, efficient communication, etc., which is more suitable for the current communication environment of IoV. In the future, we will utilize the proposed scheme to improve IoV and apply them in real applications.

Acknowledgments

This paper was supported by Project(Key scientific research Project of Henan Provincial Universities "Research on Key Technologies of Intelligent Networked Vehicle Virtual Simulation System for Real Traffic Scenes"), Project No. 23B580006.

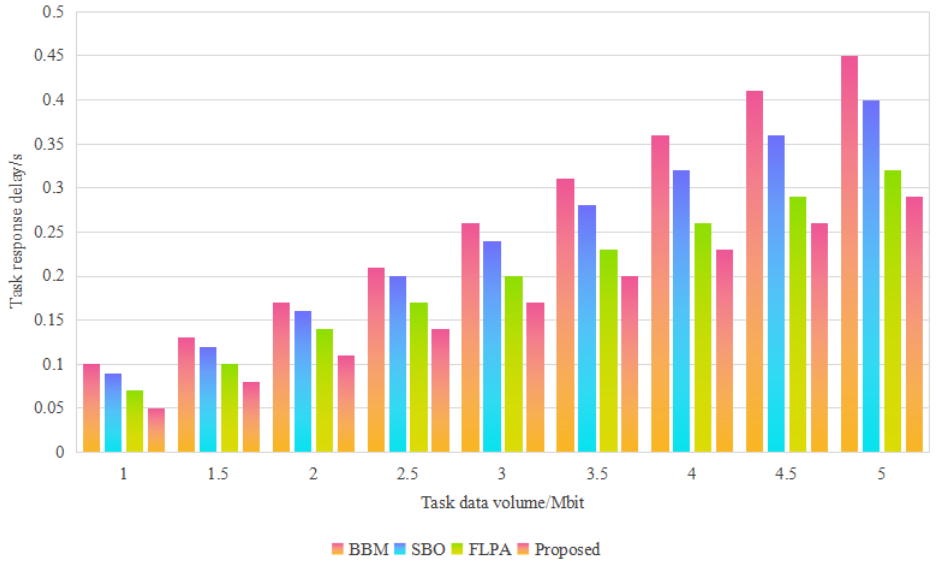


Figure 6: Comparison of delay performance of multiple unload optimization algorithms

References

[1] J. Chang, J. Ni, J. Xiao, X. Dai and H. Jin, "SynergyChain: A multichain-based data-sharing framework with hierarchical access control," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14767-14778, 2022.

[2] Z. Chen, O. Gul, B. Kantarci, "Practical Byzantine fault tolerance-based robustness for mobile crowdsensing," *Distributed Ledger Technologies: Research and Practice*, vol. 2, no. 2, 2023.

[3] M. Firdaus, K H. Rhee, "On blockchain-enhanced secure data storage and sharing in vehicular edge computing networks," *Applied Sciences*, vol. 11, no. 1, pp. 414, 2021.

[4] J. Grover, "Security of vehicular ad hoc networks using blockchain: A comprehensive review," *Vehicular Communications*, vol. 34, 2022.

[5] J. Jayabalan, N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy," *Journal of Parallel and Distributed Computing*, vol. 164, pp. 152-167, 2022.

[6] B. Ji, X. Zhang, S. Mumtaz, C. Han, C. Li, H. Wen, D. Wang, "Survey on the internet of vehicles: network architectures and applications," *IEEE Communications Standards Magazine*, vol. 4, no. 1, pp. 34-41, 2020.

[7] B. Jia, X. Zhang, J. Liu, Y. Zhang, K. Huang and Y. Liang, "Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4049-4058, 2022.

[8] M. A. Khan, "Intelligent environment enabling autonomous driving," *IEEE Access*, vol. 9, pp. 32997-33017, 2021.

[9] M. Qian, Y. Wang, Y. Zhou, L. Tian, J. Shi, "A super base station based centralized network architecture for 5G mobile communication systems," *Digital communications and Networks*, vol. 1, no. 2, pp. 152-159, 2015.

[10] A. S. Rajawat, R. Rawat, K. Barhanpurkar, R. N. Shaw, A. Ghosh, "Blockchain-based model for expanding IoT device data security," *Advances in Applications of Data-Driven Computing*, pp. 61-71, 2021.

[11] A. F. Santamaria, C. Sottile, A. Lupia and P. Raimondo, "An efficient traffic management protocol based on IEEE802.11p standard," *International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS 2014), Monterey, CA, USA*, pp. 634-641, 2014. doi: 10.1109/SPECTS.2014.6880004.

[12] H. Seo, K. -D. Lee, S. Yasukawa, Y. Peng and P. Sartori, "LTE evolution for vehicle-to-everything services," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 22-28, 2016.

[13] Q. Shi, S. Yin, K. Wang, L. Teng, H. Li, "Multichannel convolutional neural network-based fuzzy active contour model for medical image segmentation," *Evolving Systems*, vol. 13, no. 4, pp. 535-549, 2022.

[14] M. Singh, S. Kim, "Branch based blockchain technology in intelligent vehicle," *Computer Networks*, vol. 145, pp. 219-231, 2018.

[15] M. Sun, J. Zhang, "Research on the application of block chain big data platform in the construction of new smart city for low carbon emission and green environment," *Computer Communications*, vol. 149, pp. 332-342, 2020.

[16] L. Teng, H. Li, S. Yin, Y. Sun, "A modified advanced encryption standard for data security," *International*

Journal of Network Security, vol. 22, no. 1, pp. 112-117, 2020.

[17] X. Wang, S. Yin, H. Li, J. Wang, L. Teng, "A network intrusion detection method based on deep multi-scale convolutional neural network," *International Journal of Wireless Information Networks*, vol. 27, pp. 503-517, 2020.

[18] Y. Wu, S. Wang, W. Liu, W. Guo and X. Chu, "Iunius: A cross-layer peer-to-peer system with device-to-device communications," *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 7005-7017, 2016.

[19] F. Yang, S. Wang, J. Li, Z. Liu and Q. Sun, "An overview of Internet of Vehicles," *China Communications*, vol. 11, no. 10, pp. 1-15, 2014.

