IJNS
International Journal of Network Security

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

Vol. 23, No. 1 (January 2021)

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: 23, No: 1 (January 1, 2021)

International Journal of Network Security

Research on Security and Performance of Blockchain with Innovation Architecture Technology

Cheng-Ying Lin[1,2], Li-Chin Huang[3], Yi-Hui Chen[4,5], and Min-Shiang Hwang[1,6]
(Corresponding author: Min-Shiang Hwang)
Department of Computer Science & Information Engineering, Asia University, Taichung, Taiwan[1]
The Ph.D. Program in Artificial Intelligence, Asia University, Taichung, Taiwan[2]
500, Lioufeng Rd., Wufeng, Taichung 41354, Taichung, Taiwan, R.O.C.
Department of Information Management, Executive Yuan, Taipei 10058, Taiwan[3]
Department of Information Management, Chang Gung University, Taoyuan 33302, Taiwan [4]
Kawasaki Disease Center, Kaohsiung Chang Gung Memorial Hospital, Kaohsiung 83301, Taiwan[5]
(Email: cyh@gap.cgu.edu.tw)
Department of Medical Research, China Medical University Hospital, China Medical University, Taiwan[6]
(Email: mshwang@asia.edu.tw)
(Received Apr. 13, 2020; Revised and Accepted June 21, 2020; First Online June 30, 2020)

Abstract

With the development of blockchain technology, we can build many different applications on the blockchain. For example, in the financial industry, we can use blockchain's decentralized features to create an encrypted electronic currency system that does not require a third party. The system allows transactions without going through a third party. People can save some transaction costs, such as application fees or transaction fees. However, the system does not have a third party to control the data. It may lead to insufficient security of every wallet in the blockchain. Therefore, we will use public-key certificates and RFID technology to improve security. Use software and hardware two-factor authentication to prevent wallet theft. Blockchain is also a distributed ledger that anyone can see. All transaction information and smart contracts on the blockchain are entirely public. It also means that anyone can view transaction records and contract the content. It may lead to the abuse of data by illegal users. In this regard, we will use a multicast mechanism to protect private data on the blockchain and prevent data leakage. Finally, there are more and more transactions and smart contracts in the blockchain. In Bitcoin, all transaction data exceeds 80 G.B. It may cause a significant burden on some computers. In this regard, we will propose a new consensus algorithm to improve the performance of the blockchain. Transactions in the blockchain can be more efficient and faster.

Keywords: Blockchain; Consensus Algorithm; Electronic Money; Public Key Certificate; Radio Frequency Identification

1 Introduction

With the development of computer networks, the way to shop is no longer the traditional way of paying money at the physical store before taking the goods home [10,20]. Instead, it is gradually replaced by online exchanges, which has developed many innovative business models. For example, O2O (Online To Offline) [14, 22]. The convenience and speed brought by online exchanges have gradually changed people's buying and selling habits, and this trend has driven the growth of the electronic commerce [1, 21, 24].

Nowadays, electronic currency transactions mostly use third-party intermediaries' certification to ensure that the transaction can be completed [11, 12, 16]. Still, transactions through third-party intermediaries are time-consuming and expensive, and there are other risks. For example, consumer funds may be misappropriated by unethical third parties, malicious bankruptcy, derivative claims, or become a hotbed of criminal money laundering. Blockchain can solve the above problems because it can achieve decentralization; data cannot be tampered with, indelible ledger, transparent and open transactions [2–4].

There are many related applications using blockchain technology. For example, in the financial industry, we can use blockchain's decentralized characteristics to build an encrypted electronic currency system that does not require a third-party trust center [19, 23, 32]. Using this system can make transactions that do not need to go

through an intermediary and save some additional transaction costs, such as application fees or transaction fees. However, the system also lacks a third-party trust center to control data, leading to insufficient security of various currency wallets in the blockchain [6, 9, 17, 25].

In this regard, we will use digital certificates and radio frequency identification technology [27,30] to improve security. Use software plus hardware double verification to prevent wallet theft. The blockchain is also an open network ledger, and all transaction information and smart contracts on the blockchain are entirely open [8,18,31]. It also means that anyone can view other people's transaction records and contract content, leading to illegal users' data abuse. In this regard, this research will propose a group broadcast mechanism to protect private data on the blockchain and use the group confidentiality function in the group broadcast mechanism to prevent data leakage [13, 33].

Finally, many transaction records and smart contracts on the blockchain bring a heavy burden to the computer. In this regard, this research proposes a new consensus algorithm to improve the blockchain's performance, thereby making transaction data more efficient and faster [15].

This article will propose three research issues on the security and performance of blockchain with innovation architecture technology. This paper is organized as follows. Section 2 introduces three research motivations. In Section 3, we will propose three research issues for solving the research problems in Section 2. Finally, a conclusion is conducted in Section 4.

2 Research Motivations

This research will propose ways to improve the blockchain environment's infrastructure to provide users with high-security virtual currency wallets and privacy protection while improving blockchain technology's performance. The following research is aimed at different motivational statements presented by the environment.

Motivation 1. Construct a two-factor authentication virtual currency wallet to improve security.

Blockchain is a technology based on privacy security, consensus algorithms, and encryption breakthroughs. In the past, to apply for membership on the Internet, you had to fill in a lot of personal information, but only one address is required in Bitcoin, which is equivalent to an ordinary account that you can trade. Due to this feature, coupled with Bitcoin transactions' anonymity, it has become a tool for criminals to use Bitcoin as a tool for illegal transactions (for example, drug trafficking, arms transactions, payment of kidnapping ransoms, etc.).

Recently, there have been many cases of hackers stealing bitcoins in various countries worldwide, making everyone pay more and more attention to the security of virtual currency wallets. Virtual currency wallets are just like the wallet you carry on your body; actual wallets are used to put cash. The virtual currency wallet is used to put your digital currency. Just like in reality, you need to protect your wallet. Several recent major Bitcoin theft incidents are due to insufficient security of wallet software service providers. Victims of credit card theft can freeze and cancel the card. Abnormal transactions, but transactions on the blockchain are irreversible, so they are especially popular with thieves.

There are mostly two ways of stealing. One is to steal the private key database for the company's internal personnel to control all users' public key and private key (password) and then transfer the user's money, such as a foreign one. In the black market of Bitcoin, Sheep Marketplace, the boss guarded the transfer of the money and shut down the website, stealing up to 100 million U.S. dollars. Another way of stealing is for external cyber hackers to obtain the user's public key and Private key (password) and then transfer the money. This research will construct a two-factor authentication virtual currency wallet to solve the above security issues.

Motivation 2. Establish a multicast mechanism and track illegally transmitted data to protect users' intellectual property rights.

Data privacy and ownership protection on the blockchain are also significant issues. Today's most popular blockchain application, Ethereum, can sign smart contracts on the blockchain, and the blockchain is also used in healthcare. In various fields such as finance, finance, and manufacturing, this research will also study the transactions between entities and non-entities on the blockchain. The data transmitted becomes more and more diverse. We must also implement encryption mechanisms in data transmission. Protect the rights of data owners.

To protect ownership to prevent and track illegal distribution by others, the information transmitted on the blockchain may be electronic medical records or e-books, as well as music and other copyright issues. Alphabet's artificial intelligence company DeepMind should also use blockchain technology to protect medical privacy. To protect all rights and interests, we must prevent the illegal transmission of information and prevent others from transmitting copyrighted information or private information before and after transmission. The researchers constructed a group broadcast mechanism and tracked illegally transmitted data. It uses previous key encryption technology and subsequent copyright tracking to understand the person or node transmitting the data. It will prevent others from efficiently transferring protected files. Protect users' intellectual property rights.

Motivation 3. Improve the computing performance of

the blockchain to reduce the threshold and time required for transactions.

Nowadays, the transaction volume of blockchain is increasing. For Bitcoin, all transaction data is close to 80G, which is not a small burden for ordinary computer storage. How to store transaction data efficiently and quickly becomes a challenge. One of the reasons that affect performance is the consensus algorithm, that is, how to ensure that each newly created block has the same method through an invariant algorithm. In the future, it needs to be applied to larger industries. According to the current consensus algorithm, the transaction speed per second cannot meet the entire society's payment needs, which is a challenge for future scalability. For example, Bitcoin can only process seven transactions per second, while Ethereum can only process 25 transactions per second. However, the transaction volume of the financial industry is 10,000 to 100,000 transactions per second. There is still much room for improvement in performance in the future. Besides, performance issues will indirectly affect security issues.

Due to the above three motivations, this research applies various encryption and protection mechanisms to the blockchain to solve the security and efficiency issues of blockchain applications in various fields in the future.

3 Research Issues

The research framework of the blockchain security and efficiency innovation architecture technology is shown in Figure 1. Based on this structure, this article proposes the following three research topics: 1) Research on blockchain currency wallet; 2) Research on blockchain data privacy and ownership protection technology; 3) Research on using consensus algorithms to improve blockchain performance. We will introduce them in the following three subsections.

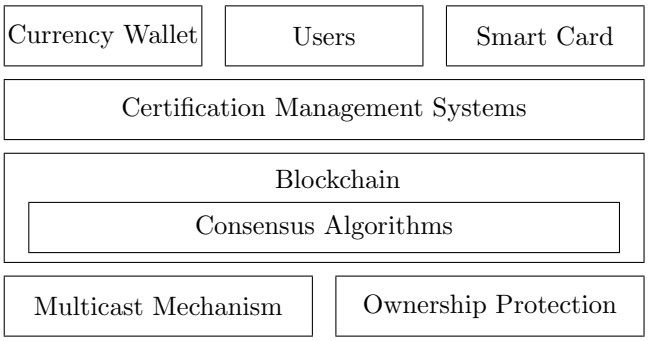


Figure 1: The research framework of the blockchain security and efficiency innovation architecture technology

3.1 Research on the Security of Blockchain Currency Wallet

The first research topic will focus on the security of virtual currency wallets in the blockchain and combine software and hardware for two-factor verification. Users must first verify their identity through a certificate authority (C.A.) to obtain a digital certificate. The private key in the asymmetric key is stored in the smart card. The software part is to prevent the database of third-party e-wallet service providers from being stolen. We use a smart card to read the private key to verify the user's identity, and the service provider cannot obtain the user's key. By combining hardware facility smart card and software authentication identity, software and hardware two-factor authentication, hackers who want to steal can even obtain the user's public key (smart card authentication) without the private key—remit funds.

In the research on the security of the blockchain virtual currency wallet, we will combine the certificate management system, the double verification of the RFID card [5, 7], and the virtual currency wallet system to improve the wallet's security. The blockchain digital certificate and certificate management system's development phase and the verification phase of the RFID encrypted private key will be executed [26, 28, 29]. The research topics include users, certificate management systems, virtual currency wallet systems, RFID cards, and blockchain.

1) The blockchain digital certificate and certificate management system's development phase:
The architecture and flowchart of the blockchain digital certificate and certificate management system's development stage are shown in Figure 2. This topic aims to issue legal digital certificates to confirm individuals, computers, and other entities on the Internet. The digital certificate is encrypted and stored on the blockchain. A certificate management system is then established to read the electronic certificate and make the electronic certificate issue unmodifiable. Multiple certificate management systems can verify the digital certificate at the same time to achieve the effect of identity verification. The research process of blockchain trusted online identity authentication and access control technology is as follows:

Step 1. The user applies for a digital certificate from the CA.

Step 2. C.A. generates a series of public elliptic curve cryptographic system parameters and generates C.A.'s public key and private key pair. According to the user I.D., the C.A. uses its private key to sign the user I.D. and generate a digital certificate.

Step 3. The CA encrypts the certificate's content and stores it on the blockchain. The remaining C.A.s can verify the legality of this operation and synchronize blockchain data.

Step 4. Save the private key to the smart card.

Step 5. Save the public key to the currency wallet.

Step 6. The user reads the electronic wallet information.

Step 7. Read the private key in the smart card and verify the holder.

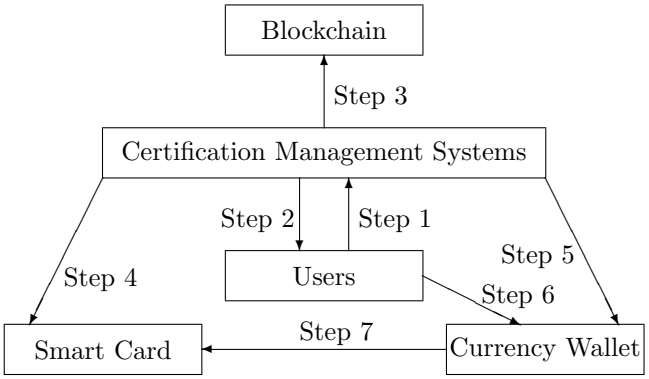


Figure 2: The architecture of blockchain virtual currency wallet

2) The verification phase of the RFID encrypted private key:
This topic aims to use a smart card to store the private key issued by the C.A., send the private key to the virtual currency wallet system, and verify it to prevent the private key from being stolen by the software service provider's hackers. Obtain the user's wallet private key from the C.A. and store it on the smart card. If a user wants to read the private wallet key, the user needs to use his/her reader sensor tag to send the private key to the back-end server (virtual currency wallet system) for verification. The identity proceeded as follows:

Step 1. The private key is encrypted and stored on the smart card.

Step 2. The public key is stored in the virtual currency wallet system.

Step 3. The card reader reads the smart card to obtain the private key and sends it to the back-end server for verification.

Step 4. Obtain the wallet use permission through verification.

3.2 Research on Blockchain Data Privacy and Ownership Protection Technology

The second research topic will focus on protecting data privacy and ownership of the blockchain. First, design a packet broadcast mechanism to protect the privacy of data shared on the blockchain. The lack of security protection for sharing on the blockchain may result in illegal users intercepting shared files and learning the content and data of shared files—the files to be shared need to have a more secure protection mechanism. As shown in Figure 3, we plan to establish a secure file sharing mechanism so that only U_2, U_4, U_5 can unlock the contents of shared files, and U_0, U_1, U_3 outside the group cannot effectively know the shared files Content information. Second, to protect the transmission of data, we will establish a prevention and tracking mechanism. We use the blockchain to pre-transmit the key, read the proprietary transaction key on the software, unlock the file, and use the tracking mechanism to track the illegal transfer. Afterward, it will punish users of files equally to deter those who intend to distribute files.

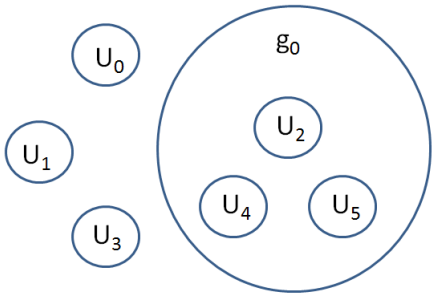


Figure 3: File security sharing mechanism

As far as the research topic of data privacy and ownership protection technology in blockchain is concerned, this goal will be achieved by combining group broadcasting mechanism, prevention mechanism, and post copyright tracking mechanism. Since it can share data on the blockchain with multiple users simultaneously, the data privacy part hopes to use packet broadcast encryption technology to meet this demand. The key management architecture diagram is shown in Figure 4. This research aims to establish a system environment based on a centralized group key management method and design a secure sharing mechanism for blockchain files. The technology developed is to broadcast the file to be shared while sharing the file. When encrypting, only users who are authorized to share can unlock the file, and the key update message is sent together with the file message to improve efficiency.

This topic will use the Chinese Residual Theorem (CRT) and the concept of privacy homomorphism to increase the amount of calculation when using public-key mechanisms to encrypt and decrypt shared files. However, it must also resolve the ensuing key update problem to make it more practical. Therefore, this part of the research can adopt a media-dependent secure multicast architecture; when a member changes, the key update operation that needs to be performed will be reserved for transmitting shared information to avoid sharing groups. Team members update the keys frequently. Besides, each group member still only needs to maintain a secret key in this mechanism, so the amount of calcu-

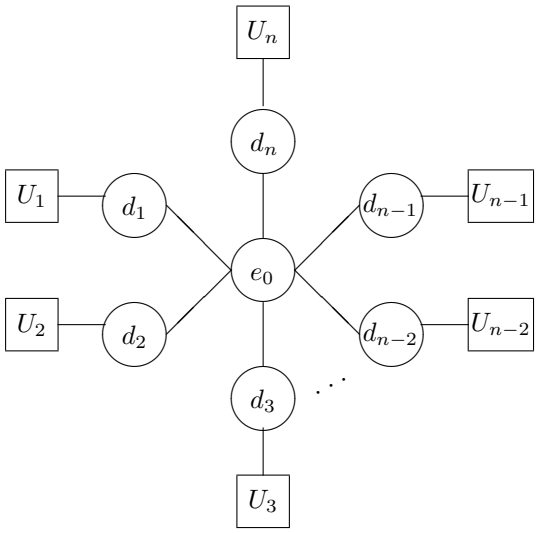


Figure 4: The key management architecture diagram of secure file sharing

lation and transmission required for key update messages is relatively saved.

Ownership protection methods need to prevent various attack methods, so its technology and method protection require incredibly high flexibility. Therefore, it is necessary to discuss and analyze the issue of flexibility repeatedly.

There are certain restrictions on the capacity and computing power of the smart card. When storing, it is necessary to consider whether the smart card's capacity and computing power can store the encrypted private key. The encryption length is the security length in the encryption process: it needs more detailed discussion and analysis.

3.3 Research on Using Consensus Algorithms to Improve Blockchain Performance

The third research topic will focus on the improvement of the blockchain performance of the consensus algorithm. It will study new consensus algorithms, the basic parameters of the consensus mechanism will be studied, and it will improve the more popular consensus algorithms currently in use. Then we will develop a more effective method.

This topic will first focus on the eight basic parameters of the consensus mechanism and conduct more in-depth research, as shown in Figure 5. Currently, we have a preliminary understanding of the consensus algorithm used in different blockchains. Therefore, we will further discuss and compare transaction calculation performance and combine the basic parameters of the consensus mechanism to find a consensus algorithm closer to the entire society's future transaction performance.

The innovative consensus mechanism's research direction is mainly based on studying the basic parameters of the consensus mechanism and the in-depth discussion of transaction calculation efficiency as an improved method. The idea is as follows:

1) The storage method of each transaction is a Merkle tree, and the transaction data hash is the Merkle root hash.

2) The public key and private key are generated by the Ellipse Extraction Digital Signature Algorithm (ECDSA). Hash is used for signatures because this method is easy to calculate the public key. Still, the public key is not easy to calculate the private key. The length of the key is more difficult to crack than traditional RSA.

3) Take advantage of PoW and PoS, using a hybrid consensus mechanism for maintenance.

Besides, we think we can start from the blockchain architecture. When many computers process blockchain transactions, not every user participates in every transaction, but an intermediate layer is established. Our idea is to centrally process a specific transaction intermediary mechanism, provide sufficient security and maintain sufficient decentralization features by the institution, and then divide blockchain transactions into parallel batch processing through the network. For example, cutting a large blockchain into several small blockchains is necessary to ensure that these small blockchains still have sufficient security. For example, permission control can also continue to each small blockchain.

When inventing a new consensus algorithm, some problems will arise. The first is whether the data security cryptography is reliable enough, and the second is which industries the algorithm is suitable for. Therefore, the new consensus algorithm must be repeatedly tested with different attack methods and evaluate its actual benefits and applications.

4 Conclusions

This article has proposed three future research issues for blockchain's security and performance with innovation architecture technology.

We summary the main works of these research issues as follows:

Topic 1: Research on the Security of Blockchain Currency Wallet

1) Development of blockchain digital certificates and certificate management systems.

   The following research work will carry out to develop the blockchain digital certificate and management center:

   a. Develop trusted digital certificates and store them on the blockchain.

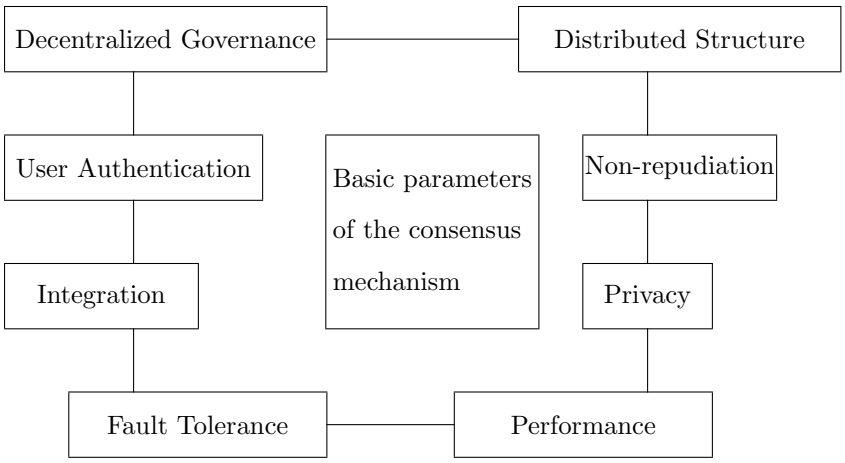


Figure 5: Basic parameters of the consensus mechanism

b. Establish a certificate management system.

2) Research and development of verifying smart card encryption private key.

The following research work will carry out to enable smart card devices to store encrypted private keys:

a. Use smart cards to store encrypted private keys without being stolen by others.
b. The background server verifies the private key and public key.

Topic 2: Research on Blockchain Data Privacy and Ownership Protection Technology

1) Research on the development of the blockchain data privacy and group broadcast mechanism.

The following research work will carry out to research and develop the blockchain data privacy and group broadcasting mechanism:

a. Research and develop the group broadcasting mechanism on the blockchain;
b. Establish a centralized group key management system.

2) Research and development of prevention and post-tracking mechanism for ownership protection.

The following research work will carry out regarding the prevention and tracing mechanism of ownership protection:

a. Develop a mechanism to transmit the transaction key on the blockchain and decrypt it on the other party's software.
b. Establish a tracking mechanism to track the spread of illegal users.

Topic 3: Research on Using Consensus Algorithms to Improve Blockchain Performance

1) Research the eight basic parameters of the consensus mechanism.
2) Research on different consensus mechanisms in-depth analysis.
3) Research and develop more effective consensus algorithms.
4) Evaluate the effectiveness of the developed consensus algorithm.
5) Research and develop innovative blockchain architecture.

The irreversible characteristics of the blockchain and the trust machine model make electronic money flourish and exchange. The convenience of e-commerce will drive the country's economic development and will make a considerable contribution to the development of information technology and the entire world economy.

Acknowledgments

The Ministry of Science and Technology partially supported this research, Taiwan (ROC), under contract no.: MOST 108-2410-H-468-023 and MOST 108-2622-8-468-001-TM1.

References

[1] R. C. Agidi, "Biometrics: The future of banking and financial service industry in Nigeria," *International Journal of Electronics and Information Engineering*, vol. 9, no. 2, pp. 91–105, 2018.

[2] P. Y. Chang, M. S. Hwang, C. C. Yang, "A Blockchain-Based Traceable Certification System," in *Security with Intelligent Computing and Big-data Services (SICBS'17)*, Advances in Intelligent Systems and Computing, vol. 733, pp. 363–369, Springer, 2018.

[3] Y. H. Chen, L. C. Huang, I. C. Lin, and M. S. Hwang, "Research on blockchain technologies in bidding systems," *International Journal of Network Security*, vol. 22, no. 6, pp. 897–904, 2020.

[4] Y. H. Chen, L. C. Huang, I. C. Lin, and M. S. Hwang, "Research on the secure financial surveillance blockchain systems," *International Journal of Network Security*, vol. 22, no. 4, pp. 708–716, 2020.

[5] Y. L. Chi, C. H. Chen, I. C. Lin, M. S. Hwang, "The secure transaction protocol in NFC card emulation mode," *International Journal of Network Security*, vol. 17, no. 4, pp. 431–438, 2015.

[6] P. Fan, Y. Liu, J. Zhu, X. Fan, and L. Wen, "Identity management security authentication based on blockchain technologies," *International Journal of Network Security*, vol. 21, no. 6, pp. 912-917, 2019.

[7] T. H. Feng, M. S. Hwang, and L. W. Syu, "An authentication protocol for lightweight NFC mobile sensors payment," *Informatica*, vol. 27, no. 4, pp. 723–732, 2016.

[8] C. K. Frantz and M. Nowostawski, "From institutions to code: Towards automated generation of smart contracts," in *IEEE 1st International Workshops on Foundations and Applications of Self Systems*, pp. 210-215, 2016.

[9] C. Hu, D. Zheng, R. Guo, A. Wu, L. Wang, and S. Y. Gao, "A novel blockchain-based anonymous handover authentication scheme in mobile networks," *International Journal of Network Security*, vol. 22, no. 5, pp. 874-884, 2020.

[10] M. S. Hwang, C. C. Lee, Yan-Chi Lai, "Traceability on low-computation partially blind signatures for electronic cash", *IEICE Fundamentals on Electronics, Communications and Computer Sciences*, vol. E85-A, no. 5, pp. 1181–1182, May 2002.

[11] M. S. Hwang, I. C. Lin, L. H. Li, "A simple micropayment scheme", *Journal of Systems and Software*, vol. 55, no. 3, pp. 221–229, Jan. 2001.

[12] M. S. Hwang and P. C. Sung, "A study of micropayment based on one-way hash chain", *International Journal of Network Security*, vol. 2, no. 2, pp. 81–90, Mar. 2006.

[13] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira and A. Akutsu, "The blockchain-based digital content distribution system," in *IEEE Fifth International Conference on Big Data and Cloud Computing*, pp. 187-190, 2015.

[14] H. Li, L. Gu, W. Gu, X. Liu, "Research on online-to-offline clothing customization mode based on consumer perceived value," *Journal of Textile Research*, vol. 41, no. 9, pp. 128–135, 2020.

[15] Z. C. Li, J. H. Huang, D. Q. Gao, Y. H. Jiang and F. Li, "ISCP: An improved blockchain consensus protocol," *International Journal of Network Security*, vol. 21, no. 3, pp. 359-367, 2019.

[16] I. C. Lin, M. S. Hwang, C. C. Chang, "The general pay-word: A micro-payment scheme based on n-dimension one-way hash chain", *Designs, Codes and Cryptography*, vol. 36, no. 1, pp. 53–67, July 2005.

[17] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *International Journal of Network Security*, vol. 19, no. 5, pp. 653-659, 2017.

[18] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292-2303, 2016.

[19] Y. Liu, M. He, and F. Pu, "Anonymous transaction of digital currency based on blockchain," *International Journal of Network Security*, vol. 22, no. 3, pp. 444-450, 2020.

[20] J. W. Lo, H. M. Lu, T. H. Sun, and M. S.Hwang, "Improved on date attachable electronic cash," *Applied Mechanics and Materials*, vol. 284, pp. 3444–3448, 2013.

[21] D. E. Saputra, S. Sutikno, and S. H. Supangkat, "General model for secure electronic cash scheme," *International Journal of Network Security*, vol. 21, no. 3, pp. 501–510, 2019.

[22] P. Tang, F. He, X. Lin, and M. Li, "Online-to-offline mobile charging system for electric vehicles: Strategic planning and online operation," *Transportation Research Part D: Transport and Environment*, vol. 87, pp. 102522, 2020. (`http://www.sciencedirect.com/science/article/pii/S1361920920307094`)

[23] H. Tewari and E. O. Nuallain, "Netcoin: A traceable P2P electronic cash system," in *IEEE International Conference on Web Services*, pp. 472-478, 2015. Ethereum, "Ethereum Frontier." https://www.ethereum.org/, 2015.

[24] F. Wang, C. C. Chang, and C. Lin, "Security analysis on secure untraceable off-line electronic cash system," *International Journal of Network Security*, vol. 18, no. 3, pp. 454–458, 2016.

[25] L. Wang, D. Zheng, R. Guo, C. Hu, and C. M. Jing, "A blockchain-based privacy-preserving authentication scheme with anonymous identity in vehicular networks," *International Journal of Network Security*, vol. 22, no. 6, pp. 981-990, 2020.

[26] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "A secure privacy and authentication protocol for passive RFID tags," *International Journal of Mobile Communications*, vol. 15, no. 3, pp. 266–277, 2017.

[27] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "Security analysis of an enhanced mobile agent device for RFID privacy protection," *IETE Technical Review*, vol. 32, no. 3, pp. 183–187, 2015.

[28] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "An improved authentication protocol for mobile agent device in RFID," *International Journal of Mobile Communications*, vol. 10, no. 5, pp. 508–520, 2012.

[29] C. H. Wei, M. S. Hwang, A. Y. H. Chin, "A mutual authentication protocol for RFID", *IEEE IT Professional*, vol. 13, no. 2, pp. 20–24, Mar. 2011.

[30] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "An authentication protocol for low-cost RFID tags", *International Journal of Mobile Communications*, vol. 9, no. 2, pp. 208–223, 2011.

[31] A. Yasin and L. Liu, "An online identity and smart contract management system," in *IEEE 40th Annual Computer Software and Applications Conference (COMPSAC'16)*, pp. 192-198, 2016.
[32] Y. Zhu, R. Guo, G. Gan and W. T. Tsai, "Interactive incontestable signature for transactions confirmation in bitcoin blockchain," in *IEEE 40th Annual Computer Software and Applications Conference (COMPSAC'16)*, pp. 443-448, 2016.
[33] G. Zyskind, O. Nathan and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *IEEE Security and Privacy Workshops*, pp. 180-184, 2015.

Biography

Cheng-Ying Lin received the M.A. in Hochschule für Musik und Theater "Felix Mendelssohn Bartholdy" Leipzig, Germany, in 2015, and B.A. in National Hsinchu University of Education,Taiwan, in 2011. He is currently pursuing a Ph.D. degree in the Ph.D. Program in Artificial Intelligence, at Asia University, Taiwan. He was the owner and trombonist of the Brass Men ensemble. He was also served as a teacher and Wind Orchestra Conductor in many schools. His current research interests include Artificial intelligence, Computer music.

Yi-Hui Chen received her Ph.D. degree in computer science and information engineering at the National Chung Cheng University. Later on, she worked at Academia Sinica as a post-doctoral fellow. Then, she worked at IBM's Taiwan Collaboratory Research Center as a Research Scientist, the Department of M-Commerce and Multimedia Applications, Asia University as an associate professor. She is now an associate professor at the Department of Information Management, Chang Gung University. Her research interests include multimedia security, semantic web, text mining, and multimedia security.

Li-Chin Huang received the B.S. in computer science from Providence University, Taiwan, in 1993 and M.S. in information management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, in 2001; and the Ph.D. degree in computer and information science from National Chung Hsing University (NCHU), Taiwan in 2001. Her current research interests include information security, cryptography, medical image, data hiding, network, security, big data, and mobile communications.

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 (U.C.), Riverside, and U.C. Davis (USA) during 2009-2010. He was a distinguished professor of the Department of Management Information Systems, NCHU, during 2007-2011. He obtained 1997, 1998, 1999, 2000, and 2001 Excellent Research Awards from the National Science Council (Taiwan). Dr. Hwang was a dean of the College of Computer Science, Asia University (A.U.), Taichung, Taiwan. He is currently a chair professor with the Department of Computer Science and Information Engineering, A.U. His current research interests include information security, electronic commerce, database, data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 300+ articles on the above research fields in international journals.

ECID: Elliptic Curve Identity-based Blind Signature Scheme

Shoulin Yin[1], Hang Li[1]*, Shahid Karim[2], and Yang Sun[1]
(Corresponding author: Hang Li)
Software College, Shenyang Normal University[1]
Shenyang 110034 China
School of Electronics and Information Engineering, Harbin Institute of Technology[2]
Harbin 150000, China
(Email: lihangsoft@163.com)
(Received June 19, 2019; Revised and Accepted Dec. 6, 2019; First Online Feb. 1, 2020)

Abstract

With the increasing development of computer and network technology, blind signature scheme has been widely used in electronic cash, electronic election, casual transmission and other fields. It can resolve the conflict between anonymity and controllability, protecting user's privacy while tracing their identities. The traditional blind signature scheme has many problems, such as high storage cost and communication cost. To solve the above problems, a blind signature scheme based on elliptic curve-identity is proposed, which adopts the dot product operation on elliptic curve to replace the bilinear pair operation and reduces the computational overhead. Under the random oracle model, the unforgeability attack is proved. And we give the security analysis of the new scheme.

Keywords: Blind Signature; Elliptic Curve; Identity; Random Oracle Model

1 Introduction

With the cryptography deeply research, the application of cryptography has come into every aspect of social life, especially in financial system and military system [6, 14]. As the main content of cryptography research, digital signature is widely used in many fields [8, 15]. Therefore, it has attracted people's attention. Many different concepts of digital signature had been proposed, such as blind signature, group signature, proxy signature and threshold signature. Electronic cash system, electronic election system and other applications play an increasingly important role in life [10, 13], but the resulted security problems are also ubiquitous. In order to better protect the privacy of users and ensure that the information submitted by the client are not stolen by the third party, the concept of blind signature is proposed. Meanwhile, various blind signature schemes come into being and are widely used in fields with anonymous requirements. Fan [4] presented a blind signature scheme with randomization based on bilinear pairing primitives. Furthermore, it provided concrete security proofs for the required properties of the proposed scheme under the random oracle model. He [5] proposed an identity based blind signature scheme without bilinear pairings to save the running time and the size of the signature. Cao [2] presented a quantum proxy weak blind signature scheme. It was based on controlled quantum teleportation. Five-qubit entangled state functions as quantum channel. The scheme used the physical characteristics of quantum mechanics to implement message blinding, so it could guarantee not only the unconditional security of the scheme but also the anonymity of the messages owner. However, some schemes are with large computational time, others are low efficiency.