[20] Y. Zhang, T. Wang, K. V. Yuen, "Construction site information decentralized management using blockchain and smart contracts," *Computer-Aided Civil and Infrastructure Engineering*, vol. 37, no. 11, pp. 1450-1467, 2022.

Biography

Zengyong Xu biography. Zengyong Xu is with School of Automobile & Henan College of Transportation. Research interests: IoV communication, Data information management, Data security.

Production Command Cockpit Safety Management System Based on Deep Neural Network

Tian Liang, Zhao Qi Gen, Zhao Zhi Ping, Chen Da, and Gu Shi Qiang
(Corresponding author: Gu Shi Qiang)

Yunnan Power Grid Co., Ltd, Kunming Enersun Technology Co., Ltd.
Kunming 650000, Yunnan, China
Email: gu_qiangshi@outlook.com

(Received Sept. 12, 2023; Revised and Accepted Jan. 23, 2024; First Online Feb. 23, 2024)
The Special Issue on Role of Artificial Intelligence in Minimizing Data Threats
Guest Editor: Prof. Dede Kurniadi (Institut Teknologi Garut, Indonesia)

Abstract

This article proposes a production command cockpit safety management system based on Deep Neural Network (DNN). This system can monitor real-time production line data and network attack information and display them as a cockpit. When the cockpit graphical interface data is abnormal, management personnel can timely detect safety hazards and take corresponding security measures. This system can handle abstract and complex problems, effectively improving the production command cockpit's stability, safety, and efficiency. The system can accurately and efficiently identify, analyze, and process internal and external risk factors through many production command simulations, with an accuracy rate of over 98%. It has good feasibility and application prospects.

Keywords: Deep Neural Networks; Network Attack; Production Command Cockpit; Real Time Monitoring; Safety Management System

1 Introduction

This article aims to discuss how to use deep neural network technology to build a more intelligent and efficient production command cockpit safety management system. The production command cockpit is a very important control center in modern industrial production, and its safety and stability are directly related to the effectiveness and sustainability of the entire production process. Traditional security management systems are usually based on simple mathematical models and empirical formulas, and cannot face complex and ever-changing industrial environments. With the development of artificial intelligence technology, the application scenarios of deep neural networks are becoming increasingly widespread. In the industry, deep neural networks are applied to the production command cockpit safety management system, which can monitor in real time, analyze data and support decision-making, timely detect abnormal working conditions, unreasonable process alarm values, and frequent production line alarms. This improves the reliability of the safety management system. When there are abnormalities in production, the system will automatically issue warning messages, identify potential risks in advance, and notify relevant personnel to handle them, Avoid production accidents and downtime losses. Realize digital transformation of the production process, making production command decision-making more efficient and the production process more orderly. At the same time, in the production command cockpit safety management system, the use of deep neural network technology can more accurately identify network attack information, not only protecting equipment in the production Internet of Things, but also protecting internal enterprise information resources in the system. The main contributions and overall structure of this paper are as follows.

Firstly, multiple deep neural network technologies such as Recurrent Neural Network (RNN), Convolutional Neural Network (CNN), Generate Adversarial Network (GAN), and Long Short Term Memory Network (LSTM) were used for comparative analysis. Finally, CNN and LSTM were combined to achieve the best prediction effect, improving the accuracy of the production command cockpit safety management system, enabling such systems to quickly and accurately identify Analyze and process the risk factors in the production process, and using relevant network technology to identify external risk factors in the production process. Then, through data cleaning, normalization, and data conversion encoding, the preprocessing of network attack training and testing datasets (KDDCup99, NSL-KDD, and other datasets) was com-

pleted to improve the training effect of the neural network. Subsequently, sparse autoencoders were used for feature extraction of test data, data training, learning the laws of security states, completing the classification of test data, extracting intrusion information, and determining the risk level and system risk recognition ability. At the same time, managers can evaluate the accuracy and robustness of the model through indicators such as recall rate, accuracy rate, IOU, F1, and mAP, demonstrating the high performance of the system. Finally, developing security measures based on the results of the neural network, such as early warning and automatic shutdown.

The remaining parts of this paper are as follows: Section 2 introduces the meaning, characteristics, classification, and role of the production command cockpit safety management system; Section 3 elaborates on previous research on production command cockpit safety management systems based on deep neural networks, as well as the research topic of this paper, including research objectives, methods, processes, and conclusions; Finally, Section 4 summarizes the current research status, points out the shortcomings of the research, and looks forward to the research direction.

2 Production Command Cockpit Safety Management System

2.1 Meaning and Characteristics

The production command cockpit is a type of management cockpit (MC) that can visually and concretely display key business data indicators (KPIs) and execution status in the production process through common charts (such as volume columns and warning radars). It supports drill through queries and abnormal key indicator warnings, achieving in-depth analysis of indicators.

The production command cockpit is similar to an aircraft dashboard, which can intuitively understand the operation status of the production line and other production safety information. Users can flexibly configure and select suitable graphics to save these configurations. The production command cockpit integrates multiple disciplines: management science, information science, and human brain science, breaking data isolation. From a time perspective, it can provide historical records and current data, and from data sources, it can improve internal and external information. It is a highly intelligent production management command center, allowing safety managers to display multiple indicators, and each indicator is associated with multiple views, Real time control of production status to ensure that the production process is always in a safe area.

2.2 Modules of the Security Management System

Safety Production Management Driver Module: This is a new dynamic visualization management mode that intuitively displays the dynamic inspection of responsible parties, safety production business information, and hidden danger information on a map, helping leaders related to safety production understand their survival status and identify internal safety hazards within the system. At the same time, it can also demonstrate the safety organizational structure and job responsibilities, conduct safety planning and task tracking, and make accurate decisions.

Safety accident warning and credit management module: Establish credit files for various production departments within the system, automatically assess performance, and dynamically adjust based on supervision and inspection results, which can play a role in accident warning and promote safety production in production and operation.

Safety production supervision and inspection, hidden danger management module: This module can achieve a series of work such as safety production inspection and reporting through the network or mobile end according to the system and industry standards, and achieve full process safety supervision and inspection. Establish a refined hazard management system, such as hazard details, hazard risk levels, etc., intelligently diagnose through hazard maps, dynamically manage accidents, and ensure stable system operation. Finally, integrate all scenarios and construct a business collaboration model with multiple scenarios for comprehensive governance.

2.3 The Role of the System

2.3.1 Production Command Management

The focus of production command management for on-site safety management is to clarify the responsibilities of on-site safety management and record them within the system. Personnel management and file management modules are set up to facilitate safety training meetings, safety information, and safety certificate management. Safety management personnel and production management personnel can monitor major hazards and identify hidden dangers. You can also scan QR codes to locate the position of operators in real time, discover abnormal data, analyze potential production risks, timely prevent, and improve the safety operation awareness of job operators. It can also monitor production equipment and facilities, ensure the safe operation of equipment, assist safety and production management personnel in on-site management, provide emergency rescue for unexpected situations, and timely complete accident investigation reports.

After the upgrade of on-site safety management, various aspects of production command and management have gradually entered the stage of digital industrial management. For example, electronic work tickets can im-

prove safety management level and work approval efficiency; In terms of training management, formulate training plans, conduct employee learning and assessment, and ensure that the main responsibilities of enterprise safety training are in place and compliant. Conduct dynamic closed-loop management of risk qualitative and quantitative classification and zoning to improve the ability to prevent and contain safety production accidents. Deepen the solution to inefficient management models for enterprises and contractors. Intelligent inspection, which can conduct inspections at fixed points, times, and items, improve execution efficiency, and synchronize real-time data, automatically perform statistical analysis, and assist in assessment and evaluation.

2.3.2 Overall Protection of Industrial Control Systems

Malhotra *et al.* [9] outlined the relationship between artificial intelligence and network security, defending from multiple aspects and constantly updating protective measures, such as malicious identification software and intrusion detection software. They also introduced the use of deep neural network DNN, an advanced technology used to directly train raw data, which can identify new and ambiguous malicious software code. They not only introduced the application of artificial intelligence in the industrial community, It also introduces applications in other fields, such as education. However, the paper mainly starts from a qualitative perspective, without a quantitative proof process. Zhou *et al.* [15] proposed a global and system architecture approach for network security in modern industrial control systems (ICS), which involves multiple protections to ensure overall system stability. Industrial Control Systems (ICS) have always been victims of network attacks. Abid *et al.* [1] proposed a new method for distributed intrusion detection using artificial intelligence methods, big data technology, and cloud environments. This method addresses the drawbacks of Intrusion Detection Systems (IDS) and further improves accuracy. In the face of the transformation of industrial control systems (ICS) from proprietary architecture to open architecture, Mohammed *et al.* [2] designed the PS-CNN (PCA Select KBest CNN) model, which has the characteristics of low false alarm rate and high accuracy.

2.3.3 Risk Recording, Detection, and Identification

The system continuously records daily production, identifies risk points, counts and categorizes them, adds risk statistical lists, evaluates the data on the lists, and develops corresponding measures. During the implementation of planned measures, check the quality of plan execution, supervise safety inspections and hazard information. In terms of business data processing, the system can perform intelligent data desensitization to ensure data security. Outliers, data security, IoT security, and network attack detection.

In terms of outlier detection, in reference [8], Kravchik proposed an anomaly detection method -1D convolutional network based on the statistical deviation between measured predicted values and observed values. This method aims to solve the problem of network attack detection in industrial control systems (ICS) by using various deep neural network architectures to apply the proposed methods, such as convolutional networks and recursive networks. The dataset for this study is the Safe Water Treatment Test Bed (SWaT), which can represent the actual situation of real industrial water treatment plants.

The test dataset includes 36 different network attacks and successfully detected 31 attacks with three false positives. The results confirm that 1D convolutional neural networks are simpler, smaller, and faster than recursive neural networks. However, the processing effect of convolutional neural networks on temporal information is poor because convolution does not associate the previous inputs and only processes the inputs. The production command cockpit safety management system is also susceptible to network attacks. Due to the diversity of data sources and forms, deep neural network technology is used to detect network attacks, which is effective.

In terms of data detection, Gao *et al.* [6] conducted multiple experiments using the STRong Intrinsic Perturbation (STRIP) method to study Trojan horse attack scenarios targeting deep neural network (DNN) models, verifying the effectiveness of this method. However, this method did not verify whether it is still effective in the speech and text fields.

In terms of IoT security detection, Zhang [14] and others proposed a six step deep learning DL driven method to summarize and analyze the application of DL method to detect network attacks against CPS systems, proving that deep learning DL is more effective than machine learning ML in the process of IoT security detection. deep learning models such as artificial neural networks (ANN) and short-term memory (LSTM) were used to classify botnet attacks by Mudassir *et al.* [10], achieving accuracy standards and protecting the security of the Internet of Things while also protecting data and privacy.

Intrusion detection systems (IDS) were used to identify malicious behavior by Khan [7], and experimental results showed that the accuracy of multiple datasets was not less than 97.6%, which proves its high accuracy. However, existing IDS solutions have limitations in detecting attacks that do not belong to their databases.

In terms of network attacks, they are mainly divided into adversarial attack techniques and defense techniques. The adversarial attack techniques mainly include methods such as deeppool, fast gradient sign method, and jacobian based saliency map attachment. There are generally several methods for defensive measures of deep neural networks against attacks. For example, input preprocessing increases noise and increases attack difficulty; Reduce network complexity; Adversarial sample training; Detect and filter adversarial samples.

3 Production Command Cockpit Safety Management System Based on Deep Neural Network

3.1 System Design

Overall system design: The system needs to select a suitable hardware platform based on the actual production situation on site to ensure stable power supply equipment. Different forms of system display can meet the needs of different management users, so the system needs to have both mobile and PC display functions. Enterprises need to configure a sufficient number of servers and allocate their main functions reasonably. The system monitoring platform is another major project that needs to be configured. The monitoring platform needs to include on-site robot inspection and system end monitoring software. Monitoring points should be set up in key areas on site to collect complete data of accident points before faults occur. After analysis by the system end monitoring software, risk alarms can also be triggered in a timely manner to ensure smooth production. Risk alarms can be set up for production, equipment, materials, or operators, Push via SMS. Even during the normal operation of the system, data mining technology can be used to optimize potential risk points and areas that need improvement on site, continuously improve system functions, and improve overall efficiency.