In blind signature, the signer does not know the specific content of the signed message, but the complete anonymity will leave a security risk. In electronic voting, for example, complete anonymity may allow voters to revote or change their vote multiple times. As a digital signature with special characteristics, blind signature was first proposed by CHAUM in 1982. In addition to meet the nature of ordinary digital signature, blind signature also needs to meet the following requirements:

1) The signer is invisible to the content of the document, that is, the signer does not know the specific content of the message.

2) The signature message is untraceable, that is, after the signature message is published, the signer cannot know which time he signed it [1].

The most intuitive metaphor for blind signature is that the document owner first puts the document to be signed into an envelope with carbon paper, and seals it (blind), then gives the document to the signer; When a signer signs an envelope, his signature is signed onto the document through carbon paper (signature); When the file owner opens the envelope, the real signature of the file can be obtained (de-blinding). Since the signer cannot see the contents of the file when signing, the blind signature is especially suitable for the domain where the privacy of the file owner needs to be protected. In this paper, we propose

a blind signature scheme based on elliptic curve-identity. Under the random oracle model, the scheme is proved to be effective in resisting the existence unforgeability attack in adaptive selection message. The new scheme does not use bilinear pairs, which reduces the computational overhead. This paper is organized as follows. Section 2 introduces the preliminaries including bilinear pairs and review of traditional blind signature scheme. In Section 3, we detailed explain the proposed blind signature scheme based on elliptic curve-identity. Section 4 gives the performance analysis of proposed scheme. Finally, a conclusion is conduced in Section 5.

2 Preliminaries

2.1 Bilinear Pairs

G_1 is a $q-order$ cyclic addition group generated by g. G_2 is a $q-order$ cyclic multiplication group. q is a large prime number [9]. $a,b \in Z_q^*$, $e: G_1 \times G_2$ is bilinear pairs with the following properties:

1) Bilinear: For all $P,Q \in G_1$ and all $a,b \in Z_q^*$, $e(aP,bQ)=e(P,Q)^{ab}$.

2) Non-degenerate: There is $g \in G_1$, so that $e(g,g) \neq 1$.

3) Computability: For all $P,Q \in G_1$, there is an effective algorithm to calculate $e(P,Q)$.

2.2 Difficulty Hypothesis

1) DDHP (Decisional Diffie-Hellman Problem). Known P, aP, bP, cP, where $a,b,c \in Z_q^*$. Judging whether $c \equiv abmodq$ is correct.

2) CDHP (Computational Diffie-Hellman Problem). Known P, aP, bP, cP, where $a,b,c \in Z_q^*$. Compute abP.

   If DDHP is easy, but CDHP is difficult in group G, G is called the Gap Diffie-Hellman group.

3) DLP (Discrete Logarithm Problem). Set the order of cyclic group G as p, $g \in G$ is a generator. Given (g,g^a), in group G, calculating $a \in Z_p^*$ is difficult.

   DLP problem is said to be difficult if there is no probability polynomial time algorithm C to solve the DLP problem with insuperable advantage.

3 Traditional Blind Signature Scheme

3.1 Review of Blind Signature

In this section, we will review the traditional blind signature scheme according to reference [3, 7].

1) System establishment. Input system safety parameter 1^k. KGC (Key generation center) generates $p-order$ cyclic addition group G_1, G_2 and cyclic multiplication group G_T, where $p \leq 2^k$ is prime number. $Q \in G_2$ is selected as generator, homeomorphic mapping $\varphi: G_2 \to G_1$, calculating $P=\varphi(Q) \in G_1$. Bilinear pair mapping is $e: G_1 \times G_2 \to G_T$. KGC randomly selects $s \in Z_p^*$, which is used as the main key of the system to keep secret. Computing $Q_p=sQ$ as the public key of the system. Selecting the safe Hash function: $H_1:(0,1)^* \to Z_p^*$, $H_2:(0,1)^* \times G_T \to Z_p^*$, $H_3:(0,1)^* \to Z_p^*$. Public parameters is $params = G_1, G_2, G_T, H_1, H_2, H_3, P, Q, Q_p, q, \varphi$.

2) Extracting key. KGC calculates the private key of signer A $S_A=\frac{1}{H_1(ID_A)+s}P$. The SA is sent to signer A through a secret channel.

3) Signature protocol. This algorithm needs to be completed by interaction between signer A and user B. It is known that the public parameter of the system is $params$, the identity and private key of A are ID_A and S_A respectively, the message $m \in 0,1^*$. c is the public information agreed by B and A in advance. It pre-computes $g=e(P,Q)$. The following is the interaction process between A and B:

   - Commitment. A randomly selects $x,y \in Z_q^*$, computing $r_1=g_1^x$, $r_2=g_2^x$, $v_1=g_1^y$, $v_2=g_2^y$ and sending (r_1,r_2,v_1,v_2) to B.
   - Blind. After receiving (r_1,r_2,v_1,v_2), B randomly selects blind factor $\alpha,\beta \in Z_q^*$, computing $\bar{r}_1 = r_1^{\alpha} g_1^{\alpha\beta} g_1^{\alpha H_1^{-1}(A) H_3^{-1}(c)} v_1^{H_3^{-1}(c)}$, $\bar{r}_2 = r_{12}^{\alpha} g_2^{\alpha\beta} v_{21}^{\alpha H_3^{-1}(c)}$, $R = \bar{r}_1^{H_1(ID_A)} \bar{r}_2$, $h = \alpha^{-1} H_2(m,c,R) + \beta H_3(c)$. Then it sends h to A.
   - Signature. After receiving h, A calculates $V_1=(xH_3(c)+y+h)P+S_A$ and sends V_1 to B.
   - Removing blind. After receiving V_1, B computes $V=\alpha V_1$, so the signature of message m is $\sigma=(m,c,R,V)$.

4) Verification. The verifier receives the signature pair $\sigma=(m,c,R,V)$, verifies equation $e(V,H_1(ID_A)Q+Q_P = R^{H_3(c)} g_1^{H_1(ID_A)H_2(m,c,R)} g_2^{H_2(m,c,R)}$, if the equation is correct, then the signature is valid, otherwise, the signature is invalid.

3.2 Scheme Attack

Through analysis, it is found that the above traditional scheme is not safe. Dishonest users can change the public information c into $\hat{c}$ without the signer and verifier being aware of it. The following is the attack process in the interaction between signer A and user B.

- Commitment. A randomly selects $x,y \in Z_q^*$, computing $r_1=g_1^x$, $r_2=g_2^x$, $v_1=g_1^y$, $v_2=g_2^y$ and sending (r_1,r_2,v_1,v_2) to B.

- Blind. After receiving (r_1, r_2, v_1, v_2), B randomly selects blind factor $\alpha, \beta \in Z_q^*$, computing $\bar{r}_1 = r_1^{\alpha H_3(c)} v_1^{\alpha} g_1^{\alpha\beta} g_1^{\alpha H_3^{-1}(ID_A)}$, $\bar{r}_2 = r_2^{\alpha H_3(c)} g_2^{\alpha\beta} v_2^{\alpha}$, $R = \bar{r}_1^{H_1(ID_A)} \bar{r}_2$, $h = \alpha^{-1} H_2(m, \hat{c}, R) + \beta H_3(\hat{c})$, $h^* = H_3^{-1}(\hat{c})h$. Then it sends h^* to A.

- Signature. After receiving h^*, A calculates $V_1' = (xH_3(c) + y + h^*)P + S_A$ and sends V_1' to B.

- Removing blind. After receiving V_1', B computes $\hat{V} = \alpha H_3(\hat{c}) V_1'$, so the signature of message m is $\sigma = (m, \hat{c}, R, \hat{V})$.

The signature verifies the equation. The dishonest user successfully replaces c with $\hat{c}$.

4 ECID: Elliptic Curve-Identity-Based Blind Signature Scheme

- Initialization. Input safety parameter k, KGC generates two major prime numbers p and q. Define elliptic curve $E(F_p)$ on finite domain F_p. Let G be an additive group of points on $E(F_p)$ whose order is q. KGC selects one basis point p of G and two safe Hash functions: $H_1 : 0,1^* \times G \to Z_p^*$ and $H_2 : 0,1^* times 0,1^* times G \to Z_p^*$. KGC randomly selects the master key $s \in Z_p^*$, the public parameter $params = p, q, E(F_p), G, P, P_{pub}, H_1, H_2$. This phase consists of the following two steps:

  1) Step 1. The selected infinity point G is a large number on the $E(F_p)$ curve.
  2) Step 2. Randomly select $x_{ID} \in Z_p^*$, and calculate the public key $X_{ID} = x_{ID}^{-1} P$, $Y_{ID} = x_{ID}^{-1} P_{pub}$, $PK_{ID} = (X_{ID}, Y_{ID})$.

- Generate part of the private key. Input identity ID of A, system main key s and system public parameter $params$. Obtain part of the private key $D_{ID} = \frac{1}{1+s^{-1}Q_{ID}} P$. Where, $Q_{ID} = H_1(ID, X_{ID}, Y_{ID})$.

- Signature protocol. This algorithm needs to be completed by interaction between signer A and user B. The message $m \in 0,1^*$. c is the public information agreed by B and A in advance. The following is the interaction process between A and B:

  – Commitment. A randomly selects $x, y \in Z_q^*$, computing $r_1 = g^x$, $r_2 = g^y$ and sending (r_1, r_2) to B.

  – Blind. After receiving (r_1, r_2), B randomly selects blind factor $\alpha, \beta \in Z_q^*$, computing $\bar{r} = (r_1 r_2)^{\alpha} g^{\beta}$, $h = \alpha^{-1} H_2(m, c, \bar{r})$. Then it sends h to A.

  – Signature. After receiving h, A calculates $V_1 = ((x + y)H_3(c) + hS_{ID})$ and sends V_1 to B.

  – Removing blind. After receiving V_1, B computes $V = \alpha V_1 + \beta H_3(c)$, so the signature of message m is $\sigma = (ID, m, c, \bar{r}, V)$.

- Verification. The verifier receives the signature pair $\sigma = (ID, m, c, \bar{r}, V)$, first computes $H_1(ID)$, $H_3(c)$, $H_2(m, c, \bar{r})$ verifies equation $g^V = \bar{r}^{H_3(c)} P_{pub}^{H_1(ID) H_2(m,c,\bar{r})}$, if the equation is correct, then the signature is valid, otherwise, the signature is invalid.

5 Performance Analysis of Proposed Scheme

5.1 Correctness Analysis

The proposed scheme is correct.

$$\begin{aligned} h &= H_2(mPx_AGPe(S, x_A + RY_A)g^{-h} \\ &= H_2(mPY_APe(\beta^{-1}(r+h)x_AR, x_A + RY_A)g^{-h} \\ &= H_2(mPY_APe(\beta^{-1}(r + h\beta + \alpha)x_ARP, x_A^{-1}P \\ &\quad + Rx_A^{-1}P_{pub})g^{-h} \\ &= H_2(mPY_APe(\beta^{-1}(r + h\beta + \alpha)P, P)g^{-h} \\ &= H_2(mPY_AP(Ug^{\alpha})^{\beta-1}) \\ &= H_2(mPY_APV). \end{aligned} \quad (1)$$

5.2 Security Analysis

The proposed blind signature scheme satisfies the blindness.

Assume that the blind signature is (m, S, h), and any set of views (U, h', S') generated by the publishing process of blind signature. The blind factor α, β is randomly selected. The following equations are established.

$$\beta = log_S S' mod p. \quad (2)$$

$$\alpha = h' - h log_S S' mod p. \quad (3)$$

There is a unique α and β, which makes above formulas true. So the proposed blind signature scheme satisfies the blindness.

5.3 Unforgeability Proving

Theorem 1. *Under the random oracle model, based on the discrete log-difficult problem, the scheme satisfies the existence unforgeability under the adaptive selection message attack and identity attack.*

Lemma 1. *Assuming that adversary A wins the following game with a non-negligible advantage ε after a series of queries (including q_{H_i} Hash queries, q_E private key extraction queries and q_V signature queries) within a polynomial bounded time t. The challenger C solves the discrete logarithm problem by an advantage no less than $\frac{\varepsilon}{\sqrt{q_{H_2}}}$.*

Table 1: Performance comparison with four schemes

Scheme	Requester	Signer	Verification	Total computation
IPB	2M+E	2M+4E	2P+M+2E	2P+2M+6E
DLM	2M+E	3M+5E	P+2M+2E	2P+2M+4E
IAQ	M+E	3M+3E	P+2M+3E	2P+4M+10E
ECID	M+E	M+2E	2M+2E	4M+4E

Proof. Assuming ID^* is a target user, the following is the interaction process between C and A. □

- System establishment stage. C runs system establishment algorithm, and returns system parameter $params = (G, H_1, H_2, H_3, p, g, P_{pub})$ to A, set $P_{pub} = g^a$.
- H_1 inquiry. C maintains list $L_1 = (ID_i, \omega_i)$, and its initial value is null. When receiving H_1 inquiry, if Q_{ID_i} is already in list L_1, Q_{ID_i} is returned. Otherwise, C randomly selects $\omega_i \in Z_p^*$ and returns ω_i to A, then updates list L_1.
- H_2 inquiry. C maintains list $L_2 = (m_i, c_i, \bar{r}_i, h_i)$, and its initial value is null. When receiving H_2 inquiry, if Hash value l_i of L_2 is already in list L_2, Hash value l_i is returned. Otherwise, C randomly selects $l_i \in Z_p^*$ and updates list L_2.
- H_3 inquiry. C maintains list $L_3 = (c_i, h_i)$, and its initial value is null. When receiving H_3 inquiry, if $\bar{h}_i$ is already in list L_3, $\bar{h}_i$ is returned. Otherwise, C randomly selects $\bar{h}_i \in Z_p^*$ and updates list L_3.
- Key extraction inquiry. C maintains list L_1. When receiving the key extraction inquiry, if $ID_i = ID^*$, C fails to exit. Otherwise, C looks up table L_1, calculates $S_{ID_i} = a\omega_i$, and returns S_{ID_i} to A, updates list L_1.
- Signature query. If such query is received (assuming that relevant Hash query and key extraction query have been done), C looks up table L_1 to get the private key of user ID_i. Then V is calculated and returned to A by combining the signature algorithm and table $L_1 - L_3$.
- Forgery. Challenger C and adversary A have $q_{H_i} (i = 1, 2, 3)$ random oracle inquiries (each inquiry time is $t_{H_i} (i = 1, 2, 3)$), q_E key extraction inquiries (each inquiry time is t_E), q_v signature inquiries (each query time is t_v, if algorithm C does not stop, under the condition of no key extraction query for ID^* and signature query for (ID^*, m^*, C^*), A can successfully forge the signature $(ID^*, \bar{r}, V)$ of the message (m^*, c^*) with probability $\frac{1}{\sqrt{q_{H_2}}}$ under a non-negligible advantage ε within time $t' < t + (t_{H_1} q_{H_1} + t_{H_2} q_{H_2} + t_{H_3} q_{H_3} + t_E q_E + t_v q_v)$.

According to Forking lemma, through the Hash replay of A, C can obtain two valid signatures $(ID^*, m^*, c^*, \bar{r}, l_1, \omega_1, \bar{h}_1, V_1)$ and $(ID^*, m^*, c^*, \bar{r}, l_2, \omega_2, \bar{h}_2, V_2)$ about $(m^*, c^*$. Let $k \in Z_p^*$ represent the discrete logarithm value, namely $g^k = \bar{r}$.

5.4 Comparison Results

We make comparison with three other blind signature schemes including IPB [11], DLM [12] and IAQ [16]. Defining point operations as P, scalar multiplication of group G_1, G_2, G_T and G as M and power multiplication as E.

As can be seen from Table 1, the total calculation amount of the proposed scheme in this paper is $4M + 4E$, in which the modular exponentiation is 4E. Compared with the scheme in reference IPB and DLM, the calculation cost of ECID is the lowest. Compared with the scheme in IAQ, the calculation cost of ECID is greatly reduced, and it improves the computational efficiency. More importantly, the scheme in this paper does not use bilinear pairings which has the largest computational overhead, and overcomes the defect of tampering with public information, so it is superior to the above schemes in terms of efficiency and security.

6 Conclusions

Based on the security analysis of traditional blind signature, this paper reveals that the public information is easy leaked. To solve this problem, this paper proposes an identity-based identity blind signature scheme. The new scheme does not use the bilinear pairings with the largest computational overhead, and can effectively resist tampering with public information attacks. Compared with the existing schemes, the new scheme has significant improvement in efficiency and safety.

Acknowledgments

This work is supported by the Natural Science Fund Guiding Program in Liaoning Province (Grant No.20180520024).

References

[1] X. Q. Cai, Y. H. Zheng, R. L. Zhang, "Cryptanalysis of a batch proxy quantum blind signature scheme," *International Journal of Theoretical Physics*, vol. 53, no. 9, pp. 3109-3115, 2014.

[2] H. J. Cao, Y. F. Yu, Q. Song, *et al.*, "A quantum proxy weak blind signature scheme based on controlled quantum teleportation," *International Journal of Theoretical Physics*, vol. 54, no. 4, pp. 1325-1333, 2015.

[3] L. Ergen, Z. Huajing, Z. Liming, *et al.*, "Analysis and improvement of an ID-based partially blind signature scheme," *Journal of Henan Normal University*, 2016.

[4] C. I. Fan, W. Z. Sun, S. M. Huang, "Provably secure randomized blind signature scheme based on bilinear pairing," *Computers & Mathematics with Applications*, vol. 60, no. 2, pp. 285-293, 2010.

[5] D. He, J. Chen, R. Zhang, "An efficient identity-based blind signature scheme without bilinear pairings," *Computers and Electrical Engineering*, vol. 37, no. 4, pp. 444-450, 2011.

[6] B. F. Hernandez, B. J. Morgan, J. Ish, *et al.* "Communication preferences and satisfaction of secure messaging among patients and providers in the military healthcare system," *Military Medicine*, vol. 183, no. 3, 2018.

[7] R. F. Huang, Q. Nong, "Efficient certificate-based blind signature scheme without bilinear pairings," *Applied Mechanics & Materials*, pp. 2735-2739, 2012. (`https://doi.org/10.4028/www.scientific.net/AMM.220-223.2735`)

[8] T. Lin, L. Hang, L. Jie, Y. Shoulin, "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.

[9] H. Li, S. L. Yin, C. Zhao and L. Teng, "A proxy re-encryption scheme based on elliptic curve group," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 1, pp. 218-227, Jan. 2017.

[10] P. L. D. Santos, I. H. Kvangraven, "Better than cash, but beware the costs: Electronic payments systems and financial inclusion in developing economies," *Development & Change*, vol. 48, no. 2, pp. 205-227, 2017.

[11] M. Specifically, "An efficient identity-based proxy blind signature for semioffline services," *Wireless Communications and Mobile Computing*, pp. 1-9, 2018. (`https://doi.org/10.1155/2018/5401890`)

[12] L. Teng, H. Li, "A high-efficiency discrete logarithm-based multi-proxy blind signature scheme," *International Journal of Network Security*, vol. 20, no. 6, pp. 1200-1205, 2018.

[13] S. L. Yin and J. Liu, "A K-means approach for map-reduce model and social network privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1215-1221, Nov. 2016.

[14] S. Yin, H. Li and J. Liu, "A new provable secure certificateless aggregate signcryption scheme," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1274-1281, Nov. 2016.

[15] Y. Yoo, R. Azarderakhsh, A. Jalali, *et al.*, "A post-quantum digital signature scheme based on supersingular isogenies," in *International Conference on Financial Cryptography & Data Security*, 2017. (`https://eprint.iacr.org/2017/186.pdf`)

[16] H. Zhu, Y. A. Tan, L. Zhu, *et al.*, "An identity-based anti-quantum privacy-preserving blind authentication in wireless sensor networks," *Sensors*, vol. 18, no. 5, pp. 1663, 2018.

Shoulin Yin biography. He received the B.Eng. and M.Eng. degree from Shenyang Normal University, Shenyang, Liaoning province, China in 2016 and 2013 respectively. Now, he is a doctor in Harbin Institute of Technology. His research interests include Multimedia Security, Network Security, Filter Algorithm, image processing and Data Mining. Email:352720214@qq.com.

Hang Li biography. He obtained his Ph.D. degree in Information Science and Engineering from Northeastern University. Hang Li is a full professor of the software college at Shenyang Normal University. His interests are wireless networks, mobile computing, cloud computing, social networks, network security and quantum cryptography. Prof. Li had published more than 30 international journal and international conference papers on the above research fields. Email:lihangsoft@163.com.

Shahid Karim biography. Shahid Karim received his BS degree in electronics from Comsats Institute of Information Technology, Abbottabad, Pakistan, and his MS degree in electronics and information engineering from Xi'an Jiaotong University, China, in 2010 and 2015, respectively. He is currently pursuing his PhD at the Department of Information and Communication Engineering, School of Electronics and Information Engineering, Harbin Institute of Technology (HIT), China. His current research interests include image processing, object detection, and classification toward remote sensing imagery. Email: shahidhit@yahoo.com.

A Sensitive-Information Hiding Treatment in Quick-Response Codes Based on Error-Correcting Framework

Mingwu Zhang[1,2], Xiao Chen[2], Yong Ding[1], and Hua Shen[2]
(Corresponding author: Mingwu Zhang)
School of Computer Science and Information Security, Guilin University of Electronic Technology[1]
1 Jinji Rd, Qixing, Guilin, Guangxi 541004, China
School of Computer Science, Hubei University of Technology[2]
(Email: scauzhang@gmail.com)
(Received June 20, 2019; Revised and Accepted Dec. 10, 2019; First Online Feb. 1, 2020)

Abstract

Quick Responding codes, namely QR codes, are widely used in various communication applications and electronic transactions such as electronic payments and information integrations, since they provide excellent characteristics such as *large data capacity*, *widely coding domain*, and *stronger error correction ability etc.* However, as the QR code is transmitted on public channel and can be scanned by any QR reader, one can obtain the data from the encoded QR code. Simultaneously, the encoding and decoding algorithms are public, the sensitive data such as paying account and password will be revealed to the QR reader, which might incubate the risk of privacy leakage.

For solving this problem, this paper proposes a novel approach to protect the private data in QR code. In our method, the secret information is embedded in the random position of a QR code matrix by utilizing an *error-correcting mechanism*, and only authorized user in possession of required keys will be able to retrieve and recover this secret data embedded and hidden in the QR code. The user without the secret key can only decode public information from the QR code. Although our hiding scheme will decrease the rate of error-correctness of QR decoding, we indicate that the analysis shows that scheme is effect om practical applications. Compared with related schemes, the proposed scheme provides higher security that is less likely to attract the attention of potential attackers.

Keywords: Data Hiding; Error-Correcting Code; Privacy Preservation; Quick Response Code

1 Introduction

Compared with traditional one-dimensional code, two-dimensional QR code provides higher storage and error correction capabilities, therefore, the QR code has been widely used in the practical application such as data input interface [14], object tracking [10], mobile payment [12], and product marketing [2] *etc.* Even though the QR code is used extensively and has many desirable properties, it still exists some security and privacy issues [7]. Because the QR code is transmitted over common channels and the encoding and decoding algorithms are public, the encoded and embedded message can be obtained by decoding the QR code with a QR reader. If a sender tries to employ two-dimensional codes to transmit private information, *i.e.*, paying account and password in QR code, will be revealed, abd thus there will lead to serious privacy leakage problems.

Generally, to protect the privacy of QR codes, the sensitive data can be stored in a back-end database, and the end users can obtain this private data by accessing to database linked with QR code URL [16, 18]. However, the URL that links to back-end databases might attract intruders' attention, which will lead to potential risks. In previous works, most of the researches on QR codes usually introduce typical security mechanism such as image steganography and text encryption, however they ignore the characteristics of the QR code and can not used in QR coding environment explicitly.

Li *et al.* [8] devised a paper-based document and credentials protection scheme using authenticatable QR barcode. In 2012, Eldefrawy *et al.* [3] proposed a document authentication scheme that is based on public-key encryption in two-dimensional QR code, which focuses on the QR code authentication with a public encryption mechanism. However, public-key encryption methods not only require heavy computational power but also attract the attention of attackers, as the QR is encoded into a cipher form. The digital watermarking schemes [4, 11, 13, 17], embedded a watermark into the high-frequency part of a QR image, can also protect the copyright of QR image, however because the pixels in QR codes are only the

blocks of white or black, which is inefficient for the digital watermarks.

Recently, several image hiding schemes that treat the QR code as a secret image and then embed the QR code into the special domain of an image. Huang *et al.* [5] proposed a reversible data embedding approach for hiding a QR code in special areas of an image. Wu *et al.* [15] devised a data embedding method for an image using QR codes. However, embedding QR code into the domains of an image will reduce the quality of the image, and the schemes in [5,15] do not take advantage of the characteristics of encoding approach of QR Code itself.

For the encoding of QR code in ISO standard ISO/IEC18004 [6], to avoid the error or damage of a QR code, it uses the error correction mechanism, *i.e.*, Reed-Solomon code (RS code), to allow the data to be recovered even if its portions are damage. Lin *et al.* [9] proposed a scheme for embedding secret data in a QR code, which exploits the error correction redundancy property of QR code. Later, Chow *et al.* [1] developed an efficient scheme, namely covert QR code, for hiding a secret QR code into a specific area of a public QR code and the only authorized user could retrieve the secret. However, the scheme proposed by Chow *et al.* [1] can extract codewords by obtaining the difference between covert QR code and the original QR code, which means that if some part of the covert QR is damaged, the embedded codewords can not be correctly extracted, whereby the hidden secret data can not be recovered.

In this paper, we propose an efficient approach for embedding a secret data into a QR code, in which the codewords of secret data are embedded into random positions of encoding matrix of public QR code by employing error correction redundancy. In order to embed the sensitive data into the QR codes by encoding the sensitive data in replace of the area of error-correct code. Our contribution is described as follows.

1) We provide a novel approach to encode the private data into secret data in replace of the area of error-correct code. In the proposed scheme, the secret data and its Reed-Solomon error correction code are embedded in the QR code together, which ensures that the secret data can be decoded correctly even if it is damaged or modified.

2) In the correction process of the QR reading, the basic computational unit is one byte, even destroying or modifying any bit or bits within a given byte could produce the same effect on the error correction performance. Thus, the processing unit of our scheme needs only one byte, which can embed as much data as possible with a given error rate.

3) In our scheme, the secret information codewords are embedded into the random positions of QR encoding matrix and also can be recovered secretly, in which it hardly attracts the extra attention of potential attackers.

Table 1: Notations and symbols

Symbols	Remark
P	Public message
M	Secret data
$\vec{P}$	Final codewords sequence of public message
$\vec{C}$	Codewords sequence of encrypted secret message
$\vec{C}^*$	Final codewords sequence of encrypted secret message
k	Symmetric secret key
k_l	Location secret key
$\vec{L}$	The sequence of location information
$\vec{P}^*$	Codeword sequence of public message embedded with secret message

The rest of this paper is organized as follows. In Section 2, we provide some preliminaries and our security requirements. We present our scheme in Section 3, and analyze and discuss the correctness and security in Section 4. The conclusion is drawn in Section 5.

2 Preliminaries

In this section, we first outline the structure and coding process of the QR code according to the QR code bar code symbology specification (ISO/IEC18004) [6] which promulgated by the international standard organization, and then we briefly introduce RS error correction code. Finally, we describe the security model of the proposed scheme.

2.1 Notations

We denoted assigning the output of an algorithm A, which takes x as input to z by $\mathsf{A}(x) \rightarrow z$. We list the notations and terms in this paper in Table 1.

2.2 Encoding of QR codes

Each QR code symbol is composed of nominal square modules set out in a regular square array, which consists of a encoding region and a function patterns (namely, finder pattern, separator pattern, timing pattern, and alignment pattern, respectively). Encoding region contains the symbol characters representing data, those representing error correction codewords, the format information and the version information, which will provide the basis for decoding. On the contrary, the pattern cannot be used for data encoding and the symbols are surrounded by blank areas. Figure 1 illustrates the structure of a QR Code with version 7.

The QR code encoding process as shown in Figure 2 [6]. Data encoding includes converting data characters into

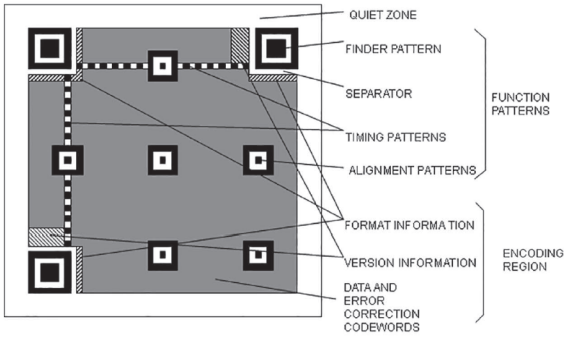


Figure 1: Structure of QR code framework

bit streams and then split the resulting bit stream into 8-bit codewords. The codeword sequence is divided into required blocks so that the error correction algorithm can be processed. Error correcting codewords are generated for each block, and the error correcting codewords are appended to the end of the data code sequence so that in case of damage of the codeword can still be identified correctly. The steps in Figure 2 are described in detail as follows:

1) *Data analysis*: Analyze the input data stream to identify the variety of different characters to be encoded.

2) *Data encoding*: Convert the data characters into a bit stream in accordance with the rules for the mode in force.

3) *Error correction coding*: Divide the codeword sequence into the required number of blocks to enable the error correction algorithms to be processed.

4) *Structure final message*: Interleave the data and error correction codewords from each block as described in and add remainder bits as necessary.

5) *Module placement in matrix*: Place the codeword modules in the matrix together with the Finder Pattern, Separators, Timing Pattern, and Alignment Patterns.

6) *Data masking*: Employ the masking patterns in turn to the encoding region of the symbol, and then evaluate the results and select the pattern which optimizes the dark/light module balance and minimizes the occurrence of undesirable patterns.

7) *Format and version information*: Generate the format and applicable version information, and then output the symbol finally.

2.3 Error Correction of QR Encode

QR code adopts Reed-Solomon error control coding to detect and correct errors while the QR is damaged, in which the error-correcting codewords can correct two types of errors, *i.e.*, *rejection error* such that the location of the error codeword is known and replacement error such that the location of the error codeword is unknown. Informally, a rejection error is a symbol character that has not been scanned or can not be decoded.

Table 2: Error correction levels in QR code

Error correction level	Recovery capacity % (approx.)
L (low)	7
M (medium)	15
Q (quality)	25
H (high)	30

A replacement error is a symbol character that has been decoded incorrectly, for example, it changes a dark module (bit 1) into a light module (bit 0) or a light module into a dark module, and the symbol characters are misinterpreted as superficially valid, but they are different codewords, which replacements error requires two error correcting codewords to correct.

Based on the feature of error correction code technology, the error correction code redundancy of the QR code can also be employed for data hiding. For example, we put the encoded sensitive data into the area of error correction. The error correction levels of the QR code is related to the embeddable capacity of secret data in a QR code. The QR code standard offers four kinds of error correction levels that is shown in Table 2.

2.4 The Model

In order to clarify the security model, we use following natations to indicate possible inputs and outputs of various algorithm:

Definition 1. *(PQR Scheme, PQRS). A perforated QR code scheme PQRS consists of the following algorithms:* $\mathsf{PQRS} = (\mathsf{Setup}, \mathsf{QRC}, \mathsf{QRD}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{RLG}, \mathsf{RS}, \mathsf{Embed}, \mathsf{Extract})$*, whose functionalities are described as follows:*

- $\mathsf{Setup}(1^\lambda) \rightarrow k$*: Taking a security parameter* λ *as input, this algorithm returns a secret key* k*.*
- $\mathsf{QRC}(M) \rightarrow QR_M$*: Taking a message* M *as input, this algorithm returns a QR code* QR_M *for* M*.*
- $\mathsf{QRD}(QR_M) \rightarrow M$*: Taking a QR code* QR_M *as input, this algorithm outputs a message* M *for* QR_M*.*
- $\mathsf{Enc}_k(M) \rightarrow \vec{C}$*: This algorithm takes a plaintext* M *and a secret key* k *as inputs, and outputs the corresponding ciphertext bytes array* $\vec{C}$*.*
- $\mathsf{Dec}_k(\vec{C}) \rightarrow M$*: This algorithm takes a ciphertext bytes array* $\vec{C}$ *and a secret key* k *as inputs, and returns the corresponding plaintext* M*.*

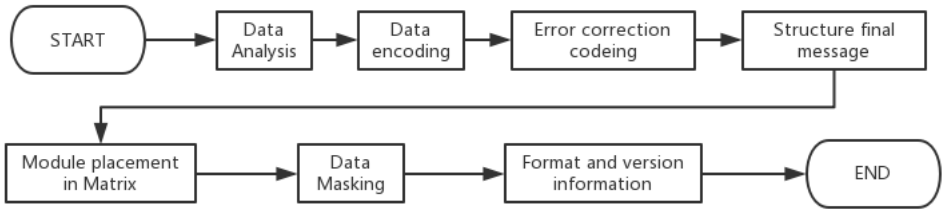


Figure 2: Encoding procedure

- $RLG(k, n, Max) \rightarrow \vec{L}$: *Using the key k and a bounded number Max as input, this algorithm outputs an array of pseudo-random numbers $\vec{L}$. Note that the array element is no more than Max and n is the array's length.*
- $RS(\vec{A}) \rightarrow \vec{A}^*$: *This algorithm takes an array of bytes $\vec{A}$ as input, and returns its RS code $\vec{A}^*$.*
- $Embed(P, M, k) \rightarrow PQR$: *This algorithm takes a public message P, a secret data M, and a secret key k as inputs, and generates a perforated QR code PQR.*
- $Extract(PQR, k) \rightarrow M$: *This algorithm takes a perforated QR code PQR and a secret key k as inputs, and outputs the secret data M.*

Correctness. For a public QR code $QR_P \leftarrow \mathsf{QRC}(P)$ where P is a public message, and a perforated QR code $PQR \leftarrow \mathsf{Embed}(P, M, k)$, the following conditions should hold:

1) $\mathsf{QRD}(QR_P) = \mathsf{QRD}(PQR) = P$;
2) $\mathsf{Extract}(PQR, k) = M$.