System management module design: mainly including role, user, permission, and log management. Role management is an organizational management module that mainly maintains data, displays functions, adjusts, updates, and retrieves internal organizational data within the system. User management mainly refers to the standardized management of member information within the system, which can update and retrieve user information. Permission management mainly involves dividing the work responsibilities of system members. The system can add, delete, and edit permissions, which not only improves work efficiency but also protects data security to a certain extent. The log management function enables tracking of form operations, personnel login, and browsing information. Other systems also have the above functions. Relatively speaking, the production command cockpit safety management system based on deep neural networks can be intelligent and more efficient.

Non functional design: A production command cockpit safety management system based on deep neural networks needs to ensure the safety of the production command system and meet other functions. For example, reliability, high performance, practicality, and security. In terms of reliability, the entire system needs to operate 24 hours a day for 365 days, with short report generation and business processing time. In terms of high performance, the system needs to have the ability to simultaneously carry a large number of user accesses, from data collection, data storage to data analysis, all designed using a distributed parallel processing architecture. In terms of practicality, it is necessary to meet the usage habits of most users, making the management interface more user-friendly, easy to understand and operate. In terms of safety, safety here refers to the design of the system itself, rather than on-site safety production. The system design itself needs to avoid medium to high risk vulnerabilities and prevent illegal access, such as the use of digital signature technology.

3.2 Security Data Sources and Processing Procedures

The overall data flow of the system is as follows: data collection at the collection end, real-time AI collaboration, online remote automatic monitoring and collection of safety production data such as risks, operations, and hidden dangers (including but not limited to video, audio, and image formats, as shown in Figure 1), for example, using sensors installed on the production line to detect temperature and humidity values in the workshop. Oracle database to receive safety production data, Hbase database to store historical data, and then perform data normalization and quality verification. Oracle database stores the processed data. At the same time, use a real-time database to store real-time data. Next, we enter the development and testing phase, where ETL (extraction, transformation, and loading) processing and workflow scheduling are carried out. We establish an early warning model, conduct data early warning, defect management, and condition evaluation, and store data analysis data in an Oracle database. Publish and launch the developed tasks, enter the data management phase, and do a good job in version management. Intelligent management and analysis of work activities and early warning information around departments and workshops, forming quantifiable charts and indicators, such as generating an electronic map of enterprise risks, visually displaying the distribution of internal security risk types and levels in different colors, presenting analysis results, historical data, and real-time data on the customer end, and then linking the data together to comprehensively visualize and develop comprehensive security strategies, Realize the role of production command.

There are many on-site data classifications that require the integration of big data technology to achieve cloud storage and distributed computing. The on-site production data mainly includes: equipment maintenance, equipment inspection, mechanical arm dynamics, robot inspection records, equipment ledger, material status, and video monitoring. The data generated by the system's operation mainly includes: working condition data and switch status, etc. On line monitoring data mainly includes: equipment insulation, environmental temperature and humidity, personnel violations, and vehicle move-

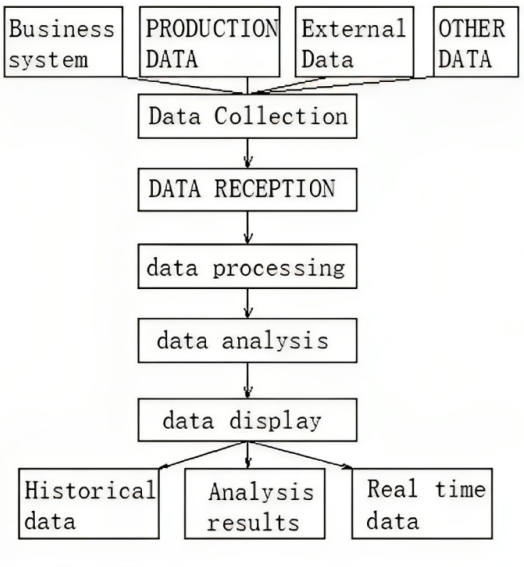


Figure 1: Security Data Processing Flow of the System

ment trajectory. The meteorological environment data mainly includes rainfall, wind and lightning conditions around the production site, and the auxiliary system data mainly includes lighting and fire protection data. There are also images, audio, video, text, molecular images, sensor signals, and video analysis data. Chenwei Tang *et al.* [11] also elaborated on the diversity of industrial data sources. Whether it is on-site data, meteorological environment data, or system data itself, these data can be roughly divided into structured data, unstructured data, and real-time data. Structured data mainly includes assets, businesses, and locations, while unstructured data mainly includes videos, map information, and report documents. Real time data mainly includes operational data, online monitoring data, meteorological data, and other data. The data sources are very extensive, such as production management systems, scheduling systems, geographic information systems (DIS), online monitoring systems, robot inspections, meteorological systems, and reporting information.

3.3 Deep Neural Network

Deep neural networks (DNN) are a computing method that mimics human brain neural networks. Based on deep neural networks, a production command cockpit safety management system can perform natural language processing, image and sound recognition, and accelerate the processing speed and accuracy of safety data. It is connected by multiple neurons and can be used for learning and training. Therefore, in the process of processing secure data, a large number of data samples and computing resources are required. During the training process, the network will gradually adjust its weight and bias, so that it can better adapt to the data and achieve the best results in the final prediction. Each layer of a deep neural network contains many independent units, and the neurons in each layer are interconnected through edges. Enter the collected data into the input layer of the model, calculate through multiple hidden layers, and obtain results and make decisions from the output layer. Shown in Figure 2.

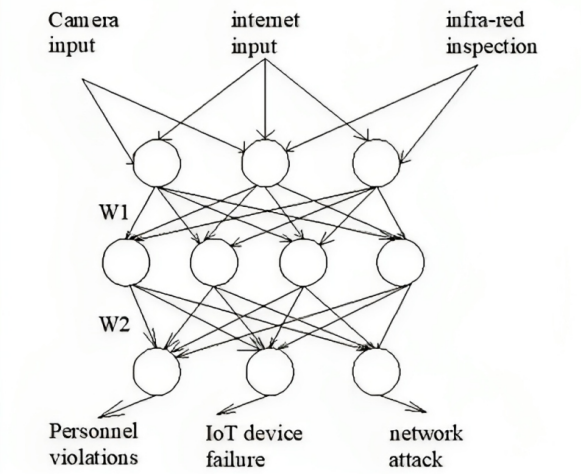


Figure 2: Simplified schematic diagram of deep neural network

3.4 Previous Studies

In the research on the production command cockpit safety management system based on deep neural networks, many attempts have been made by predecessors: Chen *et al.* [12] studied the application of deep learning in the industrial internet and the security requirements of the industrial internet, and deeply analyzed the external risks faced by the current industrial internet. A large number of manufacturing resources were originally in a closed state, facing a more open internet network environment, with weak self-protection capabilities and susceptibility to network attacks. Moreover, many new types of network attack methods have emerged, with an increasing number of attacks and faster speeds, resulting in poor performance of traditional security defense tools and technologies in new types of attacks. This research background also fits the research background of the production command cockpit safety management system in this paper. Preventing network attacks on this system is a complex project that requires technical personnel to conduct research from multiple aspects, such as data detection and IoT device detection. deep learning methods were used to network security intrusion detection by Ferrag *et al.* [5] . At the same time, 7 types of datasets and 7 deep learning models were compared, among which deep neural networks were one of them, and performance indicators such as accuracy and false alarm rate were used to measure the calculation results. Chandini [4] and others utilized deep neural network models to protect intelligent sensor production systems and ensure the security of IoT devices and data.

They also develops many algorithms to improve the accuracy of security management system detection, but different algorithms are applicable to different scenarios, such as recurrent neural network (RNN) algorithm being more suitable for text translation than convolutional neural network (CNN) algorithm. So a single algorithm has certain limitations, and if multiple algorithms are combined, accuracy can be better guaranteed. For example, combining CNN and LSTM can achieve the best prediction performance.

3.5 Research of This Paper

This article proposes a method of utilizing multiple deep neural network technologies to assist in the research of production command cockpit safety management system. The deep neural network algorithms of long and short term memory network (LSTM), convolutional neural network (CNN), generative adversarial network (GAN), and recurrent neural network (RNN) were used for verification and comparison, demonstrating the effectiveness of deep neural network application in production command cockpit safety management system, Deep neural networks are also used for modeling, analyzing and processing network attack data, accurately identifying potential security risks from more dimensions, and taking security precautions, emergency and remedial measures to ensure the safe and stable operation of the system.

3.5.1 Research Objectives and Methods

The purpose of this study is to improve the safety of the production command cockpit through deep neural network technology. To achieve this goal, we have adopted the following methods:

Collect and analyze various information generated from the command cockpit, including equipment operation status, personnel operation, environmental factors, and network threats. Utilizing deep neural network models to train and learn the collected data, achieving accurate evaluation of the safety status of the production command cockpit, and adopting corresponding safety measures to ensure the safe and stable operation of the production command cockpit.

3.5.2 Research Conditions

The platform indicators in the experiment are as follows as Table 1.

3.5.3 Research Process

The research process is divided into system production command, business data security, and network attack data.In the first part of the study, a deep neural network model was established, and L1 regularization was first performed to obtain sparse solutions. A dataset with m parameters can be defined, and then dimensionality can be reduced to obtain a low dimensional classification label set as Table 2.

Table 1: Validation Platform Indicators

parameter	index
operating system	Windows 10, 64 bit
RAM	8G
CPU	Intel(R) Core(TM) i7-9750H CPU @2.60GHz 2.59 GHz
GPU	NVIDIA GTX-1050
HDD	1T
Cores	4
Programming languages and frameworks	Python+Pytorch

$$X_1^m = \{x_u^{(1)}, x_u^{(2)}, ...x_u^{(m)}\} \tag{1}$$

$$L = j(WX + b) \tag{2}$$

$$X = h(W'X + b') \tag{3}$$

L represents the low dimensional hidden layer vector; h, j represent the activation functions of the hidden layer and the output layer, respectively. W, W' represents the weight function; b, b' represents the basis function vector. Define the error value between high and low dimensions as Table 3.

$$E = \frac{1}{N}\sum_{i-1}^{N} x_i + x_i^{r^2} \tag{4}$$

Table 2: Sparse Autoencoder Network Parameters

parameter	index
Number of hidden layers	1
Number of input/output layer neurons	50
Number of hidden layer neurons	24
Implicit and Output layer activation function	ReLU
Epochs	30
optimize	Adam

Table 3: DNN Deep Network Parameters

parameter	index
Number of hidden layers	5
Learning rate	0.2%
Block size	120
Epochs	150
loss function	square loss function
Implicit layer activation function	ReLU
Output layer activation function	Softmax
optimize	Adadelta

Define the regularization equation:

$$A = \frac{t_2}{2\mu}(|t| \le \mu); |t| - \frac{\mu}{2}(ther) \tag{5}$$

Where $\mu = 0$; A is $L1$ regularization.

ReLU activation function.

$$R = max(0, x) \tag{6}$$

The loss function is shown in Equation (7):

$$L(y, f(x)) = (y - f(x))^2 \tag{7}$$

Then perform data processing, and the data here does not include network attack data. Using datasets such as KDDCup99 and NSL-KDD, convert all data into numerical data and complete normalization processing (the following is the normalization process).