Note that in the scheme, we employ a symmetric key encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$ under key k, which can be separately deployed with any secure symmetric encryption algorithm such as AES. The security is described as: Let $\mathcal{A}$ be an adversary whose running time is polynomial. We say that the PQRS scheme is secure if there exists a negligible function such that

$$\Pr[M \leftarrow \mathcal{A}(PQR)] \leq \varepsilon(\lambda). \quad (1)$$

3 Our Scheme

In this section, we present a sensitive-data hiding scheme that embeds the secret into a QR code. Figure 3 illustrates an overview of the proposed scheme, in which the encoding procedure is generally divided into four steps.

1) At first, it extracts the codewords sequence of public message $\vec{P}$ in public QR code.
2) Then, it call the encryption algorithm to generate the encrypted secret data codeword sequence $\vec{C}$, and then creates the error-correcting codeword sequence of $\vec{C}$ that is connected with the end of encrypted secret codeword sequence $\vec{C}$ to obtain the final ciphertext of codeword $\vec{C}^*$.
3) Calling the key k of the seed of pseudo-random number generator to generate a random location sequence $\vec{L}$. Afterward, $\vec{C}^*$ is embedded into the $\vec{P}$ according to the location information provided by $\vec{L}$ in the unit of codeword, and obtains a codeword sequence $\vec{P}^*$ embedded with secret data. After that, it place $\vec{P}^*$ codeword modules in the matrix together with the finder pattern, separators, timing pattern, respectively, and adds the additional format and version information.
4) Finally, it calls the encoding algorithm to create the patched QR code.

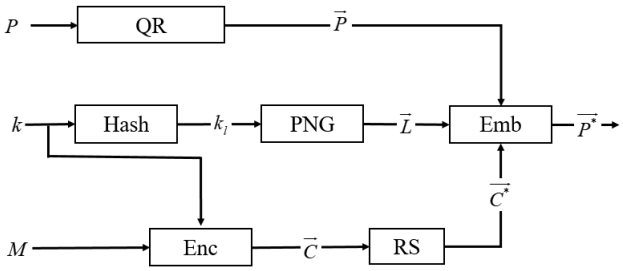


Figure 3: Overview of data-hiding procedure of the proposed scheme

According to the error correction mechanism of QR code, as long as the number of code words replaced is less than its error correction ability, the use of a standard QR code reader to scan and decode PQR code will generate public message $\vec{P}$. On the other hand, for individuals who have the secret key k, they only need to input PQR code and k in the secret extraction algorithm to extract the secret codeword sequence $\vec{C}^*$, and then correct and decrypt it to obtain the secret data M.

3.1 PQR Embedding Procedure

The purpose of embedding procedure is to embed the encrypted secret codeword sequence $\vec{C}^*$ into the random positions associated with public codeword sequence $\vec{P}$. The PQR embedding algorithm is described in Algorithm 1. Using the secret key k to place the codeword modules in

the matrix, a standard QR code, *i.e.*, PQR, is formed. If we call the standard QR code reader to decode PQR, only public message P can be achieved. However, for a user who owns the symmetric secret key k, by calling the extract algorithm he can obtain the secret data M from PQR code.

We now take a version 5 and encoding level L as an example: The QR code has 134 codewords including 26 error-correcting codewords. And thus it can accept up to 13 replacement errors. Let

$$\begin{aligned} \vec{P} &= (p_1, p_2, \cdots, p_{134}), \\ \vec{C^*} &= (c_1, c_2, c_3, c_1^*, c_2^*), \\ \vec{L} &= (101, 8, 9, 68, 19). \end{aligned}$$

Then, we have

$$\vec{P^*} = (p_1, \cdots, p_7, c_2, c_3, p_{10}, \cdots, p_{18}, c_2^*, p_{20}, \cdots, p_{67}, c_1^*, p_{69}, \cdots, p_{100}, c_1, p_{102}, \cdots, p_{134}).$$

3.2 PQR Extracting Procedure

The PQR extraction algorithm is described in Algorithm 2.

4 Analysis and Discussion

Table 3 lists the respective total number of codewords, number of error correction codewords, number of error correction blocks and the error correction code per block (c, k, r) for three standard versions of the QR code, where c denotes the total of codewords, k is the number of data codewords and r indicates the error correction capacity. For instance, an error correction code of version 5-M is represented as $(67, 43, 12)$, which indicates that the error correction algorithm can correct less than 9 replacement errors in the block. Notice that, the higher error correction capacity the higher version with more redundancy. As shown in Table 3, it shows the embeddable capacity of secret data under different QR versions and error correction levels.

As shown in Section 3.2, since the number of modified codewords is less than the error-correcting ability, decoding a PQR with a standard decoder can only obtain public information P. However, a key-holder could use a special QR code reader, equipped with Extract algorithm, can restore the secret data M. That is,

$$\begin{aligned} \mathsf{QRD}(QR_P) &= \mathsf{QRD}(PQR) = P \\ \mathsf{Extract}(PQR, k) &= M. \end{aligned}$$

Suppose that an adversary can suspect the secret information of the propose scheme. It is easily for an adversary to obtain the encrypted codewords by comparing and distinguishing between the generated original QR codes and the PQR code. The adversary can obtain the information of the number of embedded codewords. However, the

Algorithm 1 Framework of PQR embedding/encoding procedure.

Require:
Public message P;
Sensitive data M;
Secret key k.

Ensure: QR code PQR that encode P and hide M.

1: Call the QR code standard algorithm to generate QR code of public message P and extract its data codeword sequence $\vec{P} = (p_1, p_2, \cdots, p_n)$, where p_k $(1 \geq k \geq n)$ is an 8-bit binary sequence.
2: Compute the value of modifiable capacity $N = \lfloor E/2 \rfloor$, where E is the number of error correction codewords in $\vec{P}$.
3: Using key k to encrypt the secret data, $\mathsf{Enc}_k(M) \rightarrow \vec{C}$, $\vec{C} = (c_1, c_2, \cdots, c_i)$ is codeword sequence of encrypted secret data, c_k $(1 \geq k \geq i)$ is an 8-bit binary sequence.
4: Generate the RS code of $\vec{C}$, $\mathsf{RS}(\vec{C}) \rightarrow \vec{C^*}$, where $\vec{C^*}$ is final codewords sequence of encrypted secret, $\vec{C^*} = (c_1, c_2, \cdots, c_i, c_1^*, c_2^*, \cdots, c_j^*)$, $(c_1^*, c_2^*, \cdots, c_j^*)$ is error correction coding of $\vec{C}$, and c_k^* $(1 \geq k \geq j)$ is an 8-bit binary sequence. Note that $(i + j) \leq n$, because the number of replaced codewords is less than the modifiable capcity.
5: Generate the location information with pseudo-random number generator $\vec{L} = \mathsf{PRNG}(k_l, i + j, n)$, where $k_l = H(k)$, n is the the total number of $\vec{P}$, $\vec{L} = (l_1, l_2, \cdots, l_{i+j})$, $1 \geq l_k \geq n$, $(1 \geq k \geq i + j)$, $l_k \notin \{l_1, l_2, \cdots, l_{k-1}\}$.
6: Embed the final codewords sequence of secret data $\vec{C^*}$ into the codewords sequence of public message $\vec{P}$ according to the sequence of location information $\vec{L}$, in other word, replace $(c_1, c_2, \cdots, c_i, c_1^*, c_2^*, \cdots, c_j^*)$ with $(p_{L_1}, p_{L_2}, \cdots, p_{L_{i+j}})$ in $\vec{P}$ according to sequence, and obtain the codeword sequence of public message embedded with secret data $\vec{P^*}$.
7: Update the codeword sequence of public message embedded with secret data $\vec{P^*}$ in the QR's matrix to obtain the QR code (PQR) that contains the public message P and secret data M.
8: **return** PQR;

Table 3: Embeddable capacity under different QR versions and error correction levels

version	# of codewords	error correction level	# of error correction codewords	# of error correction blocks	error correction code per block (c, k, r)	embeddable capacity
5	134	L	26	1	(134,108,13)	13
		M	48	2	(67,43,12)	24
		Q	72	2 2	(33,15,9) (34,16,9)	36
		H	88	2 2	(33,11,11) (34,12,11)	44
7	196	L	40	2	(98,78,10)	20
		M	72	4	(49,31,9)	36
		Q	108	2 4	(32,14,9) (33,15,9)	54
		H	130	4 1	(39,13,13) (40,14,13)	65
10	346	L	72	2 2	(86,68,9) (87,69,9)	36
		M	130	4 1	(69,43,13) (70,44,13)	65
		Q	192	6 2	(43,19,12) (44,20,12)	96
		H	224	6 2	(43,15,14) (44,16,14)	112

Algorithm 2 Framework of PQR extracting procedure.

Require:
QR code contains public message P and PQR;
The secret key, k.

Ensure: extracted secret data M.

1: Extract codeword sequence in PQR, and obtain $\vec{P}^{'} = (p_1^{'}, p_2^{'}, ..., p_n^{'})$.
2: Generate the location information with pseudo-random number generator $\vec{L}^{'} = \mathsf{PRNG}(k_l^{'}, i+j)$, where $k_l^{'} = H(k^{'})$, $H(\cdot)$ is a one way (hash) function. Note that n is the total number of $\vec{P}^{'}$, $\vec{L}^{'} = (l_1^{'}, l_2^{'}, \cdots, l_{i+j}^{'})$, $1 \geq l_k^{'} \geq n$, $(1 \geq k \geq i+j)$, $l_k^{'} \notin \{l_1^{'}, l_2^{'}, \cdots, l_{k-1}^{'}\}$.
3: Extract the codeword sequence corresponding to the location information $\vec{L}^{'}$ in $\vec{P}^{'}$, where $\vec{C^*}^{'} = (p_{l_1}^{'}, p_{l_2}^{'}, \cdots, p_{l_{i+j}}^{'})$.
4: Call the error-correcting algorithm to set $\vec{C^*}^{'} = (p_{l_1}^{'}, p_{l_2}^{'}, \cdots, p_{l_{i+j}}^{'})$. To distinguish the original information, we write the corrected codeword to denote as $\vec{C}^{'} = (c_1^{'}, c_2^{'}, \cdots, c_i^{'})$.
5: Decrypt the codewords sequence to obtain the secret data: $\mathsf{Dec}_k(\vec{C}^{'}) \rightarrow M$.
6: **return** M.

adversary can not obtain the correct order of these codewords and he cannot decrypt these codewords without secret key k. We assume that the number of embedded codewords to be n, then the length of the random bits r-bit used in encrypting the codewords is $8n$. Therefore, the probability of the adversary $\mathcal{A}$ obtaining a correct message can be computed by

$$\begin{aligned} & \Pr[\mathcal{A} \text{ succeed in outputting } M] \\ = \; & \Pr[\mathcal{A} \text{ finds correct r-bit \& codeword order}] \\ \leq \; & \frac{1}{n!} \cdot \frac{1}{2^{8n}} \\ = \; & \frac{1}{n! \times 256^n} \end{aligned}$$

5 Conclusion

This paper proposed a novel sensitive data hiding scheme by embedding the sensitive information into a QR code, in which it employs the technique of error correction mechanism in QR encoding system to embed the secret codeword sequence into the random position of the QR encoding matrix. When we used the two-dimensional QR code reader to read the QR code, it can effective extract the encoded public information. Simultaneously, an authorized users who owned the secret key would be able to obtain the secret information in the hidden QR code.

Acknowledgements

Supported by organization the National Natural Science Foundation of China (61672010, 61702168), the Hubei Provincial Department of Education Key Project (D20181402), the open research project of The Hubei Key Laboratory of Intelligent Geo-Information Processing (KLIGIP-2017A11), the Hubei University of Technology Doctoral Startup Fund (BSQD14035).

References

[1] Y. Chow, W. Susilo, and J. Baek, "Covert QR codes: How to hide in the crowd," in *International Conference on Information Security Practice and Experience*, pp. 678–693, 2017.

[2] M. Ebling and R. Cáceres, "Bar codes everywhere you look," *IEEE Pervasive Computing*, vol. 9, no. 2, pp. 4–5, 2010.

[3] M. H. Eldefrawy, K. Alghathbar, and M. K. Khan, "Hardcopy document authentication based on public key encryption and 2D barcodes," in *International Symposium on Biometrics and Security Technologies*, pp. 77–81, 2012.

[4] M. Gao and B. Sun, "Blind watermark algorithm based on QR barcode," in *Foundations of Intelligent Systems*, pp. 457–462, 2011.

[5] H. Huang, F. Chang, and W. Fang, "Reversible data hiding with histogram-based difference expansion for QR code applications," *IEEE Transactions on Consumer Electronics*, vol. 57, no. 2, pp. 779–787, 2011.

[6] ISO/IEC, "Information technology automatic identification and data capture techniques QR code bar code symbology specification," *International Standard, ISO/IEC*, 18004, 2015. (`https://www.iso.org/standard/43655.html`)

[7] P. Kieseberg, M. Leithner, M. Mulazzani, L. Munroe, S. Schrittwieser, M. Sinha, and E. Weippl, "QR code security," in *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia*, pp. 430–435, 2010.

[8] C. M. Li, P. Hu, and W. C. Lau, "Authpaper: Protecting paper-based documents and credentials using authenticated 2D barcodes," in *IEEE International Conference on Communications (ICC'15)*, pp. 7400–7406, 2015.

[9] P. Lin, Y. Chen, J. LU, and P. Chen, "Secret hiding mechanism using QR barcode," in *International Conference on Signal-Image Technology & Internet-Based Systems*, pp. 22–25, 2013.

[10] N. Park, W. Lee, and W. Woo, "Barcode-assisted planar object tracking method for mobile augmented reality," in *International Symposium on Ubiquitous Virtual Reality*, pp. 40–43, 2011.

[11] G. Prabakaran, R. Bhavani, and M. Ramesh, "A robust QR-code video watermarking scheme based on SVD and DWT composite domain," in *International Conference on Pattern Recognition, Informatics and Mobile Engineering*, pp. 251–257, 2013.

[12] H. Ranavat, L. Chang, V. Kulkarni, J. Gao, and H. Mei, "A 2D barcode-based mobile payment system," in *The Third International Conference on Multimedia and Ubiquitous Engineering*, pp. 320–329, 2009.

[13] M. Sun, J. Si, and S. Zhang, "Research on embedding and extracting methods for digital watermarks applied to QR code images," *New Zealand Journal of Agricultural Research*, vol. 50, no. 5, pp. 861–867, 2007.

[14] R. Villn, S. Voloshynovskiy, O. Koval, and T. Pun, "Multilevel 2D bar codes: Toward high-capacity storage modules for multimedia security and management," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 4, pp. 405–420, 2006.

[15] W. Wu, Z. Lin, and W. Wong, "Application of QR-code steganography using data embedding technique," in *Information Technology Convergence*, pp. 597–605, 2013.

[16] M. Zhang, J. Huang, H. Shen, Z. Xia, and Y. Ding, "Consecutive leakage-resilient and updatable lossy trapdoor functions and application in sensitive big-data environments," *IEEE Access*, vol. 6, pp. 43936–43945, 2018.

[17] M. Zhang, Y. Yao, B. Li, and C. Tang, "Accountable mobile E-commerce scheme in intelligent cloud system transactions," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 6, pp. 1889–1899, 2018.

[18] M. Zhang, Y. Zhang, Y. Jiang, and J. Shen, "Obfuscating eves algorithm and its application in fair electronic transactions in public clouds," *IEEE Systems Journal*, vol. 13, no. 2, pp. 1478–1486, 2019.

Biography

Mingwu Zhang is a Professor at School of Computer Sciences and Information Security, Guilin University of Electronic Technology, China. He received his M.Sc. in Computer Science and Engineering from Hubei Polytechnic University in 2000 and the Ph.D. degree in South China Agric University in 2009, respectively. From August 2010 to August 2012, he has been a JSPS postdoctoral fellow at Institute of Mathematics for Industry in Kyushu University. From June 2015 to June 2016, he is a senior visiting professor at School of Information and Computing Science, University of Wollongong. His research interests include cryptography technology for network and data security, secure computation and privacy preservation.

Xiao Chen is now a master student at the School of Computers, Hubei University of Technology. His research interest focuses on the security of electronic and quick-responding barcode.

Yong Ding received the Ph.D. degree in cryptography

from Xidian University, China. He is a Professor and the Director of the Guangxi Key Laboratory of Cryptography and Information Security. His main research interests include cloud security, cryptography, and information security.

Hua Shen received the M.S. and Ph.D. degrees from Wuhan University, Wuhan, China, in 2007 and 2014, respectively. She is currently an Associate Professor with the School of Computer Science, Hubei University of Technology. Her research interests include privacy preserving, information security, and cloud computing *etc.*

Information Aggregation Method of Intuitionistic Fuzzy Set Pair Analysis in Multi-Attribute Privacy Risk Decision-Making

Yan Yan, Bingqian Wang, Lianxiu Zhang, and Xin Gao

(Corresponding author: Yan Yan)

School of Computer and Communication, Lanzhou University of Technology
No.287 Langongping Road, Qilihe District, Lanzhou 730050, China
(Email: yanyan@lut.edu.cn)

(Received June 29, 2019; Revised and Accepted Dec. 3, 2019; First Online Feb. 1, 2020)

Abstract

Big data system has the features of dynamic, complexity and uncertainty. Privacy risk assessment can be used to discover the factors that threaten privacy, determine the degree of privacy leakage, and estimate the trend of privacy leakage development. In this paper, intuitionistic fuzzy set pair analysis (IFSPA) is proposed by combining intuitionistic fuzzy and set pair analysis theory. Relevant concepts, algorithms and ranking methods are defined. In order to improve the information aggregation effect, IFSPA weighted average operator (IFSPAWA), IFSPA weighted geometric operator (IFSPAWG), IFSPA ordered weighted average operator (IFSPAOWA), IFSPA ordered weighted geometric operator (IFSPAOWG), IFSPA hybrid average operator (IFSPAHA), IFSPA hybrid geometric operator (IFSPAHG) and their properties are designed. A multi-attribute privacy risk decision-making approach is proposed. Finally, the feasibility and effectiveness of this method are verified through the analysis of specific examples.

Keywords: Aggregation Operator; Intuitionistic Fuzzy (IF); Multi Attribute Decision Making (MADM); Privacy Risk Assessment; Set Pair Analysis (SPA)

1 Introduction

Big data has the characteristics of huge volume and fast update speed, which not only brings convenience to people but also causes many security risks. Improper or uncontrolled collection, storage, use and distribution of users' information may not only result in the disclosure of personal privacy information, but also endanger their life and property security [2, 11, 13]. Privacy risk assessment is important and realistic for reducing privacy leaks and improving information security. However, the factors that lead to privacy risks are all-encompassing, and the methods of privacy risk assessment are different. In addition, the uncertainty, randomness and ambiguity introduced from various aspects such as generation, collection, storage and distribution of big data make privacy risk assessment both a MADM problem and an uncertainty problem.

Intuitionistic fuzzy set theory [1] describes the ambiguity of things by membership function and non-membership function, which is more accurate and effective than the traditional fuzzy set theory [18]. The essence of IF set theory is the same as that of vague set theory [6]. The shortcoming of both is that they can not describe the state of critical transition between membership degree and non-membership degree (or between true membership degree and false membership degree). Set pair analysis theory [19] starts out from the globality of system, analyze the relations, constraints and influences of things, and establish the connection function to describe the support (or affirmative), uncertain (or hesitant), negative (or objection) state of things, depict the ambiguity, certainty, uncertainty as well as the change of state in things. Set pair analysis theory is more accurate and effective in describing fuzzy uncertain information. The processing way of fuzzy information for set pair analysis is closer to human's cognitive thinking, which effectively makes up for the deficiencies of fuzzy sets, IF sets and vague sets.

So far, there have been many achievements on the research of IF and SPA in decision-making systems. Liu *et al.* [8] proposed operation laws for intuitionistic normal fuzzy numbers and intuitionistic normal fuzzy aggregation operators with prioritization relationships. Shi *et al.* [14] and Yan *et al.* [15] applied the multiple connection number set pair analysis theory into different risk assessment application, and used uncertainty hierarchy analysis to determine the weight range of each assessment index. Liu *et al.* [12] studied the operation property and conversion of set pair analysis interval numbers, MADM method of connection numbers, intuitionistic decision-

making with three-parameters, multi-attribute set pair analysis method with four-parameters, set pair analysis of IF MADM and linguistic interval numbers. Harish *et al.* [5] presented a nonlinear-programming (NP) model based on interval-valued intuitionistic fuzzy (IVIF) technique to solve MADM problems. In their approach, both ratings of alternatives and weights are represented by IVIF sets. The NP models are constructed on the concepts of relative-closeness coefficient and the weighted distance, and some NP models are further deduced to calculate relative-closeness of sets of alternatives, which can be used to generate the ranking order of the alternatives. Traditional MADM problems with IF information are mainly focused on an binary relation. However, real problems can not be effectively solved by an IF relation. In order to solve these issues, Zhang *et al.* [20] proposed two methods based on covering-based generalized IF rough sets as well as covering-based generalized fuzzy rough sets. Comparative analysis show that the results of covering-based generalized IF rough set models and covering-based generalized fuzzy rough set models are highly consistent. Yuan *et al.* [16] proposed intuitionistic fuzzy entropy (IFE) to overcome the shortcomings of history studies that neglect hesitancy degree and uncertainty degree. They proposed a new decision-making method based on entropy and evidential reasoning for IF multi-attribute group decision-making problems with unknown or partially unknown weight information. Liu *et al.* [9,10] extended the partitioned Heronian mean operator and the Bonferroni mean operator, and develop some new operational rules of linguistic intuitionistic fuzzy number to consider the interactions between membership function and non-membership function. Harish [4] presented a new strategy for solving MADM problem by using different entropies and unknown attribute weights, where preferences related to the attributes are in the form of interval-valued IF sets.

Although IF and SPA can effectively express uncertain, fuzzy and stochastic problems within a certain range, there are still some shortcomings and deficiencies. IF sets can better represent the fuzzyness of support and opposition status, but is powerless in describing the state of critical transition between them. SPA method can better describe certainty and uncertainty among the states of support (or affirmative), uncertain (or hesitant) and negative (or objection), but can not reflect the trend from anomaly to homomorphism and the anti-state changes. In view of the above problems, the intuitionistic fuzzy set pair analysis (IFSPA) method is proposed by combining the two. Relevant concepts, operation rules and ranking methods are provided and applied in MADM problems for privacy risk assessment.

2 Definition and Properties of IF-SPA

Definition 1. *Given two associated sets N and M, composing the pair $A = (N, M)$, X is any non-empty set on A, $A = \{< x, a_A(x), b_A(x), c_A(x) > | \, x \in X\}$ is denoted as the set pair of X on A.*

Where $a_A(x)$, $b_A(x)$, $c_A(x)$ represent the identical connection coefficient, discrepant connection coefficient, and contrary connection coefficient of element x belonging to A in X. The form of set pair link function can be expressed as:

$$\varphi_A(x) = a_A(x) + b_A(x)\, i + c_A(x)\, j. \tag{1}$$

In Formula (1), $a_A(x) : x \to [0,1]$, $b_A(x) : x \to [0,1]$, $c_A(x) : x \to [0,1]$, and they satisfy the normalization condition $a_A(x) + b_A(x) + c_A(x) = 1$. $i \in [-1,1]$, j is the contrary degree coefficient, usually be set as $j = -1$, sometimes it is a form of sign without actual meaning. When $b_A(x) = 0$, A degenerates into an intuitionistic fuzzy set; when $c_A(x) = 0$, A degenerates into a fuzzy set; when $b_A(x) = c_A(x) = 0$, A degenerates into a Cantor set. For convenience, denote the set pair number of element α as $\alpha = (a_\alpha, b_\alpha, c_\alpha)$, which satisfies the normalization condition $a_\alpha + b_\alpha + c_\alpha = 1$.

Definition 2. *X is a non-empty set, $A = \{< x, \mu_A(x), \nu_A(x) > | \, x \in X\}$ is the IF set. $\mu_A(x)$ and $\nu_A(x)$ represent the membership degree and non-membership degree of element x belonging to A. $\pi_A(x) = 1 - \mu_A(x) - \nu_A(x)$ is referred to as uncertainty degree.*

Where $\mu_A(x) : x \to [0,1]$, $\nu_A(x) : x \to [0,1]$, and $\mu_A(x) + \nu_A(x) \in [0,1]$. For convenience, set the IF number of element β as $\beta = (\mu_\beta, \nu_\beta)$, there is $\mu_\beta + \nu_\beta \in [0,1]$.

Definition 3. *Given two IF sets A and B, composing the pair $X = (A, B)$, Y is any non-empty set on X, denoted $X = \{< x, \mu_Y(x), \pi_Y(x), \nu_Y(x) > | \, x \in X\}$ as the IF set of Y on X. Where $\mu_Y(x)$, $\pi_Y(x)$, $\nu_Y(x)$ represent the IF identical connection coefficient, IF discrepant connection coefficient, and IF contrary connection coefficient of element x belonging to Y. The IF set pair link function can be expressed as:*

$$\varphi_Y(x) = \mu_Y(x) + \pi_Y(x)\, i + \nu_Y(x)\, j. \tag{2}$$

Definition 4. *For the IF set pair connection number $\varphi_Y(x) = \mu_Y(x) + \pi_Y(x)\, i + \nu_Y(x)\, j$, the IF set pair potential can be denoted as:*

$$shi(\varphi_Y(x)) = \frac{\mu_Y(x)}{\nu_Y(x)} \tag{3}$$

If $\nu_Y(x) = 0$, there will be $shi(\varphi_Y(x)) \to \infty$. when $shi(\varphi_Y(x)) > 1$, it can be denoted as the IF set pair identical potential; when $shi(\varphi_Y(x)) = 1$, it can be denoted as the equilibrium potential; when $shi(\varphi_Y(x)) < 1$, it can

be denoted as the contrary potential. The IF set pair potential reflects the trend of determinate-indeterminate relation in IFSPA. It actually treats the problem through IF set pair identical potential (feasible decision-making solution), IF set pair equilibrium potential (general solution) and IF set pair contrary potential (infeasible solution), which is a simple "clustering" process.

Definition 5. *Denote $A = (\mu_A, \pi_A, \nu_A)$ as the IF set pair number, $E(A)$ and $\sigma(A)$ are the expectation and mean square error of A:*

$$E(A) = \mu_A - \nu_A \quad (4)$$

$$\sigma(A) = \frac{\pi_A}{3} \quad (5)$$

When $\nu_A = 0$, the IF set pair number degenerates into fuzzy number, and $E(A)$ degenerates into the membership degree μ_A. The IF set pair number can be sorted based on the expectation and mean square error. For IF set pair number $\alpha = (\mu_\alpha, \pi_\alpha, \nu_\alpha)$ and $\beta = (\mu_\beta, \pi_\beta, \nu_\beta)$, if $E(\alpha) < E(\beta)$, then $\alpha < \beta$. If $E(\alpha) = E(\beta)$, then when $\sigma(\alpha) = \sigma(\beta)$ there is $\alpha < \beta$; when $\sigma(\alpha) > \sigma(\beta)$, $\alpha < \beta$; when $\sigma(\alpha) < \sigma(\beta)$, there is $\alpha < \beta$.

Definition 6. *For IF set pair number $\alpha = (\mu_\alpha, \pi_\alpha, \nu_\alpha)$, $\alpha_1 = (\mu_1, \pi_1, \nu_1)$ and $\alpha_2 = (\mu_2, \pi_2, \nu_2)$, operation rules for IF set pair number can be defined as follows:*

1) $\overline{\alpha} = (\nu_\alpha, \pi_\alpha, \mu_\alpha)$;

2) $\alpha_1 \cap \alpha_2 = (min(\mu_1, \mu_2), 1 - min(\mu_1, \mu_2) - max(\nu_1, \nu_2), max(\nu_1, \nu_2))$;

3) $\alpha_1 \cup \alpha_2 = (max(\mu_1, \mu_2), 1 - max(\mu_1, \mu_2) - min(\nu_1, \nu_2), min(\nu_1, \nu_2))$;

4) $\alpha_1 \oplus \alpha_2 = (\mu_1 + \mu_2 - \mu_1\mu_2, 1 + \mu_1\mu_2 - \mu_1 - \mu_2 - \nu_1\nu_2, \nu_1\nu_2)$;

5) $\alpha_1 \otimes \alpha_2 = (\mu_1\mu_2, 1 - \mu_1\mu_2 - \nu_1 - \nu_2 + \nu_1\nu_2, \nu_1 + \nu_2 - \nu_1\nu_2)$;

6) $n\alpha = (1 - (\pi_\alpha + \nu_\alpha)^n, (\pi_\alpha + \nu_\alpha)^n - \nu_\alpha^n, \nu_\alpha^n) = (1 - (1 - \mu_\alpha)^n, (1 - \mu_\alpha)^n - \nu_\alpha^n, \nu_\alpha^n)$ *where* $n > 0$;

7) $\alpha^n = (\mu_\alpha^n, (\mu_\alpha + \pi_\alpha)^n - \mu_\alpha^n, 1 - (\mu_\alpha + \pi_\alpha)^n) = (\mu_\alpha^n, (1 - \nu_\alpha)^n - \mu_\alpha^n, 1 - (1 - \nu_\alpha)^n)$ *where* $n > 0$.

In Definition 6, if $\pi = 0$, the IF set pair number degenerates into an IF number, the operating rules still holds [17]. According to Definition 6, the following properties can be obtained.

Property 1: The operation result of IF set pair number is also a IF set pair number.

Take the operation $\oplus$ as an example to prove, others are similar.