After manually annotating the image using a rectangular box, the actual data of the target object is compared to the width and height values of the upper image to obtain a set of 0-1 range distribution results, which is convenient for faster and better reading of different types of images. This set of data is: category sequence index, target center coordinates x and y, width height ww, hh, bottom right corner coordinates $x1, y1$, top left corner coordinates $x2, y2$.

$$\begin{aligned} x &= \frac{x1 + x2}{2ww}, \\ y &= \frac{y1 + y2}{2hh} \\ ww &= \frac{x1 - x2}{ww}, \\ hh &= \frac{y1 - y2}{hh}. \end{aligned}$$

Before training, it is necessary to enhance the data, fine tune the range of changes in tone, exposure, and color quantity, and ultimately generate 61000 image objects for training purposes.

The training and inference process of DNN are both conducted in the cloud, with ReLU selected as the nonlinear function and pooling and standardization carried out. Firstly, establish a Python+Python environment, and then import the dataset (training set and validation set). Shown in Figure 3.

```
from torchvision import datasets, transforms
transform = transforms.Compose([
        transforms.ToTensor(),
        transforms.Normalize((0.1307,), (0.3081,)) ])
dataset_train = datasets.MNIST('./data', train=True, download=True,
           transform=transform)
dataset_test = datasets.MNIST('./data', train=False,transform=transform)
print(dataset_train.data.data.shape)
print(dataset_test.data.data.shape)
```

Figure 3: Building a Training Environment

After obtaining the dataset, we put it into the DataLoader and encapsulate it. Next, we will start building a deep neural network. When building a deep neural network, complete the definition of each network layer and

```
import torch.nn as nn import torch.nn.functional as F
class Net(nn.Module):
    def __init__(self):
        super(Net, self).__init__()
        #First and Second layer convolutional neural network layer
        #The first and second layers of linear neural networks
        self.conv1 = nn.Conv2d(1, 32, 3, 1)
        self.conv2 = nn.Conv2d(32, 64, 3, 1)
        self.fc1 = nn.Linear(9216, 128)
        self.fc2 = nn.Linear(128, 10)
        # Forward propagation process, where x is the input data
    def forward(self, x):
        x = self.conv1(x) # Input to the first convolutional neural network layer
        x = F.relu(x) # Input to RELU activation function
        x = self.conv2(x) # Input to the second convolutional neural network layer
        x = F.relu(x) # Input to RELU activation function
        x = F.max_pool2d(x, 2) #Input to Pool Function
        x = torch.flatten(x, 1) #Flatten two-dimensional data to one-dimensional
        x = self.fc1(x) #Input to the first layer of linear neural network layer
        x = F.relu(x) # Input to RELU activation function
        x = self.fc2(x) #Input to the second layer of linear neural network layer
        output = F.log_softmax(x, dim=1) #Input to log_ Softmax activation function
        return output
```

Figure 4: Training process of deep neural network

the function that needs to be fitted: the forward function. Next comes the input and output data. Shown in Figure 4.

After building the deep neural network, initialize the model and Adadelta optimizer, and then enter the training phase. From single training to multiple training, perform forward propagation, loss value calculation, backpropagation, and update weights. The final model trained 61000 images, which took 5 hours, and the loss variation diagram is shown in the following Figure 5. It can be seen that as the number of iterations increases, the accuracy continues to improve.

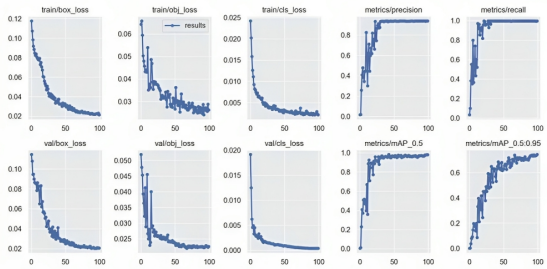


Figure 5: Results File Chart

The second part of the study is system network attacks. Once the system is attacked by external networks, all functional components within the security management system will be affected. Network attack data processing process. Shown in Figure 6.

The types of network attacks can be divided into four categories. the KDD'99 cup dataset to were used to develop predictive models and network attack datasets by Alqahtani *et al.* [3] , which classified network attacks into four categories:

1) Denial of Service (DoS). This type of network attack

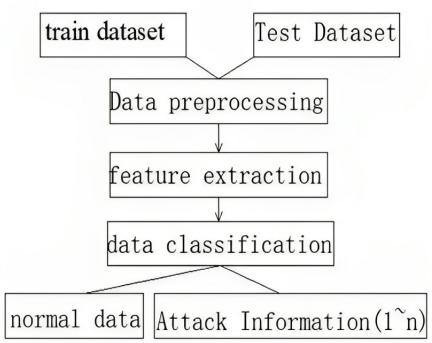


Figure 6: Deep neural network processing network attack data flow

behavior prevents legitimate users from accessing the system.

2) PROBE. The attacker attempted to obtain host information.

3) User to Root (U2R), attacker attempting to gain local access privileges.

4) Remote to Local (R2L) allows attackers to access the system without an account. Through actual testing, it is known that the first type of attack has more attacks than the other three types, with SMURF and NEPTUNE being the most common in Denial of Service (DoS), with their total number exceeding 79% of the total number of attack samples.

3.5.4 Evaluation Indicators of Research Results

In this paper, recall, accuracy, IOU, and mAP are used to evaluate the trained model:

$$\begin{aligned} Precision &= \frac{TP}{TP+FP} \\ Rcall &= \frac{TP}{TP+FN} \\ mAP &= \frac{1}{C}\sum_{k=i}^{N} P(k)R(k). \end{aligned}$$

Where
TP: True sample size
FP: False positive sample size
FN: False negative sample size
C: Number of categories
N: The amount of reference threshold,
K: Threshold
P (k): Accuracy
R (k): Recall rate.

Identify the model with the best performance through mAP values. Then adjust the threshold, recall rate, accuracy rate and IOU to meet the monitoring needs.

Identify the model with the largest mAP from numerous models, and as shown in Figure 7, the stable metrics/mAP_ 0.5 up to 0.96, metrics/mAP_ 0.5:0.95. PR_ The curve is very stable with small fluctuations, further indicating that the training effect is very good.