Proof. Set $\alpha_1 = (\mu_1, \pi_1, \nu_1)$ and $\alpha_2 = (\mu_2, \pi_2, \nu_2)$ as the IF set pair number, from Definition 1 to Definition 3 we can get: $\mu_1, \pi_1, \nu_1 \in [0, 1]$, $\mu_1 + \pi_1 + \nu_1 = 1$; $\mu_2, \pi_2, \nu_2 \in [0, 1]$, $\mu_2 + \pi_2 + \nu_2 = 1$. Thereby, $\mu_1 + \mu_2 - \mu_1\mu_2 = \mu_1(1 - \mu_2) + \mu_2 \geq 0$; $\mu_1 + \mu_2 - \mu_1\mu_2 = \mu_1 + \mu_2(1 - \mu_1) \leq \mu_1 + 1 - \mu_1 = 1$; So that: $\mu_1 + \mu_2 - \mu_1\mu_2 \in [0, 1]$. And $\nu_1 \in [0, 1]$, $\nu_2 \in [0, 1]$; so that $\nu_1\nu_2 \in [0, 1]$. Because $(\mu_1 + \mu_2 - \mu_1\mu_2) + (1 - \mu_1 - \mu_2 + \mu_1\mu_2) + \nu_1\nu_2 = 1$, so that $\alpha_1 \oplus \alpha_2$ is the IF set pair number. □

Property 2: Set $\alpha = (\mu_\alpha, \pi_\alpha, \nu_\alpha)$, $\alpha_1 = (\mu_1, \pi_1, \nu_1)$, $\alpha_2 = (\mu_2, \pi_2, \nu_2)$ and $\alpha_3 = (\mu_3, \pi_3, \nu_3)$ to be the IF set pair number, and $n_1, n_2, n_3 > 0$, then:

1) $\alpha_1 \oplus \alpha_2 = \alpha_2 \oplus \alpha_1$

Proof. According to Definitions 6, there is:

$$\begin{aligned}\alpha_1 \oplus \alpha_2 &= (\mu_1 + \mu_2 - \mu_1\mu_2, 1 + \mu_1\mu_2 - \mu_1 - \mu_2 - \nu_1\nu_2, \nu_1\nu_2)\\ &= (\mu_2 + \mu_1 - \mu_2\mu_1, 1 + \mu_2\mu_1 - \mu_2 - \mu_1 - \nu_2\nu_1, \nu_2\nu_1)\\ &= \alpha_2 \oplus \alpha_1.\end{aligned}$$

□

2) $\alpha_1 \otimes \alpha_2 = \alpha_2 \otimes \alpha_1$

Proof. According to Definitions 6, there is:

$$\begin{aligned}\alpha_1 \otimes \alpha_2 &= (\mu_1\mu_2, 1 - \mu_1\mu_2 - \nu_1 - \nu_2 + \nu_1\nu_2, \nu_1 + \nu_2 - \nu_1\nu_2)\\ &= (\mu_2\mu_1, 1 - \mu_2\mu_1 - \nu_2 - \nu_1 + \nu_2\nu_1, \nu_2 + \nu_1 - \nu_2\nu_1)\\ &= \alpha_2 \otimes \alpha_1\end{aligned}$$

□

3) $n(\alpha_1 \oplus \alpha_2) = n\alpha_1 \oplus n\alpha_2$

Proof. According to Properties (4) and (6) of Definition 6, there is:

$$\begin{aligned}n(\alpha_1 \oplus \alpha_2) &= (1 - (1 - \mu_1 - \mu_2 + \mu_1\mu_2)^n, (1 - \mu_1 - \mu_2 + \mu_1\mu_2)^n - (\nu_1\nu_2)^n, (\nu_1\nu_2)^n)\\ &= (1 - ((1 - \mu_1)(1 - \mu_2))^n, ((1 - \mu_1)(1 - \mu_2))^n - (\nu_1\nu_2)^n, (\nu_1\nu_2)^n).\end{aligned}$$

Because:

$$\begin{aligned}n\alpha_1 &= (1 - (1 - \mu_1)^n, (1 - \mu_1)^n - \nu_1^n, \nu_1^n),\\ n\alpha_2 &= (1 - (1 - \mu_2)^n, (1 - \mu_2)^n - \nu_2^n, \nu_2^n).\end{aligned}$$

Thus:

$$\begin{aligned}n\alpha_1 \oplus n\alpha_2 &= (1 - (1 - \mu_1)^n(1 - \mu_2)^n, (1 - \mu_1)^n(1 - \mu_2)^n - \nu_1^n\nu_2^n, \nu_1^n\nu_2^n)\\ &= (1 - ((1 - \mu_1)(1 - \mu_2))^n, ((1 - \mu_1)(1 - \mu_2))^n - (\nu_1\nu_2)^n, (\nu_1\nu_2)^n)\end{aligned}$$

So that: $n(\alpha_1 \oplus \alpha_2) = n\alpha_1 \oplus n\alpha_2$. □

4) $\alpha^{n_1} \otimes \alpha^{n_2} = \alpha^{n_1+n_2}$

Proof. According to Properties (5) and (7) of Definition 6, there is:

$$\alpha^{n_1} = (\mu_\alpha^{n_1}, (\mu_\alpha + \pi_\alpha)^{n_1} - \mu_\alpha^{n_1}, 1 - (\mu_\alpha + \pi_\alpha)^{n_1}),$$
$$\alpha^{n_2} = (\mu_\alpha^{n_2}, (\mu_\alpha + \pi_\alpha)^{n_2} - \mu_\alpha^{n_2}, 1 - (\mu_\alpha + \pi_\alpha)^{n_2}),$$

So that:

$$\begin{aligned}
& \alpha^{n_1} \otimes \alpha^{n_2} \\
= \; & (\mu_\alpha^{n_1}\mu_\alpha^{n_2}, 1 - \mu_\alpha^{n_1}\mu_\alpha^{n_2} - (1 - (\mu_\alpha + \pi_\alpha)^{n_1}) \\
& -(1 - (\mu_\alpha + \pi_\alpha)^{n_2}) + (1 - (\mu_\alpha + \pi_\alpha)^{n_1}) \\
& (1 - (\mu_\alpha + \pi_\alpha)^{n_2}), (1 - (\mu_\alpha + \pi_\alpha)^{n_1}) \\
& +(1 - (\mu_\alpha + \pi_\alpha)^{n_2}) \\
& -(1 - (\mu_\alpha + \pi_\alpha)^{n_1}(1 - (\mu_\alpha + \pi_\alpha)^{n_2}) \\
= \; & (\mu_\alpha^{n_1+n_2}, (\mu_\alpha + \pi_\alpha)^{n_1+n_2} - \mu_\alpha^{n_1+n_2}, \\
& 1 - (\mu_\alpha + \pi_\alpha)^{n_1+n_2})
\end{aligned}$$

While $\alpha^{n_1+n_2} = (\mu_\alpha^{n_1+n_2}, (\mu_\alpha + \pi_\alpha)^{n_1+n_2} - \mu_\alpha^{n_1+n_2}, 1-(\mu_\alpha+\pi_\alpha)^{n_1+n_2})$. Therefore: $\alpha^{n_1} \otimes \alpha^{n_2} = \alpha^{n_1+n_2}$. □

5) $(\alpha_1 \oplus \alpha_2) \oplus \alpha_3 = \alpha_1 \oplus (\alpha_2 \oplus \alpha_3)$

Proof. According to Property (4) of Definition 6, there is: $\alpha_1 \oplus \alpha_2 = (\mu_1 + \mu_2 - \mu_1\mu_2, 1 + \mu_1\mu_2 - \mu_1 - \mu_2 - \nu_1\nu_2, \nu_1\nu_2)$, so that:

$$\begin{aligned}
& (\alpha_1 \oplus \alpha_2) \oplus \alpha_3 \\
= \; & (\mu_1 + \mu_2 - \mu_1\mu_2 + \mu_3 - (\mu_1 + \mu_2 - \mu_1\mu_2)\mu_3, \\
& 1 + (\mu_1 + \mu_2 - \mu_1\mu_2)\mu_3 - (\mu_1 + \mu_2 - \mu_1\mu_2) \\
& -\mu_3 - \nu_1\nu_2\nu_3, \nu_1\nu_2\nu_3) \\
= \; & (\mu_1 + \mu_2 + \mu_3 - \mu_1\mu_2 - \mu_1\mu_3 - \mu_2\mu_3 + \mu_1\mu_2\mu_3, \\
& 1 + \mu_1\mu_2 + \mu_1\mu_3 + \mu_2\mu_3 - \mu_1\mu_2\mu_3 - \mu_1 \\
& -\mu_2 - \mu_3 - \nu_1\nu_2\nu_3, \nu_1\nu_2\nu_3).
\end{aligned}$$

Besides:

$$\begin{aligned}
& \alpha_1 \oplus (\alpha_2 \oplus \alpha_3) \\
= \; & (\mu_1 + \mu_2 + \mu_3 - \mu_2\mu_3 - (\mu_2 + \mu_3 - \mu_2\mu_3)\mu_1, \\
& 1 + (\mu_2 + \mu_3 - \mu_2\mu_3)\mu_1 - \mu_1 \\
& -(\mu_2 + \mu_3 - \mu_2\mu_3) - \nu_1\nu_2\nu_3, \nu_1\nu_2\nu_3) \\
= \; & (\mu_1 + \mu_2 + \mu_3 - \mu_1\mu_2 - \mu_1\mu_3 - \mu_2\mu_3 \\
& +\mu_1\mu_2\mu_3, 1 + \mu_1\mu_2 + \mu_1\mu_3 + \mu_2\mu_3 \\
& -\mu_1\mu_2\mu_3 - \mu_1 - \mu_2 - \mu_3 \\
& -\nu_1\nu_2\nu_3, \nu_1\nu_2\nu_3).
\end{aligned}$$

Therefore, $(\alpha_1 \oplus \alpha_2) \oplus \alpha_3 = \alpha_1 \oplus (\alpha_2 \oplus \alpha_3)$. □

6) $(\alpha_1 \otimes \alpha_2) \otimes \alpha_3 = \alpha_1 \otimes (\alpha_2 \otimes \alpha_3)$

Proof. According to Property (5) of Definition 6, there is: $\alpha_1 \otimes \alpha_2 = (\mu_1\mu_2, 1-\mu_1\mu_2-\nu_1-\nu_2+\nu_1\nu_2, \nu_1+\nu_2-\nu_1\nu_2)$. Thus:

$$\begin{aligned}
& (\alpha_1 \otimes \alpha_2) \otimes \alpha_3 \\
= \; & (\mu_1\mu_2\mu_3, 1 - \mu_1\mu_2\mu_3 - (\nu_1 + \nu_2 - \nu_1\nu_2) \\
& -\nu_3 + (\nu_1 + \nu_2 - \nu_1\nu_2)\nu_3, (\nu_1 + \nu_2 - \nu_1\nu_2) \\
& +\nu_3 - (\nu_1 + \nu_2 - \nu_1\nu_2)\nu_3) \\
= \; & (\mu_1\mu_2\mu_3, 1 - \mu_1\mu_2\mu_3 - \nu_1\nu_2\nu_3 \\
& -(\nu_1 + \nu_2 + \nu_3) + (\nu_1\nu_2 + \nu_1\nu_3 + \nu_2\nu_3), \\
& (\nu_1 + \nu_2 + \nu_3) - (\nu_1\nu_2 + \nu_1\nu_3 + \nu_2\nu_3) \\
& +\nu_1\nu_2\nu_3).
\end{aligned}$$

In a similar way:

$$\begin{aligned}
& \alpha_1 \otimes (\alpha_2 \otimes \alpha_3) \\
= \; & (\mu_1\mu_2\mu_3, 1 - \mu_1\mu_2\mu_3 - \nu_1 \\
& -(\nu_2 + \nu_3 - \nu_2\nu_3) + (\nu_2 + \nu_3 - \nu_2\nu_3)\nu_1, \\
& \nu_1 + (\nu_2 + \nu_3 - \nu_2\nu_3) - (\nu_2 + \nu_3 - \nu_2\nu_3)\nu_1) \\
= \; & (\mu_1\mu_2\mu_3, 1 - \mu_1\mu_2\mu_3 - \nu_1\nu_2\nu_3 \\
& -(\nu_1 + \nu_2 + \nu_3) + (\nu_1\nu_2 + \nu_1\nu_3 + \nu_2\nu_3), \\
& (\nu_1 + \nu_2 + \nu_3) - (\nu_1\nu_2 + \nu_1\nu_3 + \nu_2\nu_3) \\
& +\nu_1\nu_2\nu_3).
\end{aligned}$$

Therefore: $(\alpha_1 \otimes \alpha_2) \otimes \alpha_3 = \alpha_1 \otimes (\alpha_2 \otimes \alpha_3)$. □

3 Aggregation Operator of IFSPA

Big data applications often have to face data publishing tasks with the order of magnitude TB, ZB, or even more. In order to gather useful information accurately and eliminate as much confusion as possible, we propose six IF set pair information aggregation operators based on the operation property of IFSPA, which can effectively gather information such as real numbers, fuzzy numbers, and interval numbers.

Definition 7. *$\alpha_i = (\mu_i, \pi_i, \nu_i), (i = 1, 2, \ldots, n)$ is the IF set pair number, the n-dimensional IF set pair analysis weighted average operator (IFSPAWA) is defined as $IFSPAWA_\omega(\alpha_1, \alpha_2, \ldots, \alpha_n) = \sum_{j=1}^{n} \omega_j \alpha_j$, where $w = (w_1, w_2, \ldots, w_n)^T$ is the weight of attribute, $w_j \in [0, 1]$, $\sum_{j=1}^{n} \omega_j = 1$.*

According to the operation property of Definition 6, the IFSPAWA operator can be simplified into:

$$\begin{aligned}
& IFSPAWA_\omega(\alpha_1, \alpha_2, \ldots, \alpha_n) \\
= \; & (1 - \prod_{j=1}^{n}(\pi_j + \nu_j)^{\omega_j}, \prod_{j=1}^{n}(\pi_j + \nu_j)^{\omega_j} - \prod_{j=1}^{n}\nu_j^{\omega_j}, \prod_{j=1}^{n}\nu_j^{\omega_j}).
\end{aligned} \tag{6}$$

Definition 8. *$\alpha_i = (\mu_i, \pi_i, \nu_i), (i = 1, 2, \ldots, n)$ is the IF set pair number, the n-dimensional IF set pair analysis ordered weighted average operator (IFSPAOWA) can be defined as: $IFSPAOWA_\omega(\alpha_1, \alpha_2, \ldots, \alpha_n) = w_1\alpha_{\sigma(1)} \oplus w_2\alpha_{\sigma(2)} \oplus \ldots \oplus w_n\alpha_{\sigma(n)}$, $w = (w_1, w_2, \ldots, w_n)^T$, where $w_j \in [0,1]$, $\sum_{j=1}^{n} \omega_j = 1$. $\sigma(1)$,$\sigma(2)$,...,$\sigma(n)$ is the permutation for $(1, 2, \ldots, n)$. For $\forall j$, there is $\alpha_{\sigma(j-1)} \geq \alpha_{\sigma(j)}$.*

According to the operation property of Definition 6, the IFSPAOWA operator can be simplified into:

$$\begin{aligned} &IFSPAOWA_\omega(\alpha_1, \alpha_2, \ldots, \alpha_n) \\ &= (1 - \prod_{j=1}^{n} (\pi_{\sigma(j)} + \nu_{\sigma(j)})^{\omega_j}, \prod_{j=1}^{n} (\pi_{\sigma(j)} + \nu_{\sigma(j)})^{\omega_j} \\ &\quad - \prod_{j=1}^{n} \nu_{\sigma(j)}^{\omega_j}, \prod_{j=1}^{n} \nu_{\sigma(j)}^{\omega_j}). \end{aligned} \tag{7}$$

Definition 9. *Set $\alpha_i = (\mu_i, \pi_i, \nu_i), (i = 1, 2, \ldots, n)$ as the IF set pair number, the n-dimensional IF set pair analysis weighted geometric operator (IFSPAWG) is defined as $IFSPAWG_\omega(\alpha_1, \alpha_2, \ldots, \alpha_n) = \alpha_1^{\omega_1} \otimes \alpha_2^{\omega_2} \otimes \ldots \otimes \alpha_n^{\omega_n}$, $w = (w_1, w_2, \ldots, w_n)^T$, where $w_j \in [0,1]$, $\sum_{j=1}^{n} \omega_j = 1$.*

According to the operation property of Definition 6, the IFSPAWG operator can be simplified into:

$$\begin{aligned} &IFSPAWG_\omega(\alpha_1, \alpha_2, \ldots, \alpha_n) \\ &= (\prod_{j=1}^{n} \mu_j^{\omega_j}, \prod_{j=1}^{n} (1 - \nu_j)^{\omega_j} - \prod_{j=1}^{n} \mu_j^{\omega_j}, 1 - \prod_{j=1}^{n} (1 - \nu_j)^{\omega_j}). \end{aligned} \tag{8}$$

Definition 10. *Set $\alpha_i = (\mu_i, \pi_i, \nu_i), (i = 1, 2, \ldots, n)$ to be the IF set pair number, the n-dimensional IF set pair analysis ordered weighted geometric operator (IFSPAOWG) is defined as $IFSPAOWG_\omega(\alpha_1, \alpha_2, ..., \alpha_n) = \alpha_{\sigma(1)}^{\omega_1} \otimes \alpha_{\sigma(2)}^{\omega_2} \otimes \ldots \otimes \alpha_{\sigma(n)}^{\omega_n}$, $w = (w_1, w_2, ..., w_n)^T$, where $w_j \in [0,1]$, $\sum_{j=1}^{n} \omega_j = 1$, and $\sigma(1)$,$\sigma(2)$,...,$\sigma(n)$ is the permutation for $(1, 2, ..., n)$. For $\forall j$, there is $\alpha_{\sigma(j-1)} \geq \alpha_{\sigma(j)}$.*

According to the operation property of Definition 6, the IFSPAOWG operator can be simplified into:

$$\begin{aligned} &IFSPAWG_\omega(\alpha_1, \alpha_2, \ldots, \alpha_n) \\ &= (\prod_{j=1}^{n} \mu_{\sigma(j)}^{\omega_j}, \prod_{j=1}^{n} (1 - \nu_{\sigma(j)})^{\omega_j} - \prod_{j=1}^{n} \mu_{\sigma(j)}^{\omega_j}, \\ &\quad 1 - \prod_{j=1}^{n} (1 - \nu_{\sigma(j)})^{\omega_j}). \end{aligned} \tag{9}$$

Definition 11. *$\alpha_i = (\mu_i, \pi_i, \nu_i), (i = 1, 2, \ldots, n)$ is the IF set pair number, the n-dimensional IF set pair analysis hybrid average operator (IFSPAHA) is defined as $IFSPAHA_\omega(\alpha_1, \alpha_2, ..., \alpha_n) = \ddot{\alpha}_{\sigma(1)}^{\omega_1} \oplus \ddot{\alpha}_{\sigma(2)}^{\omega_2} \oplus \ldots \oplus \ddot{\alpha}_{\sigma(n)}^{\omega_n}$, where $w = (w_1, w_2, \ldots, w_n)^T$, $w_j \in [0,1]$, $\sum_{j=1}^{n} \omega_j = 1$. $\ddot{\alpha}_{\sigma(n)}$ is the j^{th} largest element of the IF set pair number, $\ddot{\alpha}_j = n\omega_j\dot{\alpha}_j$, $(j = 1, 2, \ldots, n)$, n is the balance factor, and $\sigma(1)$,$\sigma(2)$,...,$\sigma(n)$ is the permutation for $(1, 2, \ldots, n)$. For $\forall j$, there is $\ddot{\alpha}_{\sigma(j-1)} \geq \ddot{\alpha}_{\sigma(j)}$.*

According to the operation property of Definition 6, the IFSPAHA operator can be simplified into:

$$\begin{aligned} &IFSPAHA_\omega(\alpha_1, \alpha_2, \ldots, \alpha_n) \\ &= (1 - \prod_{j=1}^{n} (1 - \mu_{\ddot{\alpha}_{\sigma(j)}})^{\omega_j}, \\ &\quad \prod_{j=1}^{n} \nu_{\ddot{\alpha}_{\sigma(j)}}^{\omega_j} - \prod_{j=1}^{n} (1 - \mu_{\ddot{\alpha}_{\sigma(j)}})^{\omega_j}, \prod_{j=1}^{n} \nu_{\ddot{\alpha}_{\sigma(j)}}^{\omega_j}). \end{aligned} \tag{10}$$

Definition 12. *Set $\alpha_i = (\mu_i, \pi_i, \nu_i), (i = 1, 2, \ldots, n)$ to be the IF set pair number, the n-dimensional IF set pair analysis hybrid geometric operator (IFSPAHG) is defined as $IFSPAHG_\omega(\alpha_1, \alpha_2, ..., \alpha_n) = \ddot{\alpha}_{\sigma(1)}^{\omega_1} \otimes \ddot{\alpha}_{\sigma(2)}^{\omega_2} \otimes \ldots \otimes \ddot{\alpha}_{\sigma(n)}^{\omega_n}$, where $w = (w_1, w_2, \ldots, w_n)^T$, $w_j \in [0,1]$, $\sum_{j=1}^{n} \omega_j = 1$. $\ddot{\alpha}_j = \dot{\alpha}_j^{n\omega_j}$ $(j = 1, 2, \ldots, n)$. n is the balance factor, and $\sigma(1)$,$\sigma(2)$,...,$\sigma(n)$ is the permutation for $(1, 2, ..., n)$. For $\forall j$, there is $\ddot{\alpha}_{\sigma(j-1)} \geq \ddot{\alpha}_{\sigma(j)}$.*

According to the operation property of Definition 6, the IFSPAHG operator can be simplified into:

$$\begin{aligned} &IFSPAHG_\omega(\alpha_1, \alpha_2, \ldots, \alpha_n) \\ &= (\prod_{j=1}^{n} \mu_{\ddot{\alpha}_{\sigma(j)}}^{\omega_j}, \prod_{j=1}^{n} (1 - \nu_{\ddot{\alpha}_{\sigma(j)}})^{\omega_j} - \prod_{j=1}^{n} \mu_{\ddot{\alpha}_{\sigma(j)}}^{\omega_j}, \\ &\quad 1 - \prod_{j=1}^{n} (1 - \nu_{\ddot{\alpha}_{\sigma(j)}})^{\omega_j}). \end{aligned} \tag{11}$$

According to Definition 6, the result of IF set pair information aggregation is still the IF set pair number, and it is easy to prove that the IFSPAWA, IFSPAOWA, IFSPAWG, IFSPAOWG, IFSPAHA and IFSPAHG operator are all satisfy the following property.

Property 3: Idempotence of the aggregation of IF set pairs.

Set $\alpha_i = (\mu_i, \pi_i, \nu_i), (i = 1, 2, \ldots, n)$ to be the IF set pair number, if $\alpha_i = \alpha$, then there is: $IFSPA(WA, OWA, WG, OWG, HA, HG)_\omega(\alpha_1, ...\alpha_n) = \alpha$.

Proof. Take the IFSPAWA operator as an example to prove Property 3, the other operators are similar. Suppose there is $\alpha_i = (\mu_i, \pi_i, \nu_i)$ and $\alpha_i = \alpha$, according to

Definition 6, there is:

$$\begin{aligned} & IFSPAWA_{\omega}(\alpha_1, \alpha_2, ..., \alpha_n) \\ = & (1-\prod_{j=1}^{n}(\pi_{\alpha_j}+\nu_{\alpha_j})^{\omega_j}, \\ & \prod_{j=1}^{n}\left(\pi_{\alpha_j}+\nu_{\alpha_j}\right)^{\omega_j}-\prod_{j=1}^{n}\nu_{\alpha_j}^{\omega_j}, \prod_{j=1}^{n}\nu_{\alpha_j}^{\omega_j}) \\ = & (1-\prod_{j=1}^{n}\left(\pi_{\alpha_j}+\nu_{\alpha_j}\right)^{\omega_j}, \\ & \prod_{j=1}^{n}\left(\pi_{\alpha_j}+\nu_{\alpha_j}\right)^{\omega_j}-\prod_{j=1}^{n}\nu_{\alpha_j}^{\omega_j}, \prod_{j=1}^{n}\nu_{\alpha_j}^{\omega_j}) \\ = & (\mu_{\alpha}, \pi_{\alpha}, \nu_{\alpha}) = \alpha. \end{aligned}$$

□

Property 4: Monotonicity of the aggregation of IF set pair number.

Suppose $\alpha_i = (\mu_{\alpha i}, \pi_{\alpha i}, \nu_{\alpha i}), (i = 1, 2, \ldots, n)$ and $\beta_i = (\mu_{\beta i}, \pi_{\beta i}, \nu_{\beta i}), (i = 1, 2, \ldots, n)$ to be two sets of the IF set pair number, if $\alpha_i \leq \beta_i$, then there is: $IFSPA\left(WA, OWA, WG, OWG, HA, HG\right)_{\omega}(\alpha_1, ..., \alpha_n)$ $\leq IFSPA\left(WA, OWA, WG, OWG, HA, HG\right)_{\omega}(\beta_1, ..., \beta_n)$.

Proof. Take the IFSPAWA operator as an example to prove Property 4, the other operators are similar. Since $\alpha_i \leq \beta_i$, according to Definition 5, there is: $\mu_{\alpha_i} - \nu_{\alpha_i} \leq \mu_{\beta_i} - \nu_{\beta_i}$, So that $\mu_{\alpha_i} - \mu_{\beta_i} \leq \nu_{\alpha_i} - \nu_{\beta_i}$. There are two situations to discuss:

1) When $0 \leq \mu_{\alpha_i} - \nu_{\alpha_i} \leq \mu_{\beta_i} - \nu_{\beta_i}$, there is $\left(\mu_{\alpha_i} - \mu_{\beta_i}\right)^{\omega_i} \leq \left(\nu_{\alpha_i} - \nu_{\beta_i}\right)^{\omega_i}$, and $\left((1-\mu_{\beta_i}) - (1-\mu_{\alpha_i})\right)^{\omega_i} \leq \left(\nu_{\alpha_i} - \nu_{\beta_i}\right)^{\omega_i}$, so that $\prod_{i=1}^{n}\left(1-\mu_{\beta_i}\right)^{\omega_i} \leq \prod_{i=1}^{n}\left(1-\mu_{\alpha_i}\right)^{\omega_i}, \prod_{i=1}^{n}\nu_{\alpha}^{\omega_i} \geq \prod_{i=1}^{n}\nu_{\beta}^{\omega_i}$. Therefore:

$$\begin{aligned} & E\left(IFSPAWA_{\omega}(\alpha)\right) - E\left(IFSPAWA_{\omega}(\beta)\right) \\ = & \left(1-\prod_{i=1}^{n}\left(\pi_{\alpha}+\nu_{\alpha}\right)^{\omega_i}-\prod_{i=1}^{n}\nu_{\alpha}^{\omega_i}\right) \\ & -\left(1-\prod_{i=1}^{n}\left(\pi_{\beta}+\nu_{\beta}\right)^{\omega_i}-\prod_{i=1}^{n}\nu_{\beta}^{\omega_i}\right) \\ = & \left(\prod_{i=1}^{n}\left(\pi_{\beta}+\nu_{\beta}\right)^{\omega_i}-\prod_{i=1}^{n}\left(\pi_{\alpha}+\nu_{\alpha}\right)^{\omega_i}\right) \\ & -\left(\prod_{i=1}^{n}\nu_{\alpha}^{\omega_i}-\prod_{i=1}^{n}\nu_{\beta}^{\omega_i}\right) \\ = & \prod_{i=1}^{n}\left(1-\mu_{\beta}\right)^{\omega_i}-\prod_{i=1}^{n}\left(1-\mu_{\alpha}\right)^{\omega_i} \\ & -\left(\prod_{i=1}^{n}\nu_{\alpha}^{\omega_i}-\prod_{i=1}^{n}\nu_{\beta}^{\omega_i}\right) \leq 0. \end{aligned}$$

That is $E\left(IFSPAWA_{\omega}(\alpha)\right) \leq E\left(IFSPAWA_{\omega}(\beta)\right)$, thus: $IFSPAWA_{\omega}(\alpha_1, \cdots, \alpha_n) \leq IFSPAWA_{\omega}(\beta_1, \cdots, \beta_n)$.

2) When $\mu_{\alpha_i} - \nu_{\alpha_i} \leq \mu_{\beta_i} - \nu_{\beta_i} \leq 0$, it can be obtained by the same way that $E\left(IFSPAWA_{\omega}(\alpha)\right) - E\left(IFSPAWA_{\omega}(\beta)\right)$, therefore, Property 4 is true.

□

Property 5: Boundedness of the aggregation of the IF set pair number.

Suppose $\alpha_i = (\mu_{\alpha i}, \pi_{\alpha i}, \nu_{\alpha i}), (i = 1, 2, ..., n)$ is the IF set pair number, $\alpha_{max} = max\left(\alpha_i\right)$, $\alpha_{min} = min\left(\alpha_i\right)$, there is: $\alpha_{min} \leq IFSPA\left(WA, OWA, WG, OWG, HA, HG\right)_{\omega} \leq \alpha_{max}$.

Proof. Take the IFSPAWA operator as an example to prove Property 5, the others are similar. For $\forall j$, there is $\min\left\{\pi_{\alpha_j}\right\} \leq \pi_{\alpha_j} \leq \max\left\{\pi_{\alpha_j}\right\}$, $\min\left\{\nu_{\alpha_j}\right\} \leq \nu_{\alpha_j} \leq \max\left\{\nu_{\alpha_j}\right\}$, and $\min\left\{\mu_{\alpha_j}\right\} \leq \mu_{\alpha_j} \leq \max\left\{\mu_{\alpha_j}\right\}$. Therefore:

$$\begin{aligned} & 1-\prod_{j=1}^{n}\left(\pi_{\alpha_j}+\nu_{\alpha_j}\right)^{\omega_j} \\ = & 1-\prod_{j=1}^{n}\left(1-\mu_{\alpha_j}\right)^{\omega_j} \\ & \geq 1-\prod_{j=1}^{n}\left(1-\min\left\{\mu_{\alpha_j}\right\}\right)^{\omega_j} \\ = & 1-\left(1-\min\left\{\mu_{\alpha_j}\right\}\right)^{\sum_{j=1}^{n}\omega_j} \\ = & \min\left\{\mu_{\alpha_j}\right\} \\ \prod_{j}^{n}\nu_{\alpha_j}^{\omega_j} & \geq \prod_{j}^{n}\left(\min\left\{\nu_{\alpha_j}\right\}\right)^{\omega_j} \\ = & \min\left\{\nu_{\alpha_j}\right\}^{\sum_{j=1}^{n}\omega_j} \\ = & \min\left\{\nu_{\alpha_j}\right\}. \end{aligned}$$

Combined with Definition 5, there is: $\alpha_{min} \leq IFSPAWA_{\omega}(\alpha_1, \alpha_2, \cdots, \alpha_n)$. Similarly:

$$\begin{aligned} & 1-\prod_{j=1}^{n}\left(\pi_{\alpha_j}+\nu_{\alpha_j}\right)^{\omega_j} \\ = & 1-\prod_{j=1}^{n}\left(1-\mu_{\alpha_j}\right)^{\omega_j} \leq 1-\prod_{j=1}^{n}\left(1-\max\left\{\mu_{\alpha_j}\right\}\right)^{\omega_j} \\ = & 1-\left(1-\max\{\mu_{\alpha_j}\}\right)^{\sum_{j=1}^{n}\omega_j} = \max\{\mu_{\alpha_j}\}. \end{aligned}$$

Combined with Definition 5, there is: $IFSPAWA_{\omega}(\alpha_1, \alpha_2, \cdots, \alpha_n) \leq \alpha_{max}$. Therefore: $\alpha_{min} \leq IFSPAWA_{\omega} \leq \alpha_{max}$. □

Table 1: Index system for privacy risk assessment

Primary targets	Secondary targets	Tertiary targets
Privacy risk asset B_1	Confidentiality C_1	Data encryption T_{11}
		Data isolation T_{12}
		Key management T_{13}
		Data privacy T_{14}
	Completeness C_2	Data backup T_{21}
		Data destruction delete T_{22}
		Software upgrade T_{23}
	Availability C_3	Data migration T_{31}
		Risk identification T_{32}
Privacy risk threat B_2	Technical risk C_4	Malicious attack T_{41}
		Network monitoring T_{42}
		Vulnerability processing T_{43}
	Personal risk C_5	Internal staff T_{51}
		Authentication T_{52}
		Operation error T_{53}
Privacy risk vulnerability B_3	Organizational vulnerability C_6	Review supports T_{61}
		Legal compliance T_{62}
		Responsibility and interests T_{63}
	Technical vulnerability C_7	Service lock T_{71}
		Access control T_{72}
Other C_8		Rules and regulations T_{81}
		Privacy processing T_{82}
		Risk reporting T_{83}

4 IFSPA-based Multi-attribute Privacy Risk Decision-Making Approach

4.1 Index System for Privacy Risk Assessment

The aim of privacy risk assessment is to estimate and measure the privacy risks of system comprehensively and systematically. The factors that lead to privacy risks are all-encompassing, involving human-based and objective factors, technical and equipment factors, intrinsic and extrinsic factors, system vulnerabilities and confidential disclosure, incomplete system and deliberately attacks. In a word, privacy risk is the possibility and negative influence of data leakage in privacy information. Privacy risk assessment is useful to identify the possibility of security risks and the negative influence. Combined with the information technology security evaluation criteria (ITSEC [7]) and a large number of research about risk assessment of privacy risk at home and abroad, we establish the index system for privacy risk assessment (shown in Table 1).

4.2 Steps of Multi-attribute Privacy Risk Decision-Making

In the process of privacy risk assessment, qualitative or quantitative assessments are usually given by experts or evaluation systems. The quantitative methods are well established and relatively mature. The qualitative forms of decision-making methods are relatively complex due to possible interference and adverse effects caused by uncertainty, ambiguity, randomness and other error factors during the assessment process. It usually takes the form of fuzzy numbers (such as IF, vague sets, trigonometric fuzzy numbers, *etc.*) or semantics (such as fuzzy semantics). The paper defines the MADM problem in privacy risk assessment, which is qualitatively described by IF set pair. The following takes the IFSPAWA operator as an example to illustrate the steps of decision-making, other operators are in the similar way.

Step 1: Convert privacy risk assessment index into the IF set pair number. Get the semantics such as support, hesitation and negation in evaluation opinion, and establish the IF set pair number in the privacy risk assessment index. In this paper, the semantic conversion relations of 9 scales are adopted (shown in Table 2).

Step 2: The evaluation index of privacy risk may consist of multiple sub-indexes, so the IFSPAWA operator is used to aggregate the sub-indexes in decision matrix

Table 2: Correspondence between 9 scales semantics and various fuzzy numbers

Fuzzy Semantic	Interval Region	0-1 Scale	Vague	IFSPA number	E(A)	$\sigma(A)$	Shi
Extremely High	[1,1]	1	[1,1]	(1,0,0)	1	0	∞
Very high	[0.8,0.9]	0.9	[0.9,0.95]	(0.9,0.05,0.05)	0.85	0.0167	18
Higher	[0.7,0.8]	0.8	[0.8,0.9]	(0.8,0.1,0.1)	0.7	0.0333	8
High	[0.4,0.6]	0.7	[0.7,0.85]	(0.7,0.15,0.15)	0.55	0.05	4.667
Medium	[0,0]	0.5	[0.5,0.5]	(0.5,0,0.5)	0	0	1
Low	[-0.4,-0.1]	0.3	[0.3,0.45]	(0.3,0.15,0.55)	-0.25	0.05	0.5455
Lower	[-0.6,-0.4]	0.2	[0.2,0.3]	(02,0.1,07)	-0.5	0.0333	0.2857
Very low	[-0.8,-0.7]	0.1	[0.1,0.15]	(0.1,0.05,0.85)	-0.75	0.0167	0.1176
Extremely low	[-1,-1]	0	[0,0]	(0,0,1)	-1	0	0

to get the IF set pair decision matrix $\widetilde{D} = [d_{ij}]_{n\times m}$, where:

$$\begin{aligned} d_{ij} &= IFSPAWA\left(d_{ij}^1, d_{ij}^2, \ldots, d_{ij}^k,\right) \\ &= (1-\prod_{p=1}^{k}(\pi^{p_j}+\nu^{p_j})^{\omega_i}, \\ &\quad \prod_{p=1}^{k}(\pi^{p_j}+\nu^{p_j})^{\omega_i} - \prod_{p=1}^{k}\nu^{p_j\omega_j}, \prod_{p=1}^{k}\nu^{p_j\omega_j}). \end{aligned} \tag{12}$$

Step 3: Determine the weight of IF set pair. IF set pair can be established between the weight values and interval [0, 1]. The value of weight is calculated by the relative weight p_i and uncertain relative weight.

$$w_i^* = \frac{\sum_{k=1}^{m} p_{ik}q_{ik}}{\sum_{i=1}^{n}\sum_{k=1}^{m} p_{ik}q_{ik}} \tag{13}$$

Where

$$\begin{aligned} p_i &= \frac{1+\mu_i-\nu_i}{\sum_{i=1}^{n}(1+\mu_i-\nu_i)} = \frac{1+E(A_i)}{\sum_{i=1}^{n}(1+E(A_i))}, \\ q_i &= \frac{\mu_i+\nu_i}{\sum_{i=1}^{n}(\mu_i+\nu_i)} \end{aligned}$$

Step 4: Use the IFSPAWA operator to further aggregate the decision matrix of privacy risk index $\widetilde{D} = [d_{ij}]_{n\times m}$, so as to obtain the integrated number of IF set pairs. Where:

$$\begin{aligned} d_{ij} &= IFSPAWA(d_{i1}, d_{i2}, ..., d_{im}) \\ &= (1-\prod_{j=1}^{m}(\pi_j+\nu_j)^{\omega^{*j}}, \\ &\quad \prod_{j=1}^{m}(\pi_j+\nu_j)^{\omega^{*j}} - \prod_{j=1}^{m}\nu_j^{\omega^{*j}}, \prod_{j=1}^{m}\nu_j^{\omega^{*j}}) \\ &= (1-\prod_{j=1}^{m}\mu_j^{\omega^{*j}}, \prod_{j=1}^{m}\mu_j^{\omega^{*j}} - \prod_{j=1}^{m}\nu_j^{\omega^{*j}}, \prod_{j=1}^{m}\nu_j^{\omega^{*j}}). \end{aligned} \tag{14}$$

Step 5: Calculate the expectation and mean square error of IF set pairs, and sort it according to Definition 5 to get the final decision result.

5 Analysis of Examples

According to the privacy risk assessment index constructed in Table 1, five experts gave the assessment opinion on privacy risk assets, privacy risk threats and privacy risk vulnerabilities (as shown in Table 3), and the privacy risk assessment analysis is conducted accordingly.

Step 1: According to Table 2, the fuzzy semantics of each indicator is processed by the IF set pair number, and the privacy risk index decision matrix is obtained as shown in Table 4.

Step 2: The IFSPAWA operator is used to aggregate the subterm indexes in order to obtain the integrated decision matrix, as shown in Table 5.

Step 3: Calculate the weight of each risk indicator according to Formula (2), and get the result $w_i^* = (0.1257, 0.1217, 0.1246, 0.1106, 0.1272, 0.1262, 0.1276, 0.1364)$.

Step 4: Use the IFSPAWA operator to reaggregate the decision matrix of privacy risk index in Table 5, so as to calculate the integrated number of intuitionistic fuzzy set pairs:

$$\begin{aligned} IFSPAWA(C_1) &= (0.4432, 0.1250, 0.4318), \\ IFSPAWA(C_2) &= (0.4562, 0.1210, 0.4228), \\ IFSPAWA(C_3) &= (0.4059, 0.1264, 0.4677), \\ IFSPAWA(C_4) &= (0.4637, 0.1156, 0.4207), \\ IFSPAWA(C_5) &= (0.4302, 0.1455, 0.4243), \\ IFSPAWA(C_6) &= (0.4572, 0.1321, 0.4107), \\ IFSPAWA(C_7) &= (0.4034, 0.1432, 0.4534), \\ IFSPAWA(C_8) &= (0.4312, 0.1338, 0.4350). \end{aligned}$$

Step 5: Get the expectation, mean square error, and potential value of the integrated IF set pair number (as shown in Table 6).

Table 3: Privacy risk assessment scoring table

Index	Factors/weights	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5
C_1	T_{11} 0.3	High	Medium	High	Higher	High
	T_{12} 0.2	Low	Lower	Higher	Higher	Lower
	T_{13} 0.2	High	Higher	High	High	High
	T_{14} 0.3	Lower	High	High	Low	Low
C_2	T_{21} 0.4	High	Higher	Lower	High	Low
	T_{22} 0.5	Low	Medium	High	Higher	High
	T_{23} 0.1	High	High	Low	Low	Low
C_3	T_{31} 0.4	High	Low	High	Medium	High
	T_{32} 0.6	Higher	High	Lower	Lower	Low
C_4	T_{41} 0.3	Very High	High	High	High	High
	T_{42} 0.3	High	Low	Very low	Medium	Very low
	T_{43} 0.4	Low	High	Higher	Higher	High
C_5	T_{51} 0.5	Low	Low	High	High	High
	T_{52} 0.3	Very low	Low	Higher	High	Higher
	T_{53} 0.2	High	Low	Low	Low	High
C_6	T_{61} 0.4	High	Higher	Low	Low	Low
	T_{62} 0.4	Low	Low	High	Higher	High
	T_{63} 0.2	Higher	High	High	High	Medium
C_7	T_{71} 0.5	High	Higher	Low	High	Low
	T_{72} 0.5	High	High	Lower	Lower	Low
C_8	T_{81} 0.3	Low	Lower	High	High	High
	T_{82} 0.4	High	High	Lower	Low	Lower
	T_{83} 0.3	High	High	Low	Low	High

Table 4: Decision matrix of privacy risk index

Index	Factors/Weights	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5
C_1	T_{11} 0.3	(0.7,0.15,0.15)	(0.5,0,0.5)	(0.7,0.15,0.15)	(0.8,0.1,0.1)	(0.7,0.15,0.15)
	T_{12} 0.2	(0.3,0.15,0.55)	(0.2,0.1,0.7)	(0.8,0.1,0.1)	(0.8,0.1,0.1)	(0.2,0.1,0.7)
	T_{13} 0.2	(0.7,0.15,0.15)	(0.8,0.1,0.1)	(0.7,0.15,0.15)	(0.7,0.15,0.15)	(0.7,0.15,0.15)
	T_{14} 0.3	(0.2,0.1,0.7)	(0.7,0.15,0.15)	(0.7,0.15,0.15)	(0.3,0.15,0.55)	(0.3,0.15,0.55)
C_2	T_{21} 0.4	(0.7,0.15,0.15)	(0.8,0.1,0.1)	(0.2,0.1,0.7)	(0.7,0.15,0.15)	(0.3,0.15,0.55)
	T_{22} 0.5	(0.3,0.15,0.55)	(0.5,0,0.5)	(0.7,0.15,0.15)	(0.8,0.1,0.1)	(0.7,0.15,0.15)
	T_{23} 0.1	(0.7,0.15,0.15)	(0.7,0.15,0.15)	(0.3,0.15,0.55)	(0.3,0.15,0.55)	(0.3,0.15,0.55)
C_3	T_{31} 0.4	(0.7,0.15,0.15)	(0.3,0.15,0.55)	(0.7,0.15,0.15)	(0.5,0,0.5)	(0.7,0.15,0.15)
	T_{32} 0.6	(0.8,0.1,0.1)	(0.7,0.15,0.15)	(0.2,0.1,0.7)	(02,0.1,0.7)	(0.3,0.15,0.55)
C_4	T_{41} 0.3	(0.9,0.05,0.05)	(0.7,0.15,0.15)	(0.7,0.15,0.15)	(0.7,0.15,0.15)	(0.7,0.15,0.15)
	T_{42} 0.3	(0.7,0.15,0.15)	(0.3,0.15,0.55)	(0.1,0.05,0.85)	(0.5,0,0.5)	(0.1,0.05,0.85)
	T_{43} 0.4	(0.3,0.15,0.55)	(0.7,0.15,0.15)	(0.8,0.1,0.1)	(0.8,0.1,0.1)	(0.7,0.15,0.15)
C_5	T_{51} 0.5	(0.3,0.15,0.55)	(0.3,0.15,0.55)	(0.7,0.15,0.15)	(0.7,0.15,0.15)	(0.7,0.15,0.15)
	T_{52} 0.3	(0.1,0.05,0.85)	(0.3,0.15,0.55)	(0.8,0.1,0.1)	(0.7,0.15,0.15)	(0.8,0.1,0.1)
	T_{53} 0.2	(0.7,0.15,0.15)	(0.3,0.15,0.55)	(0.3,0.15,0.55)	(0.3,0.15,0.55)	(0.7,0.15,0.15)
C_6	T_{61} 0.4	(0.7,0.15,0.15)	(0.8,0.1,0.1)	(0.3,0.15,0.55)	(0.3,0.15,0.55)	(0.3,0.15,0.55)
	T_{62} 0.4	(0.3,0.15,0.55)	(0.3,0.15,0.55)	(0.7,0.15,0.15)	(0.8,0.1,0.1)	(0.7,0.15,0.15)
	T_{63} 0.2	(0.8,0.1,0.1)	(0.7,0.15,0.15)	(0.7,0.15,0.15)	(0.7,0.15,0.15)	(0.5,0,0.5)
C_7	T_{71} 0.5	(0.7,0.15,0.15)	(0.8,0.1,0.1)	(0.3,0.15,0.55)	(0.7,0.15,0.15)	(0.3,0.15,0.55)
	T_{72} 0.5	(0.7,0.15,0.15)	(0.7,0.15,0.15)	(0.2,0.1,0.7)	(0.2,0.1,0.7)	(0.3,0.15,0.55)
C_8	T_{81} 0.3	(0.3,0.15,0.55)	(0.2,0.1,07)	(0.7,0.15,0.15)	(0.7,0.15,0.15)	(0.7,0.15,0.15)
	T_{82} 0.4	(0.7,0.15,0.15)	(0.7,0.15,0.15)	(0.2,0.1,0.7)	(0.3,0.15,0.55)	(0.2,0.1,0.7)
	T_{83} 0.3	(0.7,0.15,0.15)	(0.7,0.15,0.15)	(0.3,0.15,0.55)	(0.3,0.15,0.55)	(0.7,0.15,0.15)

Table 5: Decision matrix of privacy risk index after subterm aggregation (IFSPAWA operator)

Index	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5
C_1	(0.135,0.556,0.309)	(0.087,0.643,0.270)	(0.140,0.722,0.138)	(0.125,0.514,0.361)	(0.140,0.558,0.301)
C_2	(0.150,0.553,0.287)	(0.057,0.710,0.233)	(0.130,0.553,0.316)	(0.125,0.735,0.140)	(0.150,0.563,0.287)
C_3	(0.120,0.762,0.118)	(0.150,0.598,0.252)	(0.120,0.502,0.378)	(0.061,0.327,0.612)	(0.150,0.523,0.327)
C_4	(0.121,0.697,0.181)	(0.150,0.629,0.222)	(0.101,0.685,0.215)	(0.087,0.730,0.183)	(0.121,0.626,0.252)
C_5	(0.121,0.396,0.483)	(0.150,0.300,0.550)	(0.135,0.693,0.172)	(0.150,0.656,0.195)	(0.135,0.732,0.133)
C_6	(0.140,0.627,0.233)	(0.130,0.655,0.215)	(0.150,0.598,0.252)	(0.130,0.655,0.215)	(0.122,0.557,0.321)
C_7	(0.150,0.700,0.150)	(0.125,0.752,0.123)	(0.125,0.254,0.621)	(0.125,0.551,0.324)	(0.150,0.300,0.550)
C_8	(0.150,0.629,0.222)	(0.135,0.627,0.238)	(0.130,0.460,0.410)	(0.150,0.478,0.373)	(0.130,0.592,0.278)

Table 6: Results of the integrated aggregation

Index	E(A)	$\sigma(A)$	Shi	Species of Potential	Situation of Risk Control
C_1	0.0114	0.0147	1.0264	Identical potential	controllable
C_2	0.0334	0.0403	1.079	Identical potential	controllable
C_3	-0.0618	0.0421	0.8679	Contrary potential	uncontrollable
C_4	0.043	0.0385	1.1022	Identical potential	controllable
C_5	0.0059	0.0485	1.0139	Identical potential	controllable
C_6	0.0465	0.044	1.1132	Identical potential	controllable
C_7	-0.05	0.0477	0.8897	Contrary potential	uncontrollable
C_8	-0.0038	0.0446	0.9913	Contrary potential	uncontrollable

Combined with Table 6 and Definition 5, privacy risk indicators and their situation of risk control can be ranked from high to low: $C_6 > C_4 > C_2 > C_1 > C_5 > C_8 > C_7 > C_3$. Further analysis shows that the privacy risk index is clustered according to the expectation value, potential value and classification of the IF set pair number. Expectation value of the privacy risk index C_6, C_4, C_2, C_1, C_5 is larger than 0, the potential value belongs to identical potential, and its privacy risk is within the controllable range. Temporarily, no measures need to be taken from the perspective of privacy protection. While the expectation value of privacy risk index C_3, C_7, C_8 is less than 0, the potential value belongs to contrary potential, and the privacy risk falls outside the controllable range. So that some measures need to be taken to protect the privacy. Besides, the privacy risk index C_3, C_7, C_8 is in the same level range, priority of protection covers the corresponding content of privacy risk index C_3 according to the size of expectation value.

6 Conclusions

Privacy risk assessment is an uncertain problem which is affected by many factors. The IF set pair aggregation method proposed in this paper has good application prospect in the field of multi-attribute privacy risk decision-making. Compared with the traditional SPA, IF, Vague sets, Fuzzy and other methods, IF set pair aggregation can solve the problems of randomness, uncertainty and ambiguity in the real society more intuitively, and can effectively describe the support (affirm), hesitate (uncertain), oppose (negate) and other information in decision-making voting without missing. It can obtain more objective and accurate decision-making results than other methods. IFSPA is the organic combination and expansion of IF and SPA. The IFSPAWA, IFSPAWG, IFSPAOWA, IFSPAOWG, IFSPAHA and IFSPAHG operators defined on this basis can improve the aggregation effect of IF set pair analysis. The method further enriches and develops MADM theory and method, showing good application value and practicability, and can be further extended to other related application fields.

Acknowledgments

This study was supported by the Nature Science Foundation of China (61762059), the Nature Science Foundation of Gansu Province (18JR3RA156), and the Science and Technology Project of Lanzhou (2017-4-105). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] K. T. Atanassov, "Intuitionistic fuzzy sets," *Fuzzy Sets and Systems*, vol. 20, no. 1, pp. 87-96, 1986.

[2] B. Fang, Y. Jia, A. Li, "Privacy preservation in big data: A survey (in Chinese)," *Big Data Research*, no. 1, pp. 1-18, 2016.

[3] Y. Fu, X. Wu, Q. Ye, *et al.*, "An approach for information systems security risk assessment on fuzzy set

and entropy-weight (in Chinese)," *Acta Electronica Sinica*, vol. 38, no. 7, pp. 1489-1494, 2010.

[4] H. Garg, "Generalized intuitionistic fuzzy entropy-based approach for solving multi-attribute decision-making problems with unknown attribute weights," in *Proceedings of the National Academy of Sciences, India Section A: Physical Sciences*, vol. 89, no. 1, pp. 129-139, 2019.

[5] H. Garg, R. Arora, "A nonlinear-programming methodology for multi-attribute decision-making problem with interval-valued intuitionistic fuzzy soft sets information," *Appl Intell*, vol. 48, pp. 2031-2046, 2018.

[6] W. L. Gau, D. J. Buehrer, "Vague sets," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 23, no. 2, pp. 610-614, 1993.

[7] ITSEC, "Information technology security evaluation criteria, version1.2," *Office for Official Publications of the European Communities*, June 1991. (`https://www.ssi.gouv.fr/uploads/2015/01/ITSEC-uk.pdf`)

[8] Z. Liu, P. Liu, "Intuitionistic normal fuzzy prioritized aggregation operators and their application to group decision making (in Chinese)," *Systems Engineering-Theory & Practice*, vol. 36, no. 2, pp. 494-504, 2016.

[9] P. Liu, J. Liu, S. Chen, "Some intuitionistic fuzzy Dombi Bonferroni mean operators and their application to multi-attribute group decision making," *Journal of the Operational Research Society*, vol. 69, no. 1, pp. 1-24, 2018.

[10] P. Liu, J. Liu, J. M. Merig, "Partitioned Heronian means based on linguistic intuitionistic fuzzy numbers for dealing with multi-attribute group decision making," *Applied Soft Computing*, vol. 62, pp. 395-422, 2018.

[11] Y. Liu, T. Zhang, X. Jin, *et al.*, "Personal privacy protection in the era of big data (in Chinese)," *Journal of Computer Research and Development*, vol. 52, no. 1, pp. 229-247, 2015.

[12] X. Liu, K. Zhao, "Triangular fuzzy number multi-atteibute decision making with the attribute weight unknown based on connection number," *Fuzzy Systems and Mathematics*, vol. 31, no. 2, pp. 95-106, 2017.

[13] L. R. Sebastian, S. Babu, J. J. Kizhakkethottam, "Challenges with big data mining: A review," in *International Conference on Soft-Computing and Networks Security*, pp. 1-4, 2015.

[14] Z. Shi, H. Wang, X. Wang, "Risk state evaluation of aviation maintenance based on multiple connection number set pair analysis (in Chinese)," *Systems Engineering and Electronics*, vol. 38, no. 3, pp. 588-594, 2016.

[15] Y. Yan, X. Hao, W. Wang, "FSSPCM: fuzzy publication of data for privacy preserving," *International Journal of Security and Its Applications*, vol. 10,no. 11, pp. 229-248, 2016.

[16] J. Yuan, X. Luo, "A threat assessment method of group targets based on interval-valued intuitionistic fuzzy multi-attribute group decision-making," *Computers & Industrial Engineering*, vol. 135, pp. 643-654, 2019.

[17] Z. Xu, "Uncertain multi-attribute decision making: Methods and applications," *Springer-Verlag Berlin Heidelberg*, 2015. DOI: 10.1007/978-3-662-45640-8.

[18] L. A. Zadeh, "Fuzzy sets," *Information and Control*, vol. 8, no. 3, pp. 338-353, 1965.

[19] K. Zhao, "Set pair analysis and its preliminary application (in Chinese)," *Exploration of Nature*, vol. 1, 1994.

[20] L. Zhang, J. Zhan, Z. Xu, "Covering-based generalized IF rough sets with applications to multi-attribute decision-making," *Information Sciences*, vol. 478, pp. 275-302, 2019.

Biography

Yan Yan received the Ph.D. degree in control theory and control engineering from Lanzhou University of Technology, China, in 2018. Her research interests include information security, privacy preserving technology, and differential privacy. She is currently an Associate Professor at School of Computer and Communication, Lanzhou University of Technology, China. She is a member of China Computer Federation.

Bingqian Wang is currently a master student of the School of Computer and Communication, Lanzhou University of Technology, China. She received the B.Eng. degree from Lanzhou University of Technology in 2018. Her research interests include privacy preservation and dynamic modeling of big data publishing system.

Lianxiu Zhang is currently a master student of the School of Computer and Communication, Lanzhou University of Technology, China. She received the B.Eng. degree from the University of Tarim in 2017. Her research interests include network and information security and privacy preservation technology.

Xin Gao is currently a master student of School of Computer and Communication, Lanzhou University of Technology, China. She received the B.Eng. degree from Harbin Normal University in 2013. Her research interests include information security and dynamic clustering.

Design and Implementation of Random Number Generator System Based on Android Smartphone Sensor

Yusuf Kurniawan and Mochamad Beta Auditama

(Corresponding author: Yusuf Kurniawan)

School of Electrical Engineering and Informatics, Institut Teknologi Bandung
Jl. Ganesha No.10, Lb. Siliwangi, Kecamatan Coblong, Kota Bandung, Jawa Barat 40132, Indonesia
(Email: yusufk@stei.itb.ac.id)

(Received May 21, 2019; revised and accepted May 2, 2020)

Abstract

An android smartphone has various types of sensors in its device. All of these sensors produce data based on environmental condition that exists around the device. These data have the potential to be used as the random number because of its non-deterministic component. To realize it, some steps need to be carried out, such as knowing the characteristic of the sensor, estimating the entropy value possessed by the sensor data, and so on. As a proof-of-concept, this research is conducted to design and implement the entropy source and pseudorandom number generator based on the android sensor. The research result shows that by using accelerometer data with XOR result as the input of entropy source and HMAC DRBG as the pseudorandom number generator, so the high quality of random number based on the android sensor can be obtained.

Keywords: Android Sensor; Entropy Source; Pseudorandom Number Generator

1 Introduction

In November 2017, there were already 2.3 billion active smartphone devices based on the Android operating system in the world. The android smartphone provides various features for its users, such as mobile banking. These features use a lot of smartphone resources, especially the random numbers.

Actually, the android operating system has already a random number generation system based on the interrupt process, I/O disk operations, and the user input [14]. This random number generation system is considered safe, but the android smartphone also has a potential resource to be used as a randomness source, which is the sensor. This paper is organized as follows :

1) Related Work;
2) Entropy Source Based on Android Sensor;
3) Pseudorandom Number Generator (PRNG);
4) Conclusion.

2 Related Work

2.1 Android Sensor

The android smartphone divides its sensor into two types, namely the base sensor and composite sensor. The base sensor is a single physical sensor that measures certain phenomena that exist in the sensor environment, whereas composite sensor is a combination of one or more single physical sensor with a specific algorithm to measure a phenomenon which is not covered by the base sensor. In this research, the composite sensor is not selected as randomness source, because only base sensor that actually produces non-deterministic data.

Table 1 shows a list of the base sensor and their reporting mode. The base sensor with a ”continuous” reporting mode will produce data continuously as long as the sensor operates, whereas the base sensor with the ”on-change” reporting mode will only produce data when a phenomenon in the environment changes significantly. To get as many random numbers as possible, the base sensor with a” continuous” reporting mode is selected as a randomness source.

Table 1: A list of base sensor in Android

Sensor name	Reporting mode
Temperature	On-change
Heart rate	On-change
Light	On-change
Proximity	On-change
Relative humidity	On-change
Pressure	Continuous
Magnetometer	Continuous
Accelerometer	Continuous
Gyroscope	Continuous

Because the pressure sensor is rarely owned by the majority of the Android smartphone and the measurement result of the

magnetometer is unstable, especially when the magnetometer is placed close to the iron material, only accelerometer and gyroscope are selected as the randomness source for now.

2.2 Micro-electromechanical Systems (MEMS)

MEMS is a modern technology to manufacture accelerometer and gyroscope on the Android smartphone. With MEMS technology, accelerometer and gyroscope can be produced as a microscale integrated device by creating and combining mechanical and electrical components [5].

In the real-world, the MEMS accelerometer and gyroscope have two dominant types of non-deterministic noise which are bias instability (BI) and Angle/ Velocity Random Walk (ARW/VRW) [4]. If the sensor is operated when not moving (motionless) and two or more set data with size and sample is created, the average value for a set data is different from each other. This difference in value is called BI error. ARW/ VRW error is caused by the Brownian motion of air particles trapped inside the MEMS device [11]. These two non-deterministic errors are the majority factors that cause MEMS accelerometer output and gyroscope to always fluctuate randomly and subsequently have the potential to generate random numbers. The magnitude of BI and ARW/VRW error owned by the MEMS accelerometer and gyroscope can be estimated using the Allan Variance (AVAR) method [10].

Table 2 shows the BI and ARW/VRW coefficient values for MEMS accelerometer and gyroscope from different types of Android smartphones, namely B and Q. For example, if the gyroscope on Andromax R is operated for an hour (3.600 seconds), the ARW error in which the coefficient value is B = 0.0012 rad.s1/2 causes the measurement result to deviate approximately 0.0012 x (3600)1/2 = 0.072 rad.

Table 2: The value of B and Q for the MEMS accelerometer and gyroscope from five different types of Android smartphones

Smartphone	Accelerometer		Gyroscope	
	B[m/s^2]	Q[(m/s).s$^{1/2}$]	B[rad/s]	B[rad/s$^{1/2}$]
A	0.0046	0.0028	2.87x10^{-5}	0.0012
B	7.34x10^{-4}	0.0022	4.83x10^{-5}	3.66x10^{-4}
C	3.69x10^{-4}	6.08x10^{-4}	No gyroscope	
D	6.39x10^{-4}	0.0014	1.26x10^{-4}	3.10x10^{-4}
E	2.61x10^{-4}	8.39x10^{-4}	3.41x10^{-5}	9.02x10^{-5}

*Note: Smartphone A, B, C, D, E consecutively are Andromax R, Asus Zenfone 2, Galaxy Fame, Galaxy Note 10,1, & Galaxy S III Mini.

2.3 Random Number Generator

There are two kinds of systems that can be used to generate the random number, namely True Random Number Generator (TRNG) and Pseudorandom Number Generator (PRNG) [13]. TRNG, or it can also be referred to as an entropy source, produces a random number with the highest quality because this output is formed from purely non-deterministic input. However, the output size of TRNG is so little, specifically, the maximum output size is equal or less than the number of the input data. This problem can be overcome by using PRNG which only involves two components, namely a seed (non-determinism data with limited size) and a deterministic algorithm. A deterministic algorithm is designed to be able to produce a long-size of high-quality random numbers from short-size seed. The existing cryptographic algorithm, such as hash function and symmetric encryption block, can be used as a PRNG deterministic algorithm.

2.4 Entropy

Entropy represents the level of difficulty at guessing the next output produced by the system [6]. For example, there are machine 1 and machine 2 where each machine producing four letters A, B, C, D randomly with the following probability of occurrence:

$$\begin{aligned} &Machine1: \\ &\quad P(A) = 0,25; P(B) = 0,25; \\ &\quad P(C) = 0,25; P(D) = 0,25. \end{aligned}$$

$$\begin{aligned} &Machine2: \\ &\quad P(A) = 0,50; P(B) = 0,25; \\ &\quad P(C) = 0,125; P(D) = 0,125. \end{aligned}$$

Thus, the entropy value for machine 1 is greater than the entropy value for machine 2, because machine 2 will produce letters A and B more often than letters C and D. This is different from machine 1 which producing its four letters with (almost) equal quantity. Below is given the equation to calculate the entropy value of a system that has n sample space:

Entropy = [p1 x log2(p1) + p2 x log2(p2) + ... + pn-1 x log2(pn-1) + pn x log2(pn)...],

with pi = the occurrence probability for the ith unique element ($1 \leq i \leq$ n).

3 Entropy Source Based on Android Sensor

The entropy source used in this research is in conformance with the NIST SP 800-90B recommendation. See Figure 1 and [9]. There are five components involved in this entropy source, namely randomness source, digitization, entropy estimation (for each sensor sample), health test, and conditioning.

3.1 Randomness Source

The randomness source is implemented by the accelerometer or gyroscope. Several specifications shall be satisfied with collecting sensor samples as follows:

1) Sensor samples are collected from five different types of Android smartphones: Andromax R, Asus Zenfone 2, Samsung Galaxy Fame (no gyroscope), Samsung Galaxy Note 10.1, and Samsung Galaxy S III Mini.

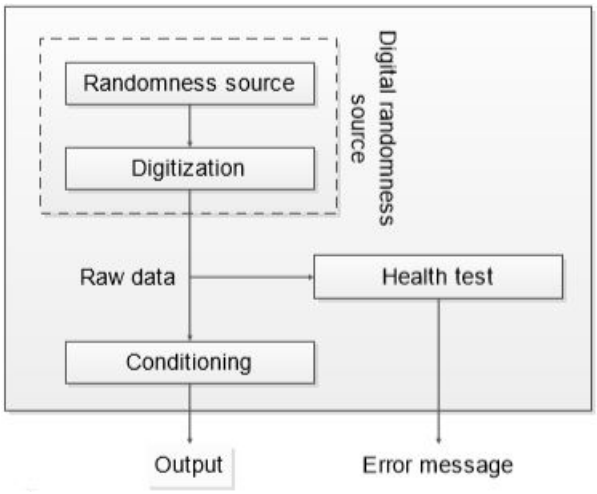


Figure 1: Entropy source model

2) The sensor sample is taken by placing the smartphone on the table, the direction of the smartphone screen is facing up to the rooftop, and the smartphone is in a motionless state.

3) The sampling period is ±0.01 second.

4) Every sample sensor consists of three independent measurement values which are the value of the measurements in the x-axis, y-axis, and z-axis orientation.

3.2 Digitalization

There are three consecutive steps to implement the digitization process:

1) Convert analog sample sensor into a binary sequence in accordance with the IEEE-574 Single-Precision 32-bit [7].

2) Choose the 8-bit position that is guessed to have the highest entropy value from the 32-bit binary sequence. The following steps are the procedure to choose these eight bits:

   - Acquire 1,100,100 samples continuously.
   - Choose 8 position bits with the occurrence percentage of bit 0 equal or very near to 50%.

3) Create a new data variant for each sample in addition to the three measurement values (x, y, and z-axis) which is the exclusive-or (XOR) result of these three measurement values.

Now, each sensor sample has four 8-bit binary sequences which are the measurement value in x-axis, y-axis, z-axis orientation and the XOR result.

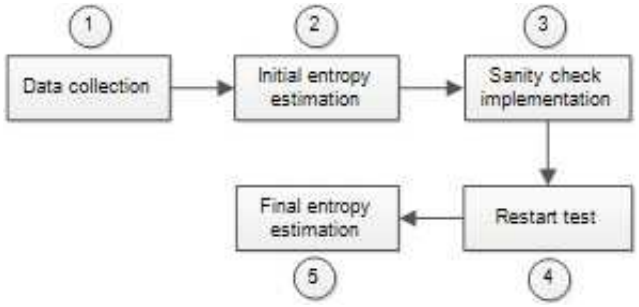


Figure 2: Entropy estimation process per sensor sample

3.3 Entropy Estimation Per Sensor Sample

Figure 2 shows the procedure of entropy estimation for each sensor sample.

1) Data collection: For each type of sensor on each Android smartphone, two types of data sets need to be formed, namely sequential data set and restart data set. Sequential data set is formed by operating the sensor continuously until 1,000,100 samples are obtained, while restart data set is formed by restarting the smartphone (power on power off power on) 1,000 times with each restart acquiring 1,010 sensor samples so that a restart matrix of 1,000 x 1,010 sensor samples is formed.

2) Initial entropy estimation: In estimating entropy value for each sensor sample, this research implements 10 entropy estimators proposed by the NIST SP 800-90B recommendation. These entropy estimators will measure entropy contained on a data set from a different point of view.

   The initial entropy estimation value $H_{initial}$ can be obtained by calculating the following equation:

   $H_{initial} = \min(H_{original}, \text{n x } H_{string})$

   with n = the bits-length of one sensor sample = 8 bits.

   The Horiginal and Hbitstring values are calculated according to the brief description below:

   - Calculating $H_{original}$ value: $H_{original}$ value can be obtained by implementing 7 entropy estimators (the collision, Markov, and compression estimator are excluded) to the sequential data set.
   - Calculating H_{string} value: It is already known that the size of the sequential data set is 1,000,100 samples. If all of these samples are concatenated sequentially, it will form a very long binary sequence which its bits-length size is 8 bits/sample x 1,000,100 sample = 8,000,800 bits. H_{string} value can be obtained by implementing all of the entropy estimators to the first 1,000,100 bits of this binary sequence.

3) Sanity check implementation: A sanity check is used to check whether the occurrence frequency of the most common sample in every row and column of the restart matrix is already as expected or not. If a smartphone sensor

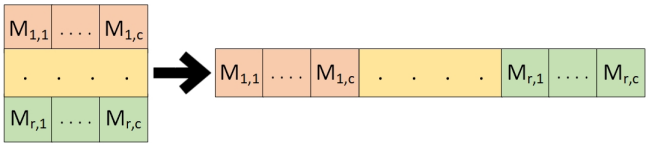
does not pass the sanity check, the entropy value of this smartphone sensor will not be estimated specifically, the entropy value is zero.

4) Restart test: The restart test is carried out to obtain row and column entropy estimation, or Hrow and Hcolumn. Both of these values are calculated by applying 7 entropy estimators (the collision, Markov, and compression estimator are excluded) to the row data set and column data set that are formed from the restart matrix, as shown in Figure 3.

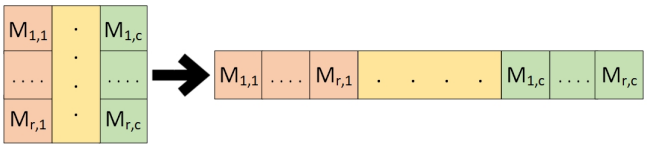
   The restart test is implemented to ensure that there is no pattern or dependency between sensor samples in a row/column matrix with sensor samples in another row/column matrix. Thus, there is no additional advantage for the attacker who has access/knowledge about sensor samples obtained from one/more restart process to guess the next sample.

5) Final entropy estimation: The final entropy estimation value (H) is calculated with the following equation: H = min($H_{initial}$,H_{row}, H_{column})

Table 3 shows the H value for accelerometer and gyroscope from five Android smartphones. Based on these values, the gyroscope is not selected as a randomness source,



(a)



(b)

Figure 3: Construction of (a) row and (b) column data set

Because many gyroscopes do not pass the sanity check and the majority of the H values for gyroscope are less than the H values for the accelerometer. Next, only accelerometer with XOR result is used as randomness source because this data variant has the highest H value than another three data variants (x, y, and z-axis) for the same sensor and smartphone type.

*Note: SC code representing that the sensor type for that type of smartphone is not passed by the sanity check.

There is an argument on why accelerometer with XOR result has the highest entropy value. Bit b has the highest entropy value if the occurrence probability b = 0 is equal to b = 1, or specifically Pr[b = 0] = Pr[b = 1] = 0.5. Suppose that there are two independent systems, X and Y, generating bit x and bit y randomly, where x,y ∈ 0,1. These bits will be XORed together to obtain bit z or z = x ⊕ y. It is known that the occurrence probability of bit 0 and bit 1 generated by X and Y are as follows:

Table 3: The H value for accelerometer and gyroscope from five Android smartphones

Smartphone	Sensor	H			
		x	y	z	XOR
Andromax R	Acccelrometer	1.63	0.35	1.94	4.98
	Gryscope	SC*	SC*	SC*	SC*
Asus Zenfone 2	Acccelrometer	1.78	2.38	3.07	6.35
	Gryscope	SC*	1.50	1.17	SC*
Galaxy Fame	Acccelrometer	2.51	3.17	3.30	6.55
	Gryscope	No gryscope			
Galaxy Note 10.1	Acccelerometer	1.31	1.71	2.49	4.36
	Gryscope	2.52	4.53	SC*	6.97
Galaxy S III Mini	Acccelrometer	3.29	3.28	3.41	3.85
	Gryscope	0.24	0.21	0.23	0.76

$$Syst.X : Pr[x = 0] = 0.5$$
$$Pr[x = 1] = 1\check{}Pr[x = 0] = 1\check{}0.5 = 0.5$$

$$Syst.Y : Pr[y = 0] = w$$
$$Pr[y = 1] = 1\check{}Pr[y = 0] = 1\check{}w$$

where 0 ≤ w << 0.5 or 0.5 >> w ≥ 1$

Therefore, the occurence probability in obtaining bit z equal to 0 or 1 are

$$Pr[z = 0] = (Pr[x = 0]xPr[y = 0]) + (Pr[x = 1]xPr[y = 1])$$
$$= (0.5xw) + (0.5x(1\check{}w))$$
$$= 0.5w + 0.5\check{}0.5w = 0.5$$

$$Pr[z = 1] = 1\check{}Pr[z = 0] = 1\check{}0.5 = 0.5$$

The occurrence probability of bit z on the above equations shows that the XOR result between entropy bit with non-entropy bit produces a probability occurrence value equal to entropy bit (see Figure 4).