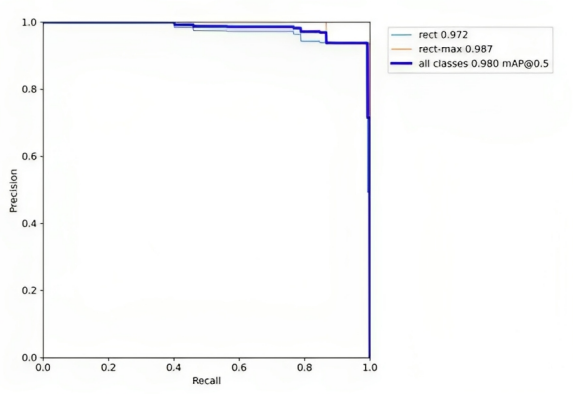


Figure 7: PR_curve

The threshold value is taken as 0.5, combined with accuracy, recall, IOU, and F1 indicators,

$$F1 = \frac{2 \times precision \cdot Rcall}{precision + Rcall}$$

F1 is a measurement indicator, and it can be seen that all classes are 0.97 at 0.707, which means that the judgment accuracy of all categories is about 0.97. At this time, the accuracy and recall are both greater than 0.97, and the F1 value also performs well. Shown in Figure 8, The model test results are good. follows as Table 4 to Table 6.

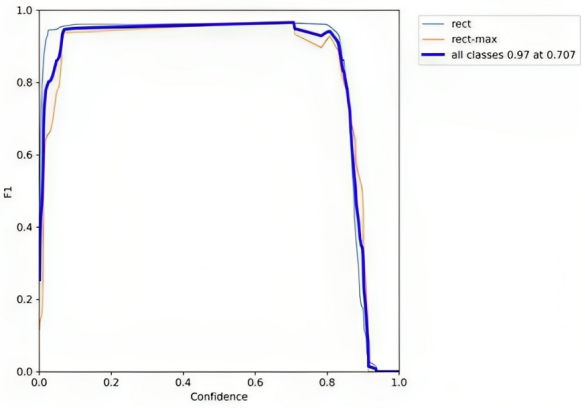


Figure 8: F1 Result Chart

3.5.5 Research Results

The convolutional neural network (CNN), long short-term memory network (LSTM), recurrent neural network (RNN), and generative adversarial network (GAN) algorithms are used to process data generated by on-site production elements such as production lines, sensors, auto-

Table 4: Comparison of Experimental Results (KDD-Cup99)

algorithm	recall	precision	IOU	mAP	F1
convolutional neural network (CNN)	97.00	97.50	96.50	97.25	97.25
recurrent neural network (RNN)	97.50	97.90	96.90	97.70	97.70
Generate adversarial network (GAN)	98.00	98.70	97.20	98.35	98.35
Long Short Term Memory Network (LSTM)	98.50	98.90	98.10	98.70	98.70
CNN+ LSTM	99.10	99.30	98.90	99.20	99.20

Table 5: Comparison of experimental results (NSL-KDD)

algorithm	**recall**	**precision**	**IOU**	**mAP**	**F1**
convolutional neural network (CNN)	97.40	97.50	96.10	97.11	97.45
recurrent neural network (RNN)	97.52	97.90	96.47	97.40	97.71
Generate adversarial network (GAN)	98.07	98.14	97.10	97.85	98.10
Long Short Term Memory Network (LSTM)	98.74	98.48	98.70	98.63	98.61
CNN+ LSTM	99.17	99.21	98.20	98.94	99.19

matic rail cars, robotic arms, CNC machine tools, warehouse goods, and operators. Convolutional neural networks (CNN) are commonly used for object detection, image classification, and semantic segmentation. Recurrent neural networks (RNNs) can learn data types with pre and post correlation, making them suitable for text translation. The LSTM algorithm has a wider applicability, such as predicting factory machine failures. The GAN algorithm is an emerging network that can generate a lot of data similar to the original data, greatly reducing the labor cost of manual annotation.

1) The deep neural network model can effectively evaluate the safety status of the production command cockpit, with a prediction accuracy of over 98%.

2) The system can monitor various information in the production command cockpit in real time, identify safety hazards in a timely manner, and provide effective support for taking effective safety measures.

By taking corresponding safety measures, the safety of the production command cockpit has been effectively improved.

4 Conclusions

In response to the complexity of the production command cockpit safety management system, a production command cockpit safety management system based on deep neural networks is proposed. Algorithms such as convolutional neural networks (CNN) in deep neural networks are used to verify system security. At the same time, a network attack detection model is established to maintain system network stability. By monitoring various data in the production command cockpit in real-time, identifying safety hazards in a timely manner, and taking corresponding safety measures, this system has good feasibility and application prospects. However, there are still some practical issues. The main difficulty is data acquisition and processing, which requires a large amount of data to obtain. However, manual data collection is time-consuming, with noise and missing data. Deep neural networks also face issues such as output stability and algorithm complexity. Moreover, Yuan *et al.* [13] found in adversarial examples that deep neural networks (DNNs) are susceptible to attacks from carefully designed input samples.

In the future, we will further optimize the deep neural network model and combine it with other technologies to construct a more intelligent and efficient production command cockpit system, improving the robustness and prediction accuracy of the system. In addition, we will actively promote the application of this system in the industrial sector, making greater contributions to ensuring the stability and safety of industrial production.

Acknowledgments

Thank you to Lakshit Malhotra, CHUNJIE ZHOU, and others involved in this paper for their published research results.

Table 6: Comparison of experimental results (UNSW-NB15)

algorithm	recall	precision	IOU	mAP	F1
convolutional neural network (CNN)	97.04	97.15	96.04	96.83	97.09
recurrent neural network (RNN)	97.24	97.49	96.41	97.13	97.36
Generate adversarial network (GAN)	98.01	98.11	97.12	97.83	98.06
Long Short Term Memory Network (LSTM)	98.44	98.18	98.14	98.27	98.31
CNN+ LSTM	98.74	99.17	98.20	98.83	99.19

References

[1] A. Abid, F. Jemili, and O. Korbaa, "Distributed deep learning approach for intrusion detection system in industrial control systems based on big data technique and transfer learning," *Journal of Information and Telecommunication*, vol. 7, no. 4, pp. 513–541, 2023.