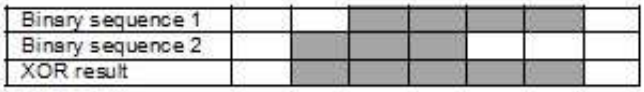


Figure 4: The XOR result between entropy bit (grey) with non-entropy bit (white)

3.4 Health Test

Health tests ensure that the randomness source is not having catastrophic failure or entropy deviation. To realize this, there

are two types of health tests are used which are repetition count test and adaptive count test. These health tests are always implemented before operating the entropy source and when the entropy source operates normally.

The repetition count test checks whether a certain sensor sample is produced C1-times consecutively or not, where C1 is the cutoff value of the repetition count test. If this cutoff value is reached, an error status is given. The adaptive proportion test checks whether the first sample in a block of 512 sensor samples is produced C2-times on that block or not, where C2 is the cutoff value of an adaptive proportion test. Same with the repetition count test, If this cutoff value is reached, an error status is given. The value of C1 and C2 are determined using the H value from Table 3.

3.5 Conditioning

Before explaining the conditioning process, starting from this conditioning step until the sensor sample is used outside the entropy source, the H value attributed to each accelerometer sample with XOR result is replaced by the smallest value that attributed to the x, y, and z-axis (see Table 4). This is done to attribute each sensor sample with a conservative H value.

Table 4: The conservative H value for five Android smartphones

Smartphone	H
Andromax R	H = min(1.63; 0.35; 1.94) = 0.35
Asus Zenfone 2	H = min(1.78; 2.35; 3.07) = 1.78
Galaxy Fame	H = min(2.51; 3.17; 3.30) = 2.51
Galaxy Note 10.1	H = min(1.31; 1.71; 2.49) = 1.31
Galaxy S III Mini	H = min(3.29; 3.28; 3.41) = 3.28

There are two reasons for implementing the conditioning process: to accumulate entropy value from several sensor samples into a single binary sequence and to remove bias contained in the sensor samples [2]. In this research, the conditioning process is implemented using the SHA-1 function as shown in Figure 5.

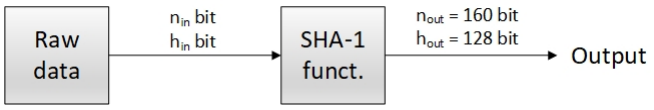


Figure 5: Conditioning process using SHA-1 function

where nin = w x n bit, hin = w x H bit, w = the number of sensor samples input, H = the entropy value for each sensor sample, and n = the binary size of a sensor sample = 8-bit. SHA-1 output is a binary sequence consisting of 160-bit and it is designed to have hout = 128 entropy bits. Figure 6 shows before and after the conditioning process on Galaxy Note 10.1 sensor samples.

4 Pseudorandom Number Generator (PRNG)

The PRNG system used in this research is implemented according to the diagram shown in Figure 7.

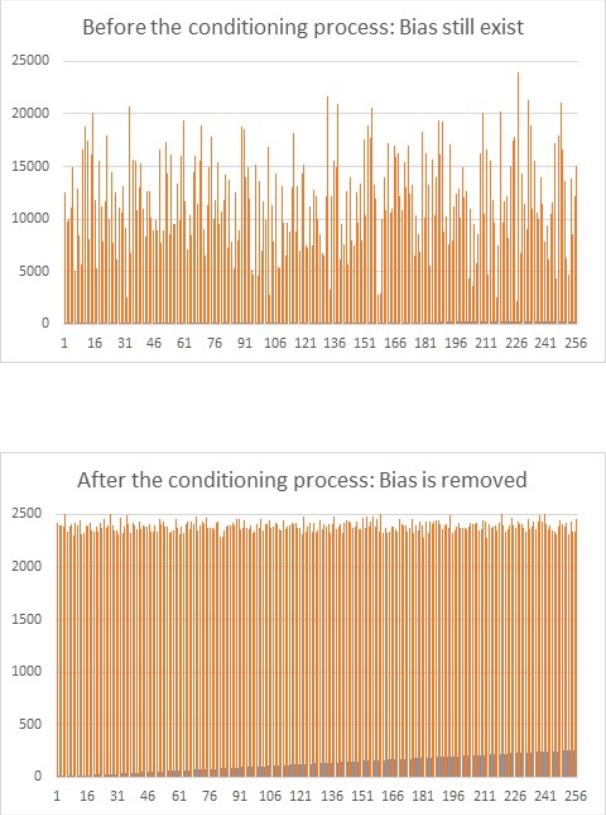


Figure 6: Before and after the conditioning process on Galaxy Note 10.1 sensor samples

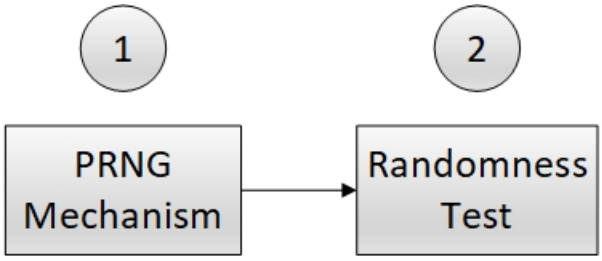


Figure 7: The implementation of PRNG system

4.1 PRNG Mechanism

NIST SP 800-90A recommendation proposed three types of PRNG mechanisms: Hash_DRBG, HMAC_DRBG, and CTR_DRBG [1]. In this research, HMAC_DRBG is chosen as the PRNG mechanism for the following reasons.

Reason not to select CTR_DRBG: CTR_DRBG uses encryption block as the building block. Encryption block has

a main character which is random permutation. Function f: $\{0,1\}^p$ $\{0,1\}^p$ is considered as random function if:

1) All of the domain and range values are equal,
2) The mapping process from domain to range is bijective,
3) Each of the domain value has an equal chance to be chosen by every domain values.

Because of the random permutation characteristic, encryption block is not appropriate to generate the random number [8]. For example, a PRNG based on encryption block is used to generate a sequence of four digits random integers 0-9 where:

- The encryption block used in here is random permutation function E(k,): $\{0,1\}^n$ x $\{0,9\} \cap \mathbb{N}$ $\{0,9\} \cap \mathbb{N}$ with k ϵ $\{0,1\}^n$,
- The algorithm implemented by the PRNG in generating four random digits is:

$E(k, r+1)||E(k, r+2)||E(k, r+3)||E(k, r+4)$
with r ϵ $\{0,9\} \cap \mathbb{N}$

Every digit in a sequence generated by the PRNG will surely have a different number. So, the total combination of four digits sequence that can be formed is 10 x 9 x 8 x 7 = 5,040 sequences from 10 x 10 x 10 x 10 = 10,000 sequences. This huge decrement of sample space size by the block encryption like this is far from random.

Reason not to select Hash_DRBG:

HMAC_DRBG has two main advantages over Hash_DRBG which are:

- The loss level when the attacker knows the critical state value [12],
- The uniqueness of value produced by the HMAC function over the value produced by the hash function.

Figure 8 shows the scheme of generating function for Hash_DRBG. If the attacker knows the counter value of k^{th} transition state, or $V^k = V^n + k$ for k ϵ [1,m], the attacker can recover the initial counter value V^0 and use it to obtain all of the hash block outputs, both before and after the k^{th} transition, in the same generate function call.

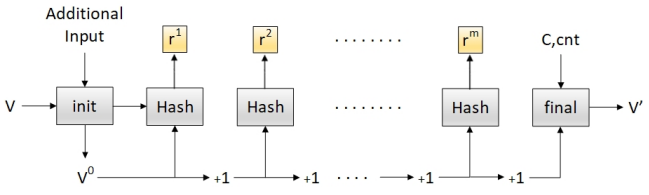


Figure 8: Generating function for Hash_DRBG

Figure 9 shows the scheme of generating function for HMAC_DRBG. If the attacker knows the initial key-value K^0 and the output value of k^{th} transition state, or r^k, the attacker can compute the next block outputs in the same generating function call by itself, specifically $r^j = HMAC(K^0, r^{j-1})$ where j ϵ [k+1,m]. For the output blocks produced before k^{th} transition state, these blocks are difficult to be recovered by the attacker even though he has already K^0 value because the attacker needs to perform preimage attack of r^j value, where $r^j = HMAC(K^0, r^{j-1})$ for j ϵ [1,k], to recover the r^{j-1} output block.

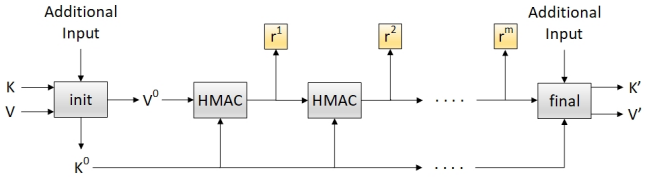


Figure 9: Generate function for HMAC_DRBG

It is known that the hash function is a deterministic function where the output value will always be the same for the same input value. Because the HMAC function implements hash function as its building block, the HMAC function is also deterministic. One thing that differentiates between hash function and HMAC function is the secret key involved in HMAC. Two equal data inputs will generate two different data outputs if the secret key used on both inputs are different. Figure 9 shows that at the end of generating function call of HMAC_DRBG, the key K^0 always updated. So, for a counter value V on two different generate function calls, the random number produced by each call will be different.

Description of HMAC_DRBG mechanism: Figure 10 shows the HMAC_DRBG mechanism. There are four functions involved in this mechanism, i.e instantiate function, reseed function, generate function, and uninstantiated function. Before explaining these functions, there is a function used by HMAC_DRBG to update internal state values K and V called HMAC_DRBG_Update, which its algorithm is:

HMAC_DRBG_Update(provided_data, K, V):
1) K = HMAC(K, V||0x00||provided_data)
2) V = HMAC(K, V)
3) If (provided_data = Null)
return(K, V)
4) K = HMAC(K, V||0x01||provided_data)
5) V = HMAC(K, V)
6) return(K, V)

Instantiate function of HMAC_DRBG:

Instantiate function is used to initialize PRNG by creating initial values for the internal state.

Instantiate_function(entropy_input, nonce, personalization_string):

1) seed_material = entropy_input ||nonce||personalization_string
2) K = 0x00 00 .. 00 comment: 160-bit
3) V = 0x01 01 .. 01 comment: 160-bit
4) (K, V) = HMAC_DRBG_Update(seed_material, K, V)
5) reseed_counter = 1
6) return(K, V, reseed_counter)

where entropy input and nonce are the binary sequence produced by the conditioning process (consisting of 128 entropy bits), while personalization string is a timestamp. Entropy input is used to inject 128 entropy bits into the internal state, nonce is used to ensure that the internal state is already injected by 128 entropy bits, and personalization string is used to differentiate the internal state value between two/more PRNG instantiation.

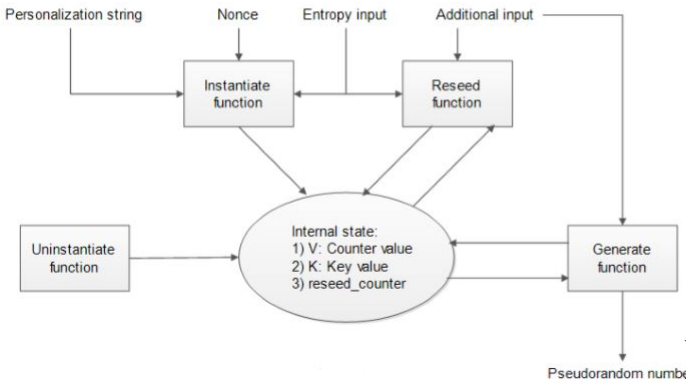


Figure 10: HMAC_DRBG mechanism

Reseed function of HMAC_DRBG:

Reseed function is used to inject new entropy bit into the PRNG internal state. where entropy input and additional input

Reseed_function(entropy_input, additional_input):
1) seed_material = entropy_input ||additional_input
2) (K, V) = HMAC_DRBG_Update(seed_material, K, V)
3) reseed_counter = 1
4) return(K, V, reseed_counter)

are the binary sequence produced by the conditioning process (consisting of 128 entropy bits). Same as before, entropy input is used for injecting 128 entropy bits into the internal state. Additional input has equal functionality with nonce, to ensure that the internal state is already injected by 128 entropy bits.

It can be seen that the insatiate function algorithm is very similar to the reseed function algorithm, specifically both algorithms inject two binary sequences, each with 128 entropy bits, into the internal state. Therefore, reseed function can be abolished and, if new entropy bits are needed, the instantiate function can be called. However, this practice is not recommended because it will be removed all of the entropy bits that previously collected; it shall be noted that the instantiate function set K and V values with a constant value, which are 0x00..00 and 0x01..01, before these values are injected with the entropy bits by calling HMAC_DRBG_Update, while the reseed function is directly injected entropy bit into K and V values without initializing these values with constant value first.

Generate function of HMAC_DRBG:

Generate function is used to produce random number as follow:

- When reseed_counter = 2^{48} requests, 11

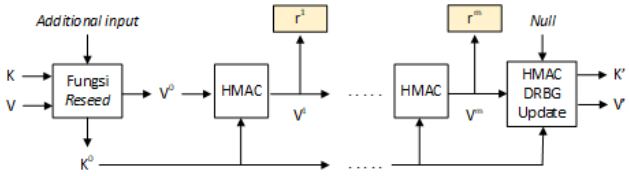


Figure 11: reseed

- When reseed_counter < 2^{48} requests, 12

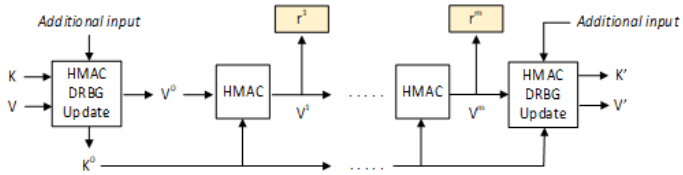


Figure 12: update

When reseed_counter is not yet reaching 2^{48} requests (or equal to 2^{48} generate function calls), the reseed function is not called at the initial of the generating process. The maximum value of reseed_counter is determined by the NIST SP 800-90B recommendation. This value is too big; it reaches the order of 10^{14}. For example, if the generate function is called every 1 second, the reseed function will be implemented after ≈ 8 million years. This is too vulnerable for the PRNG because the entropy bits will not be injected into the internal state in this period. To solve it, additional input, a 128 entropy bits binary sequence, is involved in the generate function as long as the reseed function is not called.

Uninstantiate function of HMAC_DRBG

Uninstantiate function is used to zeroing (i.e. erase) the internal state of a PRNG instantiation.

Uninstantiate_function():
1) K = null
2) V = null
3) reseed_counter = -1

4.2 Randomness Test

The randomness test for PRNG output is implemented with 15 randomness statistical tests proposed by the NIST SP 800-22 recommendation [3]. In this research, the randomness test

Table 5: The randomness test results for five Android smartphones

Test Type	Andromax R		Asus Zenfone 2		Galaxy Fame		Galaxy Note 10.1		Galaxy S III Mini	
	Minimum Pass Rate	Test Result	Minimum Pass Rate	Test Result	Minimum Pass Rate	Test Result	Minimum Pass Rate	Test Result	Minimum Pass Rate	Test Result
Frequency	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%
Block Frequency	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%
Runs	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%
Longest Run	80.00%	100.00%	80.00%	100.00%	80.00%	90.00%	80.00%	90.00%	80.00%	100.00%
Rank	80.00%	100.00%	80.00%	90.00%	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%
FFT	80.00%	100.00%	80.00%	100.00%	80.00%	90.00%	80.00%	100.00%	80.00%	100.00%
Non-Overslapping Template	80.00%	99.19%	80.00%	98.92%	80.00%	98.04%	80.00%	98.85%	80.00%	98.78%
Overslapping Template	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%
Universal	80.00%	90.00%	80.00%	90.00%	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%
Linear Complexity	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%
Serial	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%
Approximate Entropy	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%	80.00%	100.00%
Cumulative Sums	80.00%	100.00%	80.00%	100.00%	80.00%	95.00%	80.00%	100.00%	80.00%	100.00%
Random Excursions	85.71%	100.00%	80.00%	100.00%	80.00%	100.00%	85.71%	100.00%	83.33%	97.92%
Random Excursions Variant	85.71%	100.00%	80.00%	97.78%	80.00%	100.00%	85.71%	100.00%	83.33%	100.00%

is implemented on 10 data sets generated by HMAC_DRBG from every Android smartphone (one data set consisting of 1,000,000 random bits). The test results show that all of the randomness tests for five Android smartphones are passed (See Table 5).

5 Conclusion

(A) There are only two types of Android smartphone that have the potential to be used as randomness source, namely accelerometer and gyroscope. These sensors are selected because of its non-deterministic characteristic and its capability to produce sensor data in large numbers. Next, the output of each sensor type is divided into four data variants, which are the measurement value in the x-axis, y-axis, z-axis, and the XOR result of these three measurement values. After the implementation of the estimation process is done, only accelerometer data with the XOR result is chosen as the randomness source.

(B) The PRNG mechanism used in this research is HMAC_DRBG. CTR_DRBG is not selected as the PRNG mechanism because of the encryption block weakness which reduces the total combination of random numbers that can be generated.Hash_DRBG is not selected as the PRNG mechanism either because of the loss level when the attacker knows the internal state value is greater than HMAC_DRBG. Moreover, with the presence of the secret key in HMAC, even though two data inputs have equal value, HMAC will produce different output if the secret key used for each data input is different.

(C) The randomness test proposed by the NIST SP 800-22 recommendation can be implemented to measure the randomness quality of HMAC_DRBG output. In this research, HMAC_DRBG output for five types of Android smartphones is passed the randomness test.

References

[1] E. Barker and J. Kelsey, "Recommendation for random number generation using deterministic random bit generators," *NIST Special Publication 800-90A Revision 1*, 2015. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf)

[2] E. Barker and J. Kelsey, "Nist special publication 800-90c: Recommendation for random bit generator (RBG) construction," *Computer Security*, 2016. (https://csrc.nist.gov/CSRC/media/Publications/sp/800-90c/draft/documents/sp800_90c_second_draft.pdf)

[3] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, S. D. Leigh, M. Levenson, M. Vangel, N. A. Heckert, D. L. Banks, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *NIST Special Publication 800-22 Revision 1a*, 2010. (https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762)

[4] E. Falleti, F. Dovis, A.G. Quinchia, G. Falco and C. Ferrer, "A comparison between different error modeling of MEMS applied to GPS/INS integrated systems," *Sensors*, vol. 13, no. 8, pp. 9549–9588, 2013.

[5] T. W. P. Faraday, "An introduction to MEMS (micro-electromechanical systems)," *Prime Faraday Partnership's Technology Watch*, 2002. (https://www.lboro.ac.uk/microsites/mechman/research/ipm-ktn/pdf/Technology_review/an-introduction-to-mems.pdf)

[6] R. M. Gray, "Entropy and information theory," *Signals & Communication*, 2011. ISBN: 978-1-4419-7970-4.

[7] IEEE Computer Society, "Ieee standard for floating-point arithmetic," *IEEE*, 2008. (https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4610935)

[8] W. Kan, "Analysis of underlying assumptions in NIST DRBGs," *IACR Cryptology EPrint Archive*, 2007. (https://eprint.iacr.org/2007/345.pdf)

[9] J. Kelsey, K. A. McKay, M. L. Baish, M. S. Turan, E. Barker and M. Boyle, "Recommendation for the entropy sources used for random bit generation," *NIST Special Publication 800-90B*, 2018. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf)

[10] M. Matejcek and M. Sostronek, "Computation and evaluation allan variance results," in *NTSP - Proceedings of the International Conference on New Trends in Signal Processing*, 2016. DOI: 10.1109/NTSP.2016.7747786.

[11] D. Mougenot, J. Lainé, "A high-sensitivity mems-based accelerometer," *The Leading Edge*, vol. 33, no. 11, pp. 1234-1242, 2014.

[12] D. Shumow, J. Woodage, "An Analysis of the NIST SP 800-90A Standard," *IACR Cryptology EPrint Archive*, 2018. (https://eprint.iacr.org/2018/349.pdf)

[13] W. Stallings, *Cryptography and Network Security: Principles and Practice (7th Ed)*, 2016. ISBN: 1292158581.

[14] K. Wallace, K. Moran, E. Novak, G. Zhou, and K. Sun, "Toward sensor-based random number generation for mobile and iot devices," *IEEE Internet of Things Journal*, pp. 1189–1201, 2016. (https://doi.org/10.1109/JIOT.2016.2572638)

Biography

Yusuf Kurniawan received B.S Degree, M.S Degree and Ph.D Degree in Electrical Engineering from Institut Teknologi Bandung in 1994, 1997 and 2007 respectively. His research interest includes cryptography and information security.

Mochamad Beta Auditama was born in 28th September 1993. He received the B.Sc. degree in electrical engineering and M.Sc. degree in information security from Institut Teknologi Bandung, Indonesia, in 2015 and 2019. His research interest focus on cryptography.

Adaptive Fine-grained Access Control Method in Social Internet of Things

Hongbin Zhang[1,2], Pengcheng Ma[1], and Bin Liu[3,4]
(Corresponding author: Hongbin Zhang)
School of Information Science and Engineering, Hebei University of Science and Technology[1]
Shijiazhuang, P. R. China
Hebei Key Laboratory of Network and Information Security Hebei Normal[2]
School of Economics and Management, Hebei University of Science[3]
Technology Research Center of Big Data and Social Computing, Hebei University of Science[4]
(Email: hbzhang@live.com)
(Received June 27, 2019; Revised and Accepted Dec. 12, 2019; First Online Feb. 1, 2020)

Abstract

Social Internet of Things (SloT), as a new carrier of integration of social and Internet of Things, applies the research results of social networks from different aspects of the Internet of Things. Different types of connected intelligent objects interact socially, compared with random data access between them, access control technology is more stringent. This paper integrates social attributes into attribute-based access control of Internet of Things, initializes relational attribute tags, and labels social interest attributes for different objects, then quantifies tag similarity and implements initial access control authorization, integrates social attributes into game theory to dynamically adjust access control policies, so the adaptive fine-grained division of access control under the Social Internet of Things is effectively realized. The experimental results show that our method can not only effectively carry out initial authorization according to tag similarity, but also further adaptively adjust the permission policy according to social attributes, and further meet the fine-grained partition requirements of access control, which is ensure the effective implementation of access control under the Social Internet of things.

Keywords: Access control; Dynamic adaptation; Game theory; Social Attributes; Social Internet of Things

1 Introduction

Internet of things is regarded as an important opportunity for development and change in the field of information. The European Commission believes that the development and application of Internet of things will bring great contribution to solving modern social problems in the next 5-15 years. It is estimated that by 2020, there will be 25 billion various things (devices, sensors, software or databases) that can connect to the Internet wirelessly. [1]. Gartners predicts that the number of connected things will be generated by consumer applications, and most of the revenue will be contributed by enterprises. This sudden development will support the Internet of things as the economic effect of consumers, and enterprises will find new ways to use this technology. According to Manyika, by 2025, the use of the Internet of things can create 4-11 trillion economic value, which is equivalent to 11% of the world economy [9].

Social media is an Internet-based technology for sharing ideas, activities and professional interests. The development of the Internet of Things is changing the way social media is used. The daily connection between people, objects and data creates an intelligent network, which adds value to the people involved [12]. The Social Internet of Things adds attributes of social networks to the Internet of Things, analogous to human social networks to define the social relationships between objects in the Internet of Things. The model of social Internet of things is designed, the structure of social network based on objects of the Internet of things is analyzed, so that the model of human social network can be extended to a variety of fields based on things-things ,things-people, people-things and people-people [8].

Heterogeneous devices and information exchange are ubiquitous in the social Internet of things, which requires more effective access control measures for services. Traditional access control based on Internet of Things mostly choose to build trust model and risk model [5]. We propose an access control model in the social Internet of Things, which integrates social attributes into the attribute-based access control model in the Internet of Things. The game theory is used to integrate social attributes to achieve dynamic fine-grained rights partitioning in SloT environment.

The rest of this paper is organized as follows. In Sec-

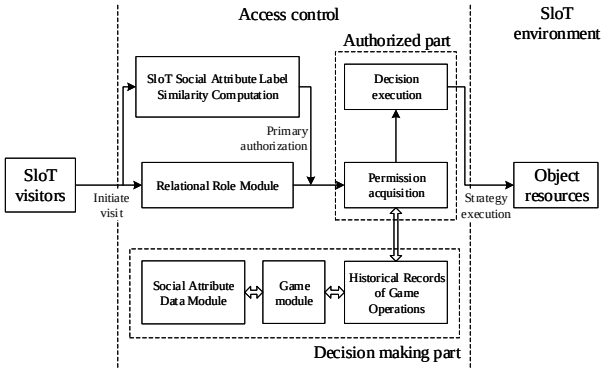


Figure 1: Access control model based on game theory

tion 2, we present the related work. Section 3 gives the preliminaries of this paper. Section 4 describes the access control model and the game process in detail. The 5th section carries on the experiment simulation and the verification as well as the method contrast. We conclude the whole paper in Section 6.

2 Related Work

Social Internet of things as a new integration carrier of social network and Internet of things, through the traditional structure of the Internet of things to add social attributes to achieve the effective operation of social Internet of things scenarios, this paper studies the idea to explore the deeper structure characteristics of the Internet of things and social network attributes based on the integration of access control methods under the current social Internet of things. Through the research of the security problem of the combination of the two, it lays a solid foundation for the research of adaptive fine-grained access control under the social Internet of things.

Social Internet of Things integrates the concepts of the Internet of Things and social networks to integrate social attributes into the huge Internet of Things terminal nodes. Akash Sinha et al proposed a framework of social Internet of Things to support the interaction between devices with different functions and heterogeneous platforms by developing applications that provide effective services for the Internet of Things by utilizing users'social behavior, which can reasonably interact with the social behavior of the Internet of Things. Literature [14]. Literature [15] through the construction of online trust model, classifies the roles of users in social networks and provides threshold trust score, which will be further applied to role allocation. Literature [2] proposes a risk-based access control model for Internet of Things (IOT) technology, which considers real-time data requests of devices in the Internet of Things and gives dynamic feedback. User context, resource sensitivity, action severity and risk history are used as input of the security risk estimation algorithm. By confirming the security risk of the request, a reasonable data basis is proposed for policy formulation. No matter the trust model or the risk model, although there are no research examples of the fusio n attributes in specific scenarios, they have rich research basis in satisfying the social network and the Internet of things scenarios, which provides ideas for the fine-grained access control division under the social Internet of things.

According to the behavior analysis of entities in reference [13] access control can be regarded as a game between requester and visitor, and a dynamic game access control model based on trust is proposed. In this paper, the access of nodes is clearly divided into two types: goodwill and malice, which obviously lacks in the fine-grained access control division work, and the article model is not in the actual access control situation, and there is no clear introduction to the implementation of the model. The trust value of nodes is evaluated according to shared contribution, shared cost and organizational contribution.The Access Control Middleware mentioned in document. The Access Control Middleware mentioned in document [4] not only considers the subject behavior and trust value, but also describes in detail the dynamic adaptation process of an access control policy based on risk value, policy and rule set. Literature [11] proposes a dynamic and fully distributed access control policy in the framework of the Internet of Things. Block chains satisfy the distributed concept of the Internet of Things, which strengthen the construction of dynamic adaptive learning model in line with the environment of the Internet of Things. However, the paper does not quantify the specific implementation of access control strategy, only proposes a conceptual framework model for follow-up. However, the dynamic and effective solution of access control under the blockchain is still of great significance to solve the problem of traditional Internet of things distributed scenarios. research.

3 Preliminaries

As a new social carrier, Social Internet of Things integrates social network concepts into Internet of Things (IoT) solutions to enhance the ability of Internet of Things network services in an objective and effective way. The effective operation of SloT poses new challenges to

the implementation of access control. We propose an access control model based on repeated game in the social Internet of things. The specific block diagram is as Figure 1.

SloT access is directly authorized if it meets the "Special relationship" in the relational role attributes. If it is not, the primary matching authorization is performed according to the SloT social attribute tag similarity. When the visitor initiates the SloT social behavior and triggers the two-party game, the two parties perform multiple repeated games.Each game record is counted into the game operation history record, and the mixed strategy Nash equilibrium calculation is performed according to the game operation history record.

3.1 Relational Attribute Label

Firstly, we divide the access control of nodes according to the similarity of labels, and then adjust the access control adaptively by using game theory according to social attributes. Based on the model. The tag similarity algorithm gives the preliminary division basis of access control.

Definition 1. *User tags are extracted from SloT's social attribute resources, the user tag behavior is represented by a set of triples, where the Ra-data record* (v, c, l) *indicates that the user (node)* v *labels the category* c *with the content* l*.*

v is the node Id, which is the account identifier of the SloT, and is used to distinguish different accounts

$$v = \{v_1; v_2; \cdots, v_i\},$$

indicating different Id;

c is the node label category, including relationships, roles, interests and other categories; l is the content of the label;

Rr-attribute (Relational role attributes), preliminary role validation and SloT node validity are carried out, which are satisfy the numerical Boolean structure.

The set of degree nodes connected by SloT node v.

$$\mathrm{f}\left(V_{i,}\right) = \left\{V_{ik,}\right\}, \quad \mathrm{k} = 1, 2, \ldots, \mathrm{n}.$$

By independently calibrating the relationship attributes between the nodes, we can get their relationship role attributes eigenvalues:

$$\mathrm{B_i}\left(\mathrm{v_i}\right) \begin{cases} 1, \text{Coincidence characteristics} \\ 0, \qquad\qquad \text{otherwise} \end{cases}, i = 1, \ldots, n.$$

I is the number of nodes with different relational attributes extracted, For example, $B1$ $(v1)$ is the relationship label information between a subject and an object. If marked as "intimate relationship", you can directly enjoy the highest privileges, but if the account is identified as "bad friends", you can directly exclude it.

3.2 Interest Attribute Label

Din-attribute: SloT node has n dynamic interest labels to define the personalized interest identification of the node for subsequent node interest similarity calculation.

In the SloT environment, facing the access requests of many nodes, the object calculates the initial authorization according to the matching similarity of the labels that the nodes have. In the process of social behavior of SloT, the nodes gradually form their own interest labels. For the account with unexpected loss of interest label attributes, we can generate the personalized interest topic labels of nodes through our improved label propagation algorithm (LPA) [6]. The specific algorithm implementation process is as follows:

Input: Adjacency Matrix of Undirected Unweighted Graph Adjacentmatrix, node number VerticeNum.

Output: Classified array for storing node labels Community.

Step 1: Save all neighbors of the i node into the neighbor array.

Step 2: When the classification criteria are not met or the iteration threshold is not exceeded, the number of tags in the neighborhood of the node is counted.

Step 3: If there is only one tag with the most number, assign the value directly; If there are multiple tags with the same number, select one at random.

Step 4: Determine whether the node label exceeds the iteration threshold, and re-enter if it does not Adjacent matrix, Until you find a community that meets the requirements community.

The object authorizes the nodes according to the Boolean value of the relationship role attribute, and then uses the similarity of interest tags as the authorization basis of other nodes, The similarity of subject and object tags still plays a dynamic role in the ubsequent access control process. The specific calculation process of label similarity is as follows.

Definition 2.

$$\begin{aligned} v_1 &= \left\{l_{i1}, l_{i2}, l_{i3}, \cdots l_{(ik)}\right\} \\ v_2 &= \left\{l_{j1}, l_{i2}, l_{j3}, \ldots l_{(jk)}\right\} \end{aligned}$$

The number of labels $m < k < n$, m and n are both single values. If the value of k is too large, the interest labels of the account nodes may be too broad to be correctly classified into valid permission levels. If the value of k is too small, the fewer the labels, the larger the similarity value is or even close to 1. And we have to further define the weights for the k labels of node v.

Table 1: Account private label corresponding number and its value corresponding table

Label serial number	Value
1	k_v
2	k_{v+1}
...	...
k-1	k_2
k	k_1

List the label vectors with the value, and then calculate the similarity between the two according to the similarity formula. The similarity formula is as following Label similarity:

$$\cos\theta = \frac{v_1 \cdot v_2}{\|v_1\| \, \|v_2\|}$$

4 Game-based Adaptive Access Control Model

In the SloT environment, besides the adaptability of label similarity, the interviewee hope to gain effective interaction from the visitors through reasonable SloT authorization, while the visitors need to pay a certain amount of SloT behavior to gain reasonable authorization from the respondents. Through effective game theory interaction, the two sides can obtain more practical value in accordance with the SloT environment to adapt to dynamic and complex SloT environment. We use the repeated game model to describe the behavior of both the subject and the object (in the game process, in order to show the game relationship between the subject and the object, we call the subject as the visitor and the object as the interviewee). The specific process of the game is as follow:

v: Indicates the player who participates in the game, and only two-party games are considered in our model, that is, the visitor and the interviewee are expressed as $v = \{v_a, v_b\}$.

u: Indicates the profit of both sides of the game, $u = \{u_a, u_b\}$.

In the course of both games, each party will seek to maximize their own interests.

$\beta(\gamma)$: discount factor: $\beta(\gamma) \in [0, 1]$ is the discount factor to control the rate of change of income with time. Which can also be understood as the patience level of the person in the game. In this paper, we take $\beta = \gamma = 1$, $\beta(\gamma)$ represent the discount factor of the visitor and the interviewee respectively.

s: The policy adopted by both sides of the game, that is, the SloT behavior. The visitor needs to pay more and more effective SloT social behavior to obtain higher SloT access rights, while the interviewee needs reasonable authorization, the two parties denoted as $\{s_a, s_b\}$.

The s expenditure (and is also the income of the interviewee) can be divided into n kinds of behaviors

So a total of $s_a == 2^n$ kinds of collection behaviors.

We stipulate that visitors must initiate SloT behavior to trigger the game, that is, the visitor initiates $2^n - 1$ sets containing SloT behaviors.

The interviewee has corresponding $s_b = 2^n - 1$ permission policy selection.

The interviewee expenditure (and is also the income of the visitor).

When the visitor adopts the $2^n - 1$ level SloT behavior, the interviewee gives the permission $2^n - 1$ level to perform repeated games.

When the t-th game is played, the visitors income (the interviewee's expenditure) is as follows

$$U_a = U_a + \beta U_a + \beta^2 U_a + \ldots + \beta^{t-1} U_a = \Sigma_t \beta^{t-1} U_a = t^* U_a$$

T is number of times. When the t-th game is played, the income of the interviewee (the visitors' expenditure) is as

$$U_b = U_b + \gamma U_b + \gamma^2 U_b + \ldots + \gamma^{t-1} U_b = \sum_t \gamma^{t-1} U_b = t^* U_b$$

T is number of times. All of the t repeated games, the final payment matrix can be obtained.

$$\begin{bmatrix} (1,1) & \ldots & (1,n) \\ \vdots & \ddots & \vdots \\ (n,1) & \ldots & (n,n) \end{bmatrix}$$

Through the payment matrix, we can find that visitors have $2^n - 1$ level of SloT behavior, the interviewee has $2^n - 1$ kinds of permission policies, and the interviewee can use game theory to find out The accessibility level of the visitor's best authority is to select the appropriate Nash Equilibrium [10] for authorization according to the game theory.

The above Nash Equilibrium only applies to the specific non-randomness action plan of each player in the pure strategy form, while the mixed strategy Nash Equilibrium shows that the player can randomly select a pure strategy from the pure strategy set according to a certain probability as the actual action. Further elaboration of hybrid Nash equilibrium makes the access control system more effective in adapting to complex and changeable SloT environment.

The probability of a visitor's action in the face of a resource is expressed as a vector form of

$$\mathrm{p} = \{p_1, p_2, \ldots, (1 - p_i)\}$$

The probability of authorization requirement of the interviewee in the face of the visitor is expressed in the vector form of

$$q = \{q_1, q_2, \ldots, (1 - q_i)\}$$

Table 2: Similarity matching value and initial permission level table

Serial number	interviewee	Visitor	Similarity Matching Value	Initial permissions
1	2A50	On3k	0.3337789963679875	2
2	bRlo	r0aw	0.4351501871273176	3
3	5osV	T0jx	0.10745062398909976	1
4	CRqw	eS2B	0.74527581901392475	4
5	z2wn	N4Gk	0.9611650085651615	5

Visitors' expectations are represented by the hierarchical value $c = \{c_1, c_2, \ldots, c_i\}$ of each level of the diagonal matrix.

The expected value of the interviewee is expressed in the diagonal value $\mathrm{d} = \{\mathrm{d}_1, \mathrm{d}_2, \ldots, \mathrm{d}_\mathrm{i}\}$ of each level of the matrix.

Visitors' expected payment is

$$EU_a = c_1 * p_1 + c_1 * p_2 + \ldots + c_i * (1 - p_{i-1}) .$$

Interviewee's expected payment is

$$EU_b = \mathrm{d}_1 * q_1 + \mathrm{d}_2 * q_2 + \ldots + \mathrm{d}_\mathrm{i} * (1 - q_{i-1}) .$$

In game theory, there are only two players, the visitor and the interviewee, but each player has a variety of strategic options, so we can calculate the expected payment of each person's mixed strategy Nash equilibrium in the face of complex situations, in order to adapt to the more dynamic and changeable SloT environment.

5 Experimental Simulation And Verification

We assume that there are 100 Id sources, each node has its own content tags of $l = 6$ from social attributes, and that there are $n = 4$ kinds SloT behaviors for visitors, then there are a total of $s = 4^2 - 1$ policy choices for the Interviewee. Our content tags based on social attributes originate from a social networking site in China. The weights of six tags are calculated according to the current ranking of the calorific value of the tag in the overall website. Our experiment sets that the weights of each Id tag are ranked according to its calorific value on the website.

Normalization method can well normalize all Id label weight values, reduce the inuence of large eigenvalues on the difference between vectors, and eliminate the imbalance caused by the difference between attributes. In the calculation of node label weight, the raw data is linearly transformed using the standardization method of dispersion:

$$x' = \frac{(x - \min)}{\max - \min}$$

In order to reflect individual differences, we randomly selected 30 Id from 100 Id sources as visitors'Ids, matched the remaining 99 Ids with label similarity, and randomly selected 5 groups as our experimental objects, giving the result as Table 2.

From Table 2, we can see that our adaptive model initially authorizes visitors according to their interest tags, allowing them to read part of the interviewee's resources. Through the study of literature [3, 7], we can know that the social behavior of online visitors meets a certain degree of Gauss distribution, so we analyze the online social behavior of some users of a domestic website, and randomly select some users and related data as the behavior basis of our method.

$$\mu = \frac{X}{N}$$

$$\sigma = \sqrt{\frac{\Sigma(X - \mu)^2}{N}}$$

σ is the standard deviation, X is the variable, μ is the total mean, and N is the total number of cases.

We take the two groups of 1-3 groups as examples. The visitor's access behavior satisfies the Gaussian distribution, but in the early stage of the experiment, we must manually remove some nodes with larger differences, corresponding to the right oblique upper triangle the lower left triangle of the payment matrix. We consider that the difference $\geqslant 5$ in the two-dimensional array is the point of great difference, which can be removed manually. Three groups of visitors were randomly selected from a certain platform to verify our experiment on the premise that their online social behavior meets the following requirements.

The 15*15 payment mmatrix of game parties based on our experimental simulation, we can easily find that the diagonal line of the matrix belongs to the ultimate ideal state of our game. Since we initially excluded the difference $\geqslant 5$ in the expected payment two-dimensional array, we left a total of 9 diagonal data in the order of 1-9 from bottom to top, then the final expectation such as the distribution in the table, that is, the visitors matched the income permissions corresponding to their own efforts, so our method was verified, and the model can adapt dynamically according to the behavior subject and object to form an effective adaptive adjustment and fine-grained access control division

$$\begin{bmatrix} (1,1) & \ldots & (1,15) \\ \vdots & \ddots & \vdots \\ (15,1) & \cdots & (15,15) \end{bmatrix}$$

Table 3: Similarity matching value and initial permission level table

Visitor situation \ Number of visits	5	10	15	20	30	40
μ=4.1, δ=2.43	5.1085	4.7077	5.5986	5.6388	5.7460	5.7470
μ=7.32, δ=3.62	4.2548	5.9819	5.0096	6.0772	6.8670	6.7359
μ=2.18, δ=2.76	6.8614	6.1879	4.6837	5.2983	5.7629	5.8656

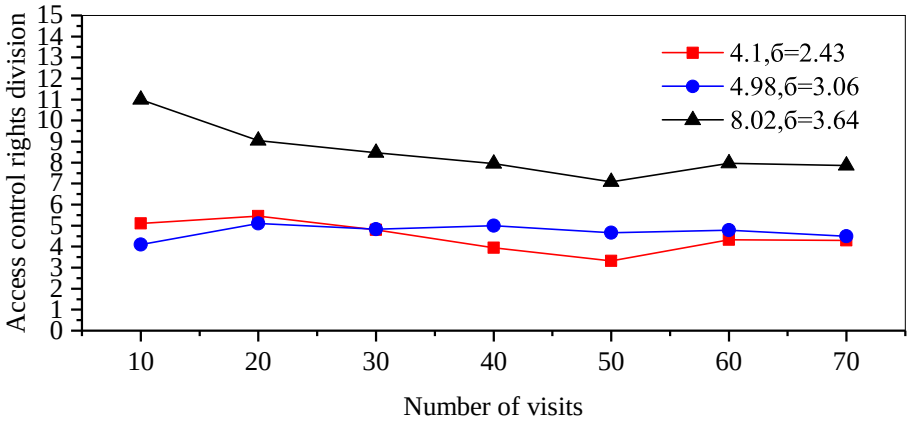


Figure 2: Access control adaptive state diagram

In our experiment, we initially authorized visitors based on tag similarity, but at the same time, similarity tags still play an important role in subsequent visitors. The third is the adaptive adjustment process of the experimental group as shown in the figure.

According to Figures 2, we can see that the experimental group starts with the initial permissions, which are granted according to the label similarity of the nodes. With the social behavior of the visitors, the double access control game is triggered. Combined with the social behavior of the visitors conforming to the Gauss distribution, the authorization strategy of the visitors gradually stabilizes, and the access control model passes through both sides. The multiple game gradually adapts to the strategies of both parties, and forms the reference basis for the access control behavior of both the subject and the object.It can be further seen from Figure 2 that at the beginning of accessing resources, the three groups of visitors have respectively obtained levels 1-3 preliminary access rights according to their own tag similarity. With the implementation of the adaptive model, they have achieved levels 1-5, levels 2-5, levels 3-7 adaptive comparison display.

6 Conclusions And Future Work

Referring to the traditional attribute-based access control model in the Internet of Things, this paper effectively integrates the social attributes of nodes and constructs a reasonable access control strategy by using game theory, which effectively guarantees the dynamic fine-grained adjustment of access control schemes in the Internet of Things. Experiments show that the model can not only preliminarily authorize based on label similarity, but also dynamically adjust access control strategies according to social attributes, which achieve fine-grained partitioning of policies. In the next step, we introduce the topic of how to dynamically and adaptively adjust social attribute tags into our access control framework. which will provide an effective theoretical and experimental basis for further implementation of access control in the social Internet of things.

Acknowledgements

This research was supported by the National Natural Science Foundation of China (61672206,61572170), Hebei Province Science and Technology Support Program (17210104D), Hebei Province Innovation Capacity Improvement Program Soft Science Research and Science Popularization Project (17K50702D), College Science and Technology Research Project of Heibei Province (ZD2015099).

References

[1] Z. Andrea, B. Nicola, C. Angelo, V. Lorenzo, and Z. Michele, “Internet of things for smart cities,” *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014.

[2] H. F. Atlam, A. Alenezi, R. K. Hussein, and G. B. Wills, "Validation of an adaptive risk-based access control model for the internet of things," in *International Journal of Computer Network and Information Security*, vol. 1, pp. 26–35, 2018.

[3] X. Dong, H. Sandra, and C. Ming, "Opinion behavior analysis in social networks under the influence of coopetitive media," vol. PP, no. 99, pp. 1–1, 2019.

[4] O. Hamdi, A. N. Ben, and S. L. Ben, "Towards a self-adaptive access control middleware for the internet of things," in *International Conference on Information Networking*, 2018. DOI: 10.1109/ICOIN.2018.8343178.

[5] B. Lee, R. Vanickis, F. Rogelio, and P. Jacob, "Situational awareness based risk-adaptable access control in enterprise networks," in *The 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS'17)*, pp. 400–405, 2017.

[6] W. Li, H. Ce, M. Wang, and X. Chen, "Stepping community detection algorithm based on label propagation and similarity," *Physica A Statistical Mechanics and Its Applications*, vol. 472, pp. 145–155, 2017.

[7] Q. Liu, Q. Liu, L. Yang, and G. Wang, "A multi-granularity collective behavior analysis approach for online social networks," *Granular Computing*, vol. 3, no. 4, pp. 333–343, 2018.

[8] A. Luigi, C. Davide, and I. Antonio, "Smart things in the social loop: Paradigms, technologies, and potentials," *Ad Hoc Networks*, vol. 18, no. 7, pp. 121–132, 2014.

[9] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, and D. Aharon, *Unlocking the Potential of the Internet of Things*, 2015. (`https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world`)

[10] J. F. Nash, "Equilibrium points in n-person games," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 36, no. 1, pp. 48–49, 1950.

[11] A. Outchakoucht, H. Es-Samaali, and J. Philippe, "Dynamic access control policy based on blockchain and machine learning for the internet of things," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 7, pp. 417–424, 2017.

[12] A. Sabri, "A proposed social web of things business framework," in *International Conference on Engineering and Technology (ICET'17)*, pp. 1–5, 2017.

[13] M. Shunan, "Dynamic game access control based on trust," in *IEEE Trustcom/BigDataSE/ISPA*, 2015. DOI: 10.1109/Trustcom.2015.532.

[14] A. Sinha and P. Kumar, "A novel framework for social internet of things," *Indian Journal of Science and Technology*, vol. 9, no. 36, 2016.

[15] T. Vedashree and N. M. Parikshit, "Trust-based access control in multi-role environment of online social networks," *Wireless Personal Communications*, no. 1, pp. 1–9, 2018.

Biography

Hongbin Zhang is an Associate Professor of the School of Information Science and Engineering at the HEBUST, he received his BS degree from the Department of Automation at HEBUST in 1998, his MEng and PhD degrees from the School of Computer Science and Technology at the Xidian University in 2005 and 2009, respectively. His current research interests include security and management of network, insider threat analysis, etc

Pengcheng Ma is a graduate student of Hebei University of Science and Technology, majoring in Internet of Things security and management during his postgraduate period, and has published two papers in related fields.

Yan Zhang 23 years old, an undergraduate from Shenyang Normal University, major in information security management. In the four years of college, after completing her studies, she enjoys reading the book related to this major. Under the guidance of the teacher, she has published two articles in EI journals.23 years old, an undergraduate from Shenyang Normal University, major in information security management. In the four years of college, after completing her studies, she enjoys reading the book related to this major. Under the guidance of the teacher, she has published two articles in EI journals.

A P2P Anonymous Communication Scheme in IOT Based on Blockchain

Ye Lu
(Corresponding author: Ye Lu)
Baoji University of Arts and Sciences
Baoji, Shaanxi 721000, China
(Email: luye528@126.com)
(Received Sept. 22, 2019; Revised and Accepted Dec. 16, 2019; First Online Feb. 10, 2020)

Abstract

In order to ensure the anonymity and non-traceability of the identity of Internet of things devices across administrative domains, an anonymous communication scheme based on alliance blockchain is proposed. Centralized identity authentication and decentralized message communication mechanisms are implemented by dividing the base domain and the interconnect domain. The zero-knowledge proof of identity is based on the identity authentication mechanism of the Merkle-tree. Further, the aggregation signature privacy protection scheme based on the CoinJoin idea is proposed to confuse the domain manager node identity to resist the identity association analysis attack. Finally, a consensus mechanism based on reputation evaluation strategy is proposed for message consistency. Security and efficiency analysis show that the proposed solution can protect identity privacy with lower storage and computational overhead.

Keywords: Anonymous; Consensus Mechanism; Identity Authentication

1 Introduction

IOT refers to a network that implements information exchange between heterogeneous devices through various communication technologies. Its remarkable characteristics are heterogeneous and low power consumption. The devices in the large-scale internet of things often belong to different managers, which affect their network architecture. The centralized IoT usually lacks interactivity, limits its intelligence, and deviates from the IoT 's purpose of driving people, and there is a risk of perjury and information leakage. The equipment in the distributed internet of things and its company have the demand of information interaction both inside and outside the area, which involves the interest game between them, and it affects the user undefine's identity privacy and information security in the absence of trust.

In the distributed and de-trusted form, blockchain technology has become an important cornerstone for solving decentralization and building trust. Blockchain technology is superior in that it can guarantee complete traceability, tamper resistance, replay and public verifiability of messages. The blockchain theory establishes trust between nodes based on the high-energy POW consensus mechanism and the transaction fee incentive mechanism. In order to expand the application of blockchain technology, a semi-centralized alliance and a fully centralized private chain have been developed.

The distributed IoT management mode relates to cross-domain information interaction between a plurality of devices and management platforms, and has common characteristics with the chain block chain.

Therefore, this paper proposes a lightweight and efficient anonymous authentication scheme based on alliance chain technology. The main contributions of this paper include three aspects:

1) A distributed network model based on the alliance chain is proposed, and the double-chain structure of the centralized identity authentication chain and the distributed message chain is realized by dividing the basic domain and the interconnection domain.

2) A scheme of zero knowledge proof of identity based on Merkle tree is proposed, and a privacy protection scheme of aggregated signature based on CoinJoin is proposed, which realizes the anonymity and non-traceability of identity.

3) In order to solve the problem of efficiency, the credit value evaluation and the FCFS strategy are put forward to solve the problem of message consistency.

2 Related Research

The alliance chain is a special form of the private chain. Its particularity is reflected in the authentication and negotiation process of message and identity completed by the proxy node. Literature [18] constructed and

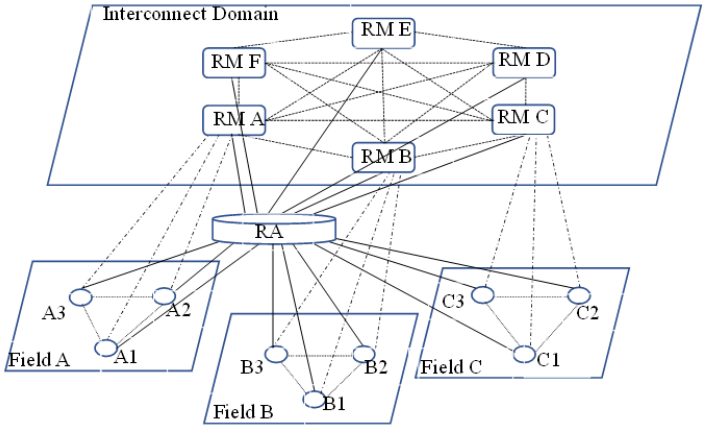


Figure 1: BC-IOT network architecture

prospected he blockchain application of intelligent distributed power energy system, and proposed the concept of "blockchain group" based on alliance chain, which realizes full-service coverage, and innovation proposes cross-domain overlapping verification ideas. In literature [8], the security events of Blockchain are analyzed, and it is found that the problems mainly focus on privacy disclosure and consensus evil.

In terms of privacy protection, literature [13] indicates that, despite the anonymity of the address, an attacker can still bind the address to the user ID through social engineering. Literature [7] proposed the Coinjoin idea, which confuses the address relationship between transactions and protects user identity privacy. Literature [17] constructed a blockchain-based privacy protection scheme based on homomorphic encryption and smart contract technology. This scheme can realize the claims function without acquiring the identity of the claim object. However, the scheme does not give the detailed design of the multi-party consensus algorithm.

In terms of identity authentication, the literature [3] pointing out that due to the differences in requirements and scenarios, the blockchain authentication system should be weighed in terms of privacy, security and timeliness. In [10], for the cross-domain authentication problem in information service, the PKI domain blockchain certificate service system guarantees the credibility of the third-party server and designs a cross-domain authentication protocol. In [19], a trust chain model and system architecture is designed based on the blockchain certificate authority, which realizes two-way entity authentication, but does not solve the privacy leakage problem.

3 The Authentication Based on Merkle Tree

3.1 The Network Architecture

According to the cross-platform access and P2P communication increased dramatically, the structure of IoT is divided into a basic domain and an interconnected domain. The Regional Manager (RM) is responsible for the communication of all terminal nodes in the domain. The interconnection domain is composed of multiple domain managers, and the communication consensus is obtained based on the alliance chain mechanism. In order to reduce the storage and communication load, ensure identity privacy and traceability, the data structure based on the Merkle tree is defined. Finally, the domain manager performs identity authentication on behalf of the terminal node. See Section 4 for details.

The network architecture (BC-IOT) is shown in Figure 1. In the field A, the node A1 wants to join the network and needs to register at the RA first. When A1 needs to communicate with C1, A1 must obtain the certificate at the RA through RMA and establish a connection with C1 through RMC. Specifically path A1 ⇒ RMA ⇒ RMC⇒ C1. Due to the low computing and storage capacity of the terminal nodes, each node only records the messages between itself and the area manager, and finally stores the data in a chained database. Each area manager has strong storage and computing capabilities, and can communicate with other area managers and terminal nodes in the area for communication and fee settlement. Therefore, the area manager performs consensus recording of inter-area communication and transactions.

3.2 Authentication Scheme

As the only registration center of the whole network, RA is responsible for registering various types of nodes and recording the identity of the nodes into the identity table of the Merkle tree structure. The specific steps include the system key generation phase, the registration phase, and the certification phase.

In the key generation phase, the zone manager or terminal node makes a registration request to the RA. The RA sends its own public key to the node, and the node generates a random number r, and combines the RA public key to generate the private key PR_{node} and the public key PU_{node} of the node itself.

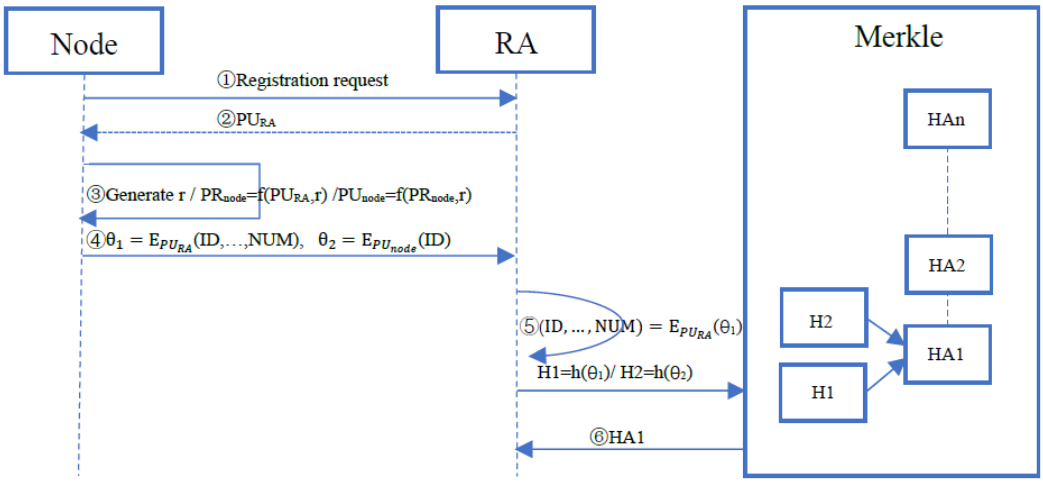


Figure 2: Node registration process

In the identity registration phase, in order to protect the node identity privacy and authentication efficiency, the Merkle tree structure is used to store the hash value of the node identity information, and the RA uses the relevant path node information to verify the data integrity of each leaf node and provide identity tracing. The node uses PU_{RA} to encrypt the information such as its own fingerprint ID and number to obtain the secret value $heta_1$, and selects a specific parameter such as ID, encrypts the ID with the PU_{node} to obtain the secret value θ_2, and transmits θ_1 and θ_2 to the RA. The RA obtains the node fingerprint and number information by decryption, and then calculates $H1 = h(\theta_1)$, $H2 = h(\theta_2)$ and HA1 respectively and stores them in the Merkle data table, waiting for node authentication, and finally returns HA1 to the terminal node. Figure 2 shows the process of node key generation and registration.

In the identity authentication phase, the terminal node needs to perform identity authentication before communicating (see Figure 3). Taking terminal node A1 as an example, A1 initiates an authentication request to RMA, and calculates $\phi = E_{PU_{NODE}}(ID)$ and $E_{PU_{RA}}(\phi, HA1, T, r)$, and then $E_{PU_{RA}}(\phi, HA1, T, r)$ is sent to the RMA, where T is a timestamp to prevent replay attacks. The RMA signs the message and sends the result to the registration authority RA. The RA decrypts the message, obtains ϕ, and requests the identity hash values $HA1$ and $H1$ from the Merkle tree. If the calculation results for $H1$ and $H2'$ are the same as $HA1$, the authentication is successful. This authentication scheme guarantees the privacy of the user. The domain manager RM authentication process is similar and will not be described again.

4 Anonymous Scheme Based on Aggregate Signature

4.1 Anonymous Scheme

Due to the clear message burst device address, an attacker can obtain the user ID by anonymous analysis. This section is based on the CoinJoin idea [7], which further protects user node identity privacy by using a one-way aggregation signature algorithm. All domain managers in the system act as miners for transaction information verification, packaging and identity confusion, and the transaction model still uses the UTXO structure. The one-way aggregation signature includes 5 algorithms: domain manager key generation algorithm, signature algorithm, verification algorithm, aggregation algorithm, and aggregation verification algorithm. The length of aggregated signature is the same as the pre-aggregation independent signature. The aggregation algorithm only needs to obtain the separate signature message pair and public key that participate in the signature domain manager. As long as obtains the aggregate signature, the aggregate domain manager public key, and the message set, the signature validity can be verified.

Parameter Convention: Large prime number P, elliptic curve groups G and G_1, Generating element g of group G, Bilinear map $e_1 : G \times G \Rightarrow G_1$;

Key Generation Algorithm: The private key for the domain manager RMA is generated based on random numbers R, $X_i \overset{R}{\leftarrow} Z_p$, the public key is $PK_{RMA} = g^{x_u} \in G$, where the total number of domain managers is k.

Signature Algorithm: The signed message is $M_i \in \{0,1\}^*$, the hash function is $H_i = Hash(M_i) \in G$, and the signature is $J_i = H_i^{x_i} \in G$.

Verification Algorithm: Determine whether it is ture

$$e_1(PK = g^{x_i}, H_i) = e_1(g, J_i = H_i^{x_i}).$$

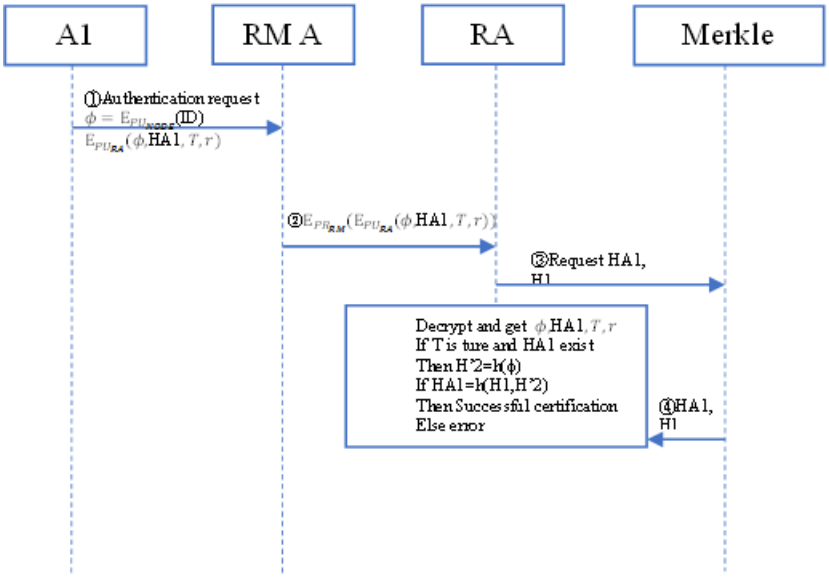


Figure 3: Node authentication process

Aggregation Algorithm: M_i requirements are different, the result of the aggregation is signature:

$$J = \prod_{i=1}^{k} J_i = \prod_{i=1}^{k} (H_i)^{x_i} = \prod_{i=1}^{k} (Hash(M_i))^{x_i}$$

Aggregation Verification Algorithm: Verify that the following formula is true:

$$\prod_{i=1}^{k} e(v_i = g^{x_i}, h_i) = e(g_1, J = \prod_{i=1}^{k} J_i = \prod_{i=1}^{k} h_i^{x_i})$$

The security of the above-mentioned aggregate signature scheme depends on the random oracle model. It is necessary to assume that the decision DDH problem is easy but the gap GDH is difficult to calculate the CDH problem and the original images of the Bilinear map are different groups. In addition, the uni-directionality of the aggregate signature scheme is reflected in the difficulty of independently extracting individual signatures from the aggregate signature, which is equivalent to the CDH problem. To ensure that the transaction information is different, a pseudo-random number d needs to be added for each output transaction. For a transaction output ciphertext with the same pseudo-random number, the transaction confirmation must be delayed until the next block confirmation. The miner forces a random arrangement for a number of transactions, including the input-free Coinjoin transaction (TXcoinbase) and the aggregation signature $J = \prod_{i=1}^{k} J_b$. The signature and transaction content within the block is:

$$\begin{aligned} J, TX &= (TX_1, TX_2, \cdots, TX_i, \cdots) \\ TX_i &= [TX_{coinbase}, TX_{ina,b}(1, TX_{outc,d}), PK_{RMA}]_i \end{aligned}$$

In order to reduce the space occupied by the secondary information in the block, and maximize the number of transactions in the block, the transaction output public key in the block only needs to include the payee's signature public key for the transaction ownership certificate.

4.2 Anonymous Scheme Comparison

The selective blending scheme has a bootstrap phase (Bootstrapping), and the obfuscation process is not mandatory. Although the XIM [1] bulletin board can be used to pair the users, the weak anonymous set users will reduce the privacy protection of the entire network, such as the Monroe coin using the ring signature scheme. This scheme and the [11] schemes force the embedding of the coin-coin mechanism to ensure the size of the anonymous set and resist analysis attacks. In addition, although [14] combined with homomorphic encryption and selective hybrids to achieve full anonymity, which does not resist analytical attacks [12]. Compared with other blockchain privacy protection schemes, this scheme achieves full anonymity and supports blockchain pruning. The constructed blockchain only retains the aggregate transaction signature, reducing the storage load. Table 1 gives a comparison of the performance with other schemes in this paper.

5 Consensus Based on Reputation Value

In order to meet the information interaction of each node in the IOT model proposed in this paper, it is very important to seek an efficient consensus mechanism. Bitcoin adopts the POW mechanism, which has the problem of

Table 1: Anonymity comparison

Literature	Privacy	Bootstrapping	Anti-Analysis	Pruning	Efficiency
[11]	Y	/	Y	N	M
[14]	Y	Y	N	Y	M
[4]	Y	N	N	N	Variable
[16]	N	/	N	N	L (n^2 ciphertext)
Ours	Y	Y	Y	Y	M (n ciphertext)

huge computational power. Based on the DPOS mechanism, Ethereum are voted by all nodes and generates blocks. The transaction fee is used to motivate the nodes to be honest and participate in verification. However, there are still shortcomings such as low throughput and transaction fees. The solution proposed in this paper is not an electronic money plan, so the transaction fee incentive mechanism is excluded. In this solution, all regional manager forms a coalition-chain, and each regional manager has business crossover and interest bundling, so the credibility is high, and the billing right can be obtained based on the reputation evaluation method, so the block consistency is maintained. If the accounting period is 1 minute, then in a billing cycle, the regional manager with the highest evaluation value of the previous block obtains the billing right, and the reputation value is calculated from the past reputation value and the current period credibility value.

Assuming the registration of each domain manager, the same initial reputation value C_0 is obtained. Each time the regional manager trades on behalf of the terminal node, it will get the evaluation of the terminal node, and the evaluation result is used for the regional manager reputation value calculation. If the evaluation value is approved, the evaluation result C_{app} is a positive value, and if the evaluation value is negative, the evaluation result is that C_{den} is a negative value. The terminal node signs the result with its own private key and adds the timestamp T to send the ciphertext $E_{PR_{NODE}}(C_{app}, T)$ to the area manager. The zone manager confuses ciphertext, transaction records and identity and broadcasts it to the entire network. The terminal node signs the evaluation with the private key so that the zone manager cannot forge the evaluation. The added timestamp prevents the zone manager from using the expired evaluation to defraud the accounting rights.

When a billing cycle arrives, the zone manager decrypts all the evaluations D in the cycle and calculates the total evaluation obtained in this cycle according to Equation (1).

$$D = \frac{1}{n}(k \times C_{app} + (n-k) \cdot C_{den}),\ k \in \{0, 1, \cdots, n\}. \quad (1)$$

Where n is the number of transactions, and k is the number of times the evaluation result is approved. This method of calculating the average value ensures that the reputation value is not affected by the number of terminals in the area and is applicable to domain managers of different cardinalities. Let the reputation value of the regional manager in the i^{th} accounting period be C_i, then the reputation value of the t^{th} cycle can be calculated by Equation (2).

$$C_t = \sum_{i=0}^{t-1} C_i e^{-(t-i)} + D_i. \quad (2)$$

The first parameter is the influence value of the previous reputation value on the current reputation value. According to the law of real life, the earlier the event, the smaller the impact on the current event. Therefore, in order to reduce the impact of past behavior on the current reputation value, the algorithm introduces a decrement factor, so that the weight of the past reputation value decreases with time. The influence of the past reputation value on the current reputation value is calculated by the following formula.

$$\sum_{i=0}^{t-1} C_i e^{-(t-i)}. \quad (3)$$

The zone manager broadcasts its current reputation value in the interconnected domain federation-chain and verifies the zone manager that gets the highest reputation value. After the verification is passed, the zone manager with the highest reputation value obtains the accounting right of the current block, and completes the generation of the block in the current cycle. In addition, for the zone manager with the same evaluation value in the cycle, the first-come-first-served strategy (FCFS) is used to determine the accounting rights. The last regional manager of each period's reputation value needs to compensate all the terminal nodes in the area until the registration authority cancels the management right of the area manager, and the punishment is used as an incentive mechanism to encourage the regional managers to participate in accounting and verification honestly.