[2] M. Al-Humairi, "Developing an efficient attack detection model for an industrial control system using cnn-based approaches : attack detection using ps-cnn,". tech. rep., 2023.

[3] H. Alqahtani, I. H. Sarker, A. Kalim, S. Md. M. Hossain, S. Ikhlaq, and S. Hossain, "Cyber intrusion detection using machine learning classification techniques," in *COMS2 2020: Computing Science, Communication and Security*, p. 121–131, Gujarat, India, March 2020.

[4] V. Chandini, U. Mounika, V. Akshaya, and K. Aarathi, "Securing smart sensing production system using deep neural network model," *Journal of Information Security and Applications*, vol. 14, no. 2, p. 619–627, 2023.

[5] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, p. 102419, 2020.

[6] 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 *ACSAC '19: Proceedings of the 35th Annual Computer Security Applications Conference*, p. 113–125, Puerto Rico, San Juan, USA, December 2019.

[7] I. A. Khan, M. Keshk, D. Pi, N. Khan, Y. Hussain, and H. Soliman, "Enhancing iiot networks protection: A robust security model for attack detection in internet industrial control systems," *Ad Hoc Networks*, vol. 134, p. 102930, 2022.

[8] M. Kravchik and A. Shabtai, "Detecting cyber attacks in industrial control systems using convolutional neural networks," in *CPS-SPC '18: Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy*, p. 72–83, Toronto, Canada, October 2018.

[9] L. Malhotra, B. Bhushan, and R. V. Singh, "Artificial intelligence and deep learning-based solutions to enhance cyber security," in *Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 2021*, pp. 1–7, April 2021.

[10] M. Mudassir, D. Unal, M. Hammoudeh, and F. Azzedin, "Detection of botnet attacks against industrial iot systems by multilayer deep learning approaches," *IEEE/CAA Journal of Automatica Sinica*, vol. 2022, pp. 1–12, 2022.

[11] C. Tang, C. Yu, Y. Gao, J. Chen, J. Yang, J. Lang, C. Liu, L. Zhong, Z. He, and J. Lv, "Deep learning in nuclear industry: A survey," *Big Data Mining and Analytics*, vol. 5, no. 2, pp. 140 – 160, 2022.

[12] C. Yang, R. Ma, Y. Wang, and Y. Zhai, "Deep learning and industrial internet security: Application and challenges," *Strategic Study of Chinese Academy of Engineering*, vol. 23, no. 2, pp. 95–103, 2021.

[13] X. Yuan, P. He, Q. Zhu, and X. Li, "Adversarial examples: Attacks and defenses for deep learning," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 30, no. 9, pp. 2805 – 2824, 2019.

[14] J. Zhang, L. Pan, Q. L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: A survey," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 3, pp. 377 – 391, 2022.

[15] C. Zhou, B. Hu, Y. Shi, Y. C. Tian, X. Li, and Y. Zhao, "A unified architectural approach for cyberattack-resilient industrial control systems," *Proceedings of the IEEE*, vol. 109, no. 4, pp. 517 – 541, 2021.

Biography

Tian Liang belongs to Han nationality, Heilongjiang. He received his bachelor's degree. He is an engineer. His research interests may include intelligent substation and substation operation

Zhao Qigen belongs to Han nationality, Yunnan. He received his bachelor's degree. Currently he is an engineer. His research interests include production technology management

Zhao Zhiping belongs to Bai ethnic group, Yunnan. She

received her undergraduate. Currently, She is an engineer. Her research interests are include computer science and application

Chen Da belongs to Han nationality, Yunnan. He received his undergraduate. Currently, He is an engineer. His research interests are include Information and Computer Science

Gu Shiqiang belongs to Han nationality, Guizhou. He received his undergraduate. Currently, He is an engineer. His research interest include Network Engineering

Guide for Authors
International Journal of Network Security

IJNS will be committed to the timely publication of very high-quality, peer-reviewed, original papers that advance the state-of-the art and applications of network security. Topics will include, but not be limited to, the following: Biometric Security, Communications and Networks Security, Cryptography, Database Security, Electronic Commerce Security, Multimedia Security, System Security, etc.

1. Submission Procedure

Authors are strongly encouraged to submit their papers electronically by using online manuscript submission at http://ijns.jalaxy.com.tw/.

2. General

Articles must be written in good English. Submission of an article implies that the work described has not been published previously, that it is not under consideration for publication elsewhere. It will not be published elsewhere in the same form, in English or in any other language, without the written consent of the Publisher.

2.1 Length Limitation:

All papers should be concisely written and be no longer than 30 double-spaced pages (12-point font, approximately 26 lines/page) including figures.

2.2 Title page

The title page should contain the article title, author(s) names and affiliations, address, an abstract not exceeding 100 words, and a list of three to five keywords.

2.3 Corresponding author

Clearly indicate who is willing to handle correspondence at all stages of refereeing and publication. Ensure that telephone and fax numbers (with country and area code) are provided in addition to the e-mail address and the complete postal address.

2.4 References

References should be listed alphabetically, in the same way as follows:
For a paper in a journal: M. S. Hwang, C. C. Chang, and K. F. Hwang, ``An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445--446, 2002.

For a book: Dorothy E. R. Denning, *Cryptography and Data Security*. Massachusetts: Addison-Wesley, 1982.

For a paper in a proceeding: M. S. Hwang, C. C. Lee, and Y. L. Tang, ``Two simple batch verifying multiple digital signatures," in *The Third International Conference on Information and Communication Security (ICICS2001)*, pp. 13--16, Xian, China, 2001.

In text, references should be indicated by [number].

Subscription Information

Individual subscriptions to IJNS are available at the annual rate of US$ 200.00 or NT 7,000 (Taiwan). The rate is US$1000.00 or NT 30,000 (Taiwan) for institutional subscriptions. Price includes surface postage, packing and handling charges worldwide. Please make your payment payable to "Jalaxy Technique Co., LTD." For detailed information, please refer to http://ijns.jalaxy.com.tw or Email to ijns.publishing@gmail.com.