6 Efficiency and Privacy Analysis

The IOT system structure based on the alliance chain enables smart terminals to have more initiative. Each message is recorded in the blockchain system. The data is

traceable and cannot be tampered with, which improves the security and reliability of the data. The biggest contribution of this solution is to achieve strong user identity privacy and improve consensus efficiency while ensuring nearly zero growth in key storage overhead.

6.1 Efficiency Analysis

According to the development of the current hardware system, the selection of the cryptographic security parameters needs to ensure that the modulus based on the large integer decomposition scheme is 256B, and the security parameter based on the elliptic curve scheme is 32B.Therefore, the length of the public key contained in the transaction on the elliptic curve chain of the scheme signature is $PK_{RMA} = g^{x_i} = 33B$. Because the scheme adopts the aggregate signature scheme, the signatures of all transactions in the block are aggregated into one signature, which reduces the size of the transactions in the block. Therefore, this section quantitatively evaluates the number of transactions that can be accommodated in a single block in this document and in each reference.

For the original Bitcoin blockchain system, the average size of the block in the past year was 644.2 KB, and the number of transactions included was 1682KB [2]. After deducting the block header and related information about 100B, it can be calculated that each transaction size is about 392B. Among them, the data that is not related to input and output at the beginning and end of the transaction is 8B. Regardless of the P2PKH case and the transaction input and output counter size, each input contains 32B previous transaction hash value, 4B index, 64B ECDSA signature and 4B serial number, and each output contains 33B ECDSA public key and 8B amount. Among them, the data that is not related to input and output at the beginning and end of the transaction is 8B.Regardless of the P2PKH case and the transaction input and output counter size, each input contains 32B previous transaction hash value, 4B index, 64B ECDSA signature and 4B serial number, and each output contains 33B ECDSA public key and 8B amount. Therefore, if the input and output are considered equal, there are about 2.649 input and output on average; Consider the limit case for single input, 6.832 output or single output, 3.299 input.

According to the above transaction input and output data, the number of transactions in each scheme block is calculated at the limit input and output and the equal input and output. The results are shown in Table 2. Analysis of the data in Table 2 can be consistent with the key length of the original BTC scheme, and the number of transactions per unit time is reduced, but the key storage space is saved.

6.2 Privacy Security Analysis

In terms of user identity privacy, first, the registration information of the user equipment is encrypted by the public key of the registration authority, and only the registration authority can decrypt it with its own private key, the external attacker cannot obtain the user ID of the terminal device. The authentication information of the terminal node in the communication process is different from the registration information. The terminal encrypts the single element in the registration information with its own public key. Even if it is intercepted by the attacker, the device fingerprint and user information cannot be accurately obtained, which protects the device security and user identity. According to the Merkle tree principle, the registration authority compares the registration information and the authentication information of the terminal, and neither party can change the device registration information to ensure that the identity cannot be modified. Table 3 gives a comparison of attack performance. The "Y" in the table indicates that it can defend against such attacks, and the "N" indicates that it cannot defend against such attacks.

In the block generation phase, the zone manager broadcasts each piece of information in the federated chain, and the current cycle reputation value is verified by the highest domain manager, so that the message and transaction data cannot be tampered with and traceability is provided. The scheme adopts the reputation value and the FCFS consensus mechanism, which avoids the defects of node mining energy consumption and improves the speed of the block. The domain manager reputation value is determined by the forward reputation value and the terminal node participating in the communication in the current cycle. Other nodes can also verify the current reputation value of each node, increase the difficulty of forging blocks, The increased timestamp is used to resist the replay attack of malicious nodes. The security risks of micro-transactions and data transmission in IOT have been resolved.

7 Conclusions

This paper proposes a lightweight and efficient anonymous authentication scheme based on the Blockchain. A BC-IOT network model is proposed, which realizes the double-chain structure of the centralized identity authentication chain and the decentralized message chain. For identity authentication, based on the Merkle tree, the zero knowledge proof of identity is realized. Thirdly, the proposed aggregated signature privacy protection scheme protects the identity anonymity of message exchange between domains. Finally, aiming at the efficiency problem, a reputation evaluation and FCFS strategy are proposed to solve the accounting rights and message consistency. The comparison of security and efficiency analysis and related literatures shows that the scheme guarantees zero growth of key storage overhead, realizes strong user identity privacy and improves consensus efficiency.

Table 2: Number of transactions in the block

Literatures	PK Length/B	TXs Number In=Out=2.649	TXs Number In=1,Out=6.832	TXs Number In=3.299,Out=1
BTC	33	1682	1682	1682
[14]	66	1208	837	1465
[16]	545	207	87	457
Ours	33	687	319	1260

Table 3: Security comparison

Literatures	Malicious Node Attack	Registration Authority Attack	Middleman Attack	ThirdParty Attack	Analytical Attack
[5]	N	N	Y	N	N
[6]	Y	N	Y	Y	N
[9]	Y	N	Y	Y	N
[15]	Y	N	N	Y	N
Ours	Y	Y	Y	Y	Y

Acknowledgments

This work is funded by the Shaanxi Provincial Department of Education Scientific Research Project (19JK0040) and Science and Technology Plan Project of Shaanxi Province NO.2020GY-041. The authors would like to thank the anonymous reviewers and the editors for their suggestions.

References

[1] G. Bissias, A. P. Ozisik, B. N. Levine, *et al.*, "Sybil-resistant mixing for bitcoin," in *Proceedings of the 13th Workshop on Privacy in the Electronic Society (WPES'14)*, pp. 149–158, 2014.

[2] Blockchain Ltd., *Blockchain Charts*, 2018. (`https://www.blockchain.com/en/charts`)

[3] G. S. Dong, Y. X. Chen, Z. X. Zhang, *et al.*, "Research on identity management authentication based on blockchain," *Computer Science*, vol. 11, no. 45, pp. 59–66, 2018.

[4] E. Heilman, F. Baldimtsi, S. Goldberg, "Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions," in *International Conference on Financial Cryptography and Data Security*, 2016.

[5] S. Lee, J. Bong, S. Shin, *et al.*, "A security mechanism of Smart Grid AMI network through smart device mutual authentication," in *International Conference on Information Networking (ICOIN'14)*, IEEE, 2014.

[6] H. Li, R. Lu, L. Zhou, *et al.*, "An efficient merkle-tree-based authentication scheme for smart grid," *IEEE Systems Journal*, vol. 2, no. 8, pp. 655–663, 2014.

[7] X. L. Li, H. Y. Wang, J. T. Gao, W. Li, "Anonymous revocation scheme for bitcoin confusion," *Journal of Electronics and Information Technology*, vol. 8, no. 41, pp. 1815–1822, 2019.

[8] I. C. Lin, T. C. Liao, "A survey of blockchain security issues and challenges," *International Journal of Network Security*, vol. 19, no. 5, pp. 653–659, 2017.

[9] Y. Liu, C. Cheng, T. Gu, *et al.*, "A lightweight authenticated communication scheme for smart grid," *IEEE Sensors Journal*, vol. 3, no. 16, pp. 836–842, 2016.

[10] X. T. Ma, W. P. Ma, X. X. Li, "A cross domain authentication scheme based on blockchain technology," *Acta Electronica Sinica*, vol. 11, no. 46, pp. 13–21, 2018.

[11] I. Miers, C. Garman, M. Green, *et al.*, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *IEEE Symposium on Security and Privacy*, 2013.

[12] M. Möser, K. Soska, E. Heilman, *et al.*, "An Empirical analysis of traceability in the monero blockchain," *Proceedings on Privacy Enhancing Technologies*, vol. 3, pp. 143–163, 2018.

[13] D. Ron, A. Shamir, "Quantitate analysis of the full bitcoin transaction graph," in *Proceedings of the 17th International Conference on Financial Cryptography and Data Security*, pp. 34–51, 2013.

[14] T. Ruffing, P. Moreno-Sanchez, "ValueShuffle: Mixing confidential transactions for comprehensive transaction privacy in bitcoin," in *Financial Cryptography and Data Security*, pp. 133–154, 2017.

[15] N. Saxena, B. J. Choi, "Integrated distributed authentication protocol for smart grid communications," *IEEE Systems Journal*, vol. 12, no. 2, pp. 2545–2556, 2018.

[16] Q. Wang, B. Qin, J.K. Hu, *et al.*, "Preserving transaction privacy in Bitcoin," *Future Generation Computer Systems*, vol. 8, no. 46, 2017.

[17] W. Y. Xu, L. Wu, Y. X. Yan, "Privacy-preserving scheme of electronic health records based on blockchain and homomorphic encryption," *Journal of Computer Research and Development*, vol. 10, no. 55, pp. 141–151, 2018.

[18] J. Zhang, W. Z. Gao, Y. C. Zhang, *et al.*, "Blockchain based intelligent distributed electrical energy systems: Needs, concepts, approaches and vision," *ACTA Automatica Sinica*, vol. 9, no. 4, pp. 1544–1554, 2017.

[19] Z. C. Zhang, L. X. Li, Z. H. Li, *et al.*, "Efficient cross-domain authentication scheme based on blockchain technology," *Journal of Computer Applications*, vol. 2, no. 38, pp. 316–320, 2018.

Biography

Ye Lu is a lecturer and Ph. D. supervisor at the Computer College of Baoji University of Arts and Sciences, China. His main research interests include IOT, network protocol security and Blockchain, etc.

A k-Anonymous Location Privacy Protection Method of Polygon Based on Density Distribution

Yong-Bing Zhang[1,2], Qiu-Yu Zhang[1], Yan Yan[1], Yi-Long Jiang[2], and Mo-Yi Zhang[1]
(Corresponding author: Qiu-Yu Zhang)

School of Computer and Communication, Lanzhou University of Technology[1]
No. 287, Lan-Gong-Ping Road, Lanzhou 730050, China
(Email: zhangqylz@163.com)
Gansu Institute of Mechanical & Electrical Engineering[2]
No. 107, Chi-Yu Road, Tianshui, Gansu 741001, China
(Received July 26, 2019; Revised and Accepted Dec. 28, 2019; First Online Feb. 3, 2020)

Abstract

In order to solve the problem of out-off-balance caused by accuracy of location information between privacy protection security and query service quality, considering basic information comprehensively such as the environment and geographical features and so on, and adopting k-anonymous privacy protection mechanism, we present a k-anonymous location privacy protection method of polygon based on density distribution. Firstly, a k-anonymous irregular polygon region is structured in whole area. Then, according to the preset anonymous region and density threshold, the better effects of anonymous are obtained by expanding the region or adding the random dummy locations. Experimental results show that the proposed method improves the efficiency of anonymous and query accuracy. The balance between privacy protection security and query quality is achieved.

Keywords: Anonymous Region; Density Distribution; Irregular Polygon; k-*Anonymous; Location-Based Service (LBS); Location Privacy Protection*

1 Introduction

With the development of mobile location technology and wireless communication technology, more and more mobile devices in the market have GPS precise positioning function, which makes Location-Based Service (LBS) become one of the most promising services to mobile users [11]. However, when LBS services provide convenience and great benefits to the society, its problem of sensitive information leakage has attached more attentions by many people. Because users' location is shared among different Location Service Providers (LSPs), untrustworthy third parties can easily steal users' privacy via analyzing and comparing these location information [17]. For example, through capturing recent users' trace, some location information can be analyzed by adversary such as home addresses, workplaces, and health conditions, etc. Therefore, it is necessary to ensure the safety of users' location privacy.

In order to prevent the leakage of location privacy information, many different methods are proposed by experts and scholars, including fuzzy method, encryption method and strategy-based method. Because of the better reliability, the fuzzy method is the most commonly used in the field of location privacy protection, which is mainly realized by means of spatial anonymity or dummy location, and needs the help of Fully-Trusted Third Party (TTP) [22]. When there is a location service requirement, the mobile user first sends the query request to the TTP, a k-anonymous region containing the user's location is generated by the TTP and then it will be sent to the LBS server for query. In the existing methods, the anonymous region is constructed by regular geometric shapes. However, the actual terrain is not a regular geometry. Therefore, the area of invalid region is increased greatly, which not only consumes more time, but also reduces the accuracy of the query result.

In the k-anonymous location privacy protection, in order to improve query efficiency and query accuracy, a k-anonymous location privacy protection method of polygon based on density distribution is proposed. In this paper, we give full consideration to the geographical features of the current region and the density distribution. Firstly, a k-anonymous irregular polygon region is structured in whole area. Then, according to the density threshold, the location privacy protection is implemented by combining spatial anonymity and dummy location. The proposed method improves the query accuracy and the query service quality.

Our main contributions can be summarized as follows:

1) According to the characteristics of different geographic shapes, a polygon anonymous region construction method is proposed, which improves the accuracy of query result.

2) A fast polygon generation algorithm is applied to construct anonymous region, which improves the query efficiency.

3) According to neighbor users' density distribution, a location privacy protection method combining spatial anonymity and dummy location is proposed, which improves the effectiveness of location privacy protection.

The remaining part of this paper is organized as follows. Section 2 reviews related work of location privacy protection. Section 3 gives system model of this paper. Section 4 describes two algorithms and analysis. Section 5 gives the experimental results and performance analysis as compared with other related methods. Finally, we conclude our paper in Section 6.

2 Related Work

The location privacy protection methods are divided into two main categories [8] according to the system architecture, including distributed structure [9] based on Point to Point (P2P) and central server structure based on TTP [16]. In the distributed structure, location privacy protection is accomplished through collaboration between users. Chow *et al.* [4] proposed a P2P-based spatial anonymity method. In this method, the k-anonymous privacy protection based on distributed architecture is achieved by using location information of neighbors' node, but the security of the neighbors' node is ignored. The P2P-based scheme is simple and flexible, but which greatly increases various overhead of the smart phone. Furthermore, the users' locations are mobile rather than static. In centralized structure based on TTP, a method of location privacy protection based on TTP is proposed by Xie *et al.* [18]. This structure model has a good effect of privacy protection, which is currently the primary choice for location privacy protection. Li *et al.* [13] proposed a location privacy protection scheme based on efficient information cache, which reduces the number of times that the users' access to TTP. In this method, the query efficiency is improved, and the probability of information leakage is reduced, but the burden of the mobile client is increased.

In addition, Cheng *et al.* [3] put forward an independent structure model, and users' location privacy is protected according to their own abilities and knowledge. The structure of this method is simple, which is easy to merge with other structures, but it requires high performance for mobile clients. Li *et al.* [12] put forward a multi-server architecture, users can be divided into different subsets according to the security requirements, and each location server can only obtain partial subset. The concealment of location is improved in this method, but it is mainly suitable for the social network. Li *et al.* [14] put forward a location privacy protection method based on privacy information retrieval, and its location privacy protection is implemented by using retrieval and encryption. The location privacy is well protected in this method, but the overhead of communication and hardware is increased, and the query quality is reduced. With the maturity and popularity of cloud service technology, Yuji *et al.* [24] proposed a location privacy protection method based on searchable encryption. By accessing to the cloud server in the encrypted state, the security of location data and query records is guaranteed, but query efficiency and query accuracy need to be improved further.

In recent research, k-anonymous [25] is still the mainstream method of location privacy protection, which was born in the relational database, and its key attribute is dealt with using generalization and fuzzy technology. So none of the records can be distinguished from other k-1 records, and the location anonymity is realized. The method of k-anonymity location privacy protection is mainly divided into spatial region anonymity and dummy anonymity. Gruteser *et al.* [7] proposed a k-anonymity location privacy protection method, and its location privacy is protected by constructing k-anonymous region. The region must meet two conditions: 1) The area of the region reaches a certain value; 2) There are k users in the region. Due to the above two limitations, the effect of location privacy protection is improved, but all users must have the same location anonymity requirement.

Gedik *et al.* [6] put forward the location k-anonymity method to meet the user's personalized privacy requirements. The user can define the k value and anonymous level to realize personalized anonymity, but the actual effect is poor when the k value is too large. Lu *et al.* [15] have designed the k-anonymous method to add dummy locations by using circular or rectangular regions, but too many randomized locations are easily recognized by adversaries. Yin *et al.* [23] proposed an improved k-anonymity method. By setting the range of k parameters, the combination of pseudonyms and anonymity was used to improve the privacy protection effect, but the density of the anonymous region was not considered. Dewri *et al.* [5] adopts dummy location instead of user's current location to send query requests, but the accuracy of query results is low, and the extra communication cost of LBS server is increased. Jia *et al.* [10] put forward a method of combining k-anonymity and encryption technology, double protection is achieved via encrypted user and TTP, but the communication cost was relatively large.

In the research of k-anonymous region construction, Bamba *et al.* [1] put forward the method of Grid partition. In this method, there were two algorithms for Top-Down Grid Cloaking and Bottom-Up Grid, which were available for different privacy requirements. Xu *et al.* [20]

proved that the size of k-anonymous region has great influence on the accuracy of query results, which provided guidance for the research of division of anonymous regions. On this basis, Zhao *et al.* [26] proposed a method of circle anonymous region division, and Yang *et al.* [21] proposed an augmented reality rectangle partition anonymous method. These methods divided the whole area into a combination of some geometric shapes to achieve privacy protection, and further reduced the area of anonymous regions. In order to make the number of users to meet the privacy protection requirements, it is usually realized by enlarging or reconstructing the region. But in k-anonymous location privacy protection method, k-density and area parameters need to be fully considered, and the best anonymous region is generated according to the terrain characteristics.

The above methods solve the problems of LBS privacy protection from different angles, and different ways to construct anonymous regions are proposed. But in practical applications, the shapes of these anonymous regions are often influenced by the terrain such as desert, high mountains and river. Anonymous regions are not regular geometric shapes, such as circles, rectangles, etc. These methods increased the area of invalid areas, such as circles, rectangles, grids and other regular geometric shapes, and increased the computing cost of the server. Moreover, adversaries can easily analyze and identify the users'location based on invalid region and terrain features. Then, Xie *et al.* [19] proposed a k-anonymity algorithm of irregular polygon. By constructing an irregular polygonal anonymous region, the area of the invalid region is reduced. However, it takes much time to generate anonymous region of polygon, and query quality is reduced. Moreover, this method only considers the Euclidean space distance, but not the users' density distribution and the diversity of the environment.

Therefore, in the k-anonymous location privacy protection method, it is necessary to fully consider the users' density distribution and the terrain features. Based on the above analysis, a k-anonymous location privacy protection method of polygon based on density distribution is proposed. According to the density distribution of users, the method combining k-anonymity and dummy location is adopted to further improve the privacy protection effect and query quality.

3 System Model

3.1 System Structure

In LBS service, the most widely used is to query the nearest interest point. If users want to know the nearest shopping mall, hotel, gas station, hospital, etc., they need to send their current location to the LBS server. However, LBS server is not reliable, and users' location information will be leaked to third parties intentionally or unintentionally, which will lead to privacy leakage. In the TTP-based structure, when a user needs to obtain location service, who do not send their location to LBS server directly, but first send query request to TTP. The query request will be sent to LBS server after anonymous processing by TTP. The system structure model is shown in Figure 1.

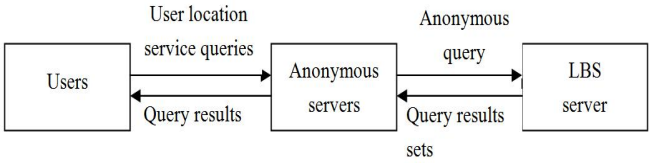


Figure 1: System structure model

In practical applications, the users hope that anonymous region can best match the actual terrain, such as street trend, bridge shape, shopping mall shape, etc., as shown in Figure 2, which can better meet users' privacy requirements and improves the accuracy of query result. In this paper, according to the geographical features of the user's location, the anonymous region of irregular polygon is constructed, as shown in Figure 3. Adopting the polygon boundary fast construction algorithm, the polygon anonymous region is generated quickly, which improves efficiency of anonymous region generation. Based on the density of users, the strategy of spatial region anonymity and dummy location is adopted, and the effectiveness of location privacy protection is further improved.

Figure 2: Effect of terrain on structuring anonymous region

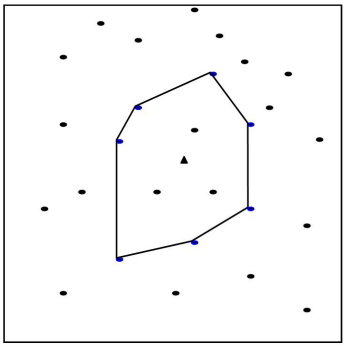


Figure 3: Polygon regional construction block diagram

3.2 Definition

Definition 1. *Let Rs represents an irregular polygonal anonymous region. Rs can be defined as* $Rs = \{U_{id}, (x_u, y_u, k\}$*, Among them,* U_{id} *represents the user's identity information; Let* (x_u, y_u) *represents the user's location coordinates:* x_u *represents the longitude of the location,* y_u *represents the latitude of the location; let k represents the anonymous parameter specified by the user.*

Definition 2. *Let* ρ *represents the density of users in the Rs region, and set threshold parameters* ρ_{max} *and* ρ_{min} *for it. Among them,* ρ_{max} *represents the maximum density, and* ρ_{min} *represents the minimum density..*

Definition 3. *Let* $S(Rs)$ *represents the area of the anonymous region. Let* S_{min} *represents the minimum area that users can accept, and* S_{max} *represents the maximum area that users can accept.*

Definition 4. *Let* $N(Rs)$ *represents the number of users in the Rs region. It can achieve the best anonymous effect when* $N(Rs) = k$*.* $N(Rs)$ *is an important parameter index, determining the degree of anonymity and the size of* $S(Rs)$ *in the system.*

4 Algorithmic Description

In this paper, a k-anonymous location privacy protection method of polygon based on density distribution is proposed. When a user queries the location, a polygon region including k locations is generated in the current area, and the k-density in the polygon region is calculated. If the k-density meets the set threshold, the polygon region with the geometric center of the polygon area as the anchor point is sent to LBS server for query. If the density is larger than the maximum threshold, the area of the polygon will be further expanded, and then the polygon region with the geometric center of the polygon area as the anchor point is sent to LBS server for query. If the density is less than the minimum threshold, a number of dummy locations are added in the polygon region, and then k locations (including dummy locations and neighbor users' locations) are sent to LBS for query.

The proposed method is realized by the following two algorithms: Algorithm 1 quickly generates an irregular polygon k anonymous region according to the coordinates of the query user and the neighbors. Algorithm 2 calculates the density of the users in the anonymous region, and adopts the corresponding anonymous strategy according to the density parameter threshold. The two algorithms are described as follows.

4.1 Algorithm 1

The principle is realized by using double-end queue: let D is a double-end queue, and all the operations of D are described in terms of that to enter the tail of queue, to go out of the tail of queue, to enter the head of queue, to go out of the head of queue.

Algorithm 1: Constructing a k-anonymous region of polygon.

Input: User's coordinates (x_u, y_u), requirement parameter k.

Output: Generate a polygonal anonymous region containing k locations.

Step 1: $n = 1$, $(x_u, y_u) = 0$.

Step 2: Set a location position near the user, take this position as the center, gradually scan the k locations, and record the coordinates of each point with (x_i, y_i).

Step 3: Select the point with minimum x-coordinate from the coordinates (x_i, y_i). If there are many points that satisfy this condition, then the point with minimum y-coordinate is selected, and the point is recorded as P_0.

Step 4: Select one direction against clockwise direction. P_x represents an arbitrary point, calculate the angle between $\overrightarrow{P_0P_x}$ and the negative direction of y axis. Here $\overrightarrow{P_0P_x}$ is the vector between P_0 and P_x.

Step 5: According to the angle calculated from Step 4, sort all the points from small to large, then get an ordered set $C = P_0, P_1, P_2, \cdots, P_{n-1}$.

Step 6: Remember at a certain time, the state of double-end queue D is $C = P_t, P_{t-1}, \cdots, P_0, \cdots, P_{b-1}, P_b$, traversing every point in the C:

1) If the point is P_0, then P_0 enters the tail of the queue firstly; if the point is P_1, then P_1 enters the tail of the queue; if the point is P_2, then P_2 enters the tail of the queue, and also the head of the queue.

2) Suppose that the current point P_i is traversed.

(1) If $P_{b-1}P_bP_i$ can keep the left-turn characteristics, then continue, otherwise P_b goes out of the tail of the queue; so repeat until $P_{b-m-1}P_{b-m}P_i$ can meet the left-turn characteristic, and P_i enters the tail of the queue.

(2) If $P_iP_tP_{t-1}$ can keep the left-turn characteristic, then continue, otherwise P_t goes out of the head of the queue, so repeat until $P_iP_{t-n}P_{t-n-1}$ can meet left-turn characteristic, and P_i enters the head of the queue.

Step 7: Returns the double-ended queue.

Step 8: The polygon k-anonymous region Rs is constructed.

4.2 Algorithm 2

Algorithm 2: Generating a k-anonymous result set.

Input: The k-anonymous region Rs.

Output: A k-anonymous result set.

Step 1: Set the maximum (ρ_{max}) and minimum (ρ_{min}) of the k-density.

Step 2: Take all vertices of the polygon from the double-end queue.

Step 3: Calculate the area $S(Rs)$ of the polygon region.

Step 4: Calculate S_{max} and S_{min} according to (ρ_{max}) and (ρ_{min}) .

Step 5: Judge:

1) If $S(Rs)<S_{min}$, then $k \leftarrow k+1$, execute Algorithms 1 and 2 in turn, then Step 6;
2) If $S_{min}<S(Rs)<S_{max}$, then Step 6;
3) If $S(Rs)>S_{max}$, execute Algorithms 1 and 2 in turn, then Step 7.

Step 6: Calculate the coordinate of the center location, then take the geometric center as the anchor point, and send the k-anonymous region of polygon to the LBS server for query.

Step 7: Add $[k-N(Rs)]$ dummy locations to the region randomly, and then send k locations including $N(Rs)$ users' location and $[k-N(Rs)]$ dummy locations to the LBS server for query.

4.3 Algorithm 1 Description

N location points are obtained by scanning around the query user, one of its with the minimum x-coordinate is picked. If a point with the minimum x-coordinate is not unique, a point with the minimum y-coordinate is picked. This point is defined as $P_0(x_0, y_0)$, and clockwise is selected as the default direction. The angle is calculated between $\overrightarrow{P_0P_x}$ and the negative direction of y axis, here $\overrightarrow{P_0P_x}$ is the vector between P_0 and P_x. By sorting all the points from small to large, an ordered set $C = P_0, P_1, P_2, \cdots, P_{n-1}$ is obtained. According to the following methods, all the outermost points in the set are found.

Assuming that P_i, P_j, P_k are three consecutive points on the boundary of the region (polygon vertex), its must maintain a trend of left-turn, that is $\overrightarrow{P_iP_j} \times \overrightarrow{P_jP_k} > 0$. If the three points are represented as (x_i, y_i), (x_j, y_j), (x_k, y_k), there are: $\overrightarrow{P_iP_j} = (x_j - x_i, y_j - y_i)$, $\overrightarrow{P_jP_k} = (x_k - x_j, y_k - y_j)$.

According to Algorithm 1, a k-anonymous region of polygon containing k locations is generated, as shown in Figure 4. The solid triangle symbol represents the current location of the user, and an irregular polygonal anonymous region which consists of 16 location positions is constructed.

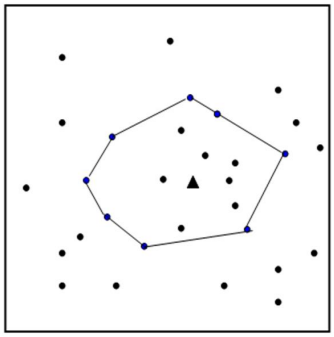


Figure 4: Block diagram of polygon region generation

4.4 Algorithm 2 Description

According to Algorithm 1, the coordinates of all vertices of convex polygon are obtained.

Suppose the n vertices on a convex polygon are ordered counterclockwise as $P_1(x_1, y_1)$, $P_2(x_2, y_2)$, $\cdots$, $P_n(x_n, y_n)$, then the area of the polygon is:

$$S_n = \frac{1}{2}\sum_{i=1}^{n-1}(x_i y_{i+1} - x_{i+1} y_i) + \frac{1}{2}(x_n y_1 - x_1 y_n) \quad (1)$$

The area $S(Rs)$ of the polygon k-anonymous region is calculated by Equation (1). The maximum area (S_{max}) is calculated by $S_{max} = k/\rho_{min}$, and the minimum area (S_{min}) is calculated by $S_{min} = k/\rho_{max}$.

Then judge by (S_{max}) and (S_{min}):

1) If $S(Rs)<S_{min}$, the anonymous region needs to be further expanded, and then the method of spatial anonymity is used to protect location privacy.
2) If $S_{min}<S(Rs)<S_{max}$, the anonymous region meets the user's requirements, and then the method of spatial anonymity is used to protect location privacy.
3) If $S(Rs)>Smax$, the method of spatial anonymity is invalid, the location privacy protection is implemented by combining spatial anonymity and dummy locations.

4.5 Algorithm Analysis

In this paper, an irregular polygon k-anonymous region including the user's current location is quickly constructed. And then the area of the polygon anonymous region is calculated. The size of the polygon region not only affects effect of the location privacy protection, but also affects the quality of the location service. Therefore, the area threshold needs to be set, so that the size of the anonymous region is kept in a suitable range. The influence of the $S(Rs)$ on the system anonymity is as follows:

when $S(Rs)<S_{min}$, the anonymous region is too small and the range of the region is close to the exact location of the user. In this case, an adversary is very easy to inference the location of the user; when $S(Rs) > S_{max}$, the anonymous region is too large, which reduces the accuracy of query results and consumes too much resources. Therefore, in the construction of anonymous regions, S_{max} and S_{min} need to be set beforehand.

In the anonymous region, it is known from $\rho = N(Rs)/S(Rs)$ that ρ is proportional to $S(Rs)$. Therefore, the density threshold is determined, and the area threshold is determined accordingly, that is $S_{max} = k/\rho_{min}$, $S_{min} = k/\rho_{max}$. In the k-anonymous region, when the k-density is too large, it indicates that the current location is in densely populated region such as schools, hospitals, stations, churches, etc. In this case, although the k value meets the anonymity requirement, the adversary can easily obtain the user's exact location. When the k-density is too small, it indicates that the current location is in a region where few people are in that such as desert, lake, mountain, etc. In this case, the spatial anonymity method is invalid. Therefore, the area threshold of anonymous region is determined by density, and different anonymity strategies are adopted according to area threshold, which can better improve the anonymity effect.

In the anonymity processing, there are three cases according to the area threshold:

1) $S(Rs)<S_{min}$;

2) $S_{min}<S(Rs)<S_{max}$;

3) $S(Rs)>S_{max}$.

In Cases 1 and 2, spatial anonymity is used to protect location privacy. At the same time, in order to improve the accuracy of query, the central node is used as the anchor point for query. When the query result set is returned, the user can calculate the exact query result according to the distance between the current location and anchor. The central node in this algorithm is represented by $O(x_0, y_0)$, its coordinate is calculated by Equation (2). The distance between the user's current location and anchor is calculated by Equation (3), which can be used as the measure of the accuracy of query result.

$$\begin{cases} x_0 = \frac{x_1+x_2+\cdots+x_n}{n} \\ y_0 = \frac{y_1+y_2+\cdots+y_n}{n} \end{cases} \tag{2}$$

$$d = \sqrt{(x_u - x_0)^2 + (y_u - y_0)^2} \tag{3}$$

In Case 3, the method of spatial anonymity is invalid, the location privacy protection is implemented by combining spatial anonymity and dummy locations, which effectively remedies the shortcoming of spatial anonymity method. Moreover, in the selection of dummy locations, the queried neighbor users are regarded as part of the dummy locations, which further improves the indistinguishability between dummy locations and the current location.

5 Experimental Results and Analysis

In this paper, a network-based mobile node generator [2] developed by Thomas Brinkhoff, which is used to generate 1000 data nodes distributed in the whole area through a real map. The hardware environment of the experiment is as follows: 3.2 GHz Intel Core i5 processor with memory size of 4 GB. The operating system is Windows 7. The proposed algorithm is implemented by Eclipse development platform and Java programming language. Table 1 is configured for the default parameters of the experiment.

Table 1: Experimental default parameter configuration

Parameter	Value
k	[0, 100]
ρ_{min}	0.002
ρ_{max}	0.02
Number of users	[0, 1000]
Space range (km^2)	0.8×0.8

5.1 Comparison of Anonymous Time

Firstly, efficiency of the proposed method is verified by experiments. In Figure 5, we compare the anonymous region generation time with the polygon method [19] and the proposed method. As shown in Figure 5, with the increase of k, the anonymous region generation time of both methods is increasing, and its growth trends are roughly the same. As can be seen from Figure 5, the polygon partition method takes much more time than the proposed method. From the experimental result we can see that the proposed method has better efficiency.

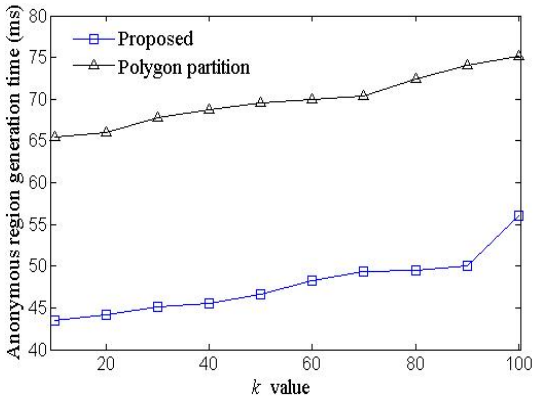


Figure 5: Average generation time of dummy

The result in Figure 5 is the best way. However, in the process of anonymous region generation, when the k value is insufficient, both methods need to repeat the algorithm several times. In addition, the proposed method

needs to calculate the area and density of the anonymous region, and takes different anonymity measures according to the density threshold. When the algorithm is executed many times, the time taken for both methods is shown in Figure 6 and Figure 7.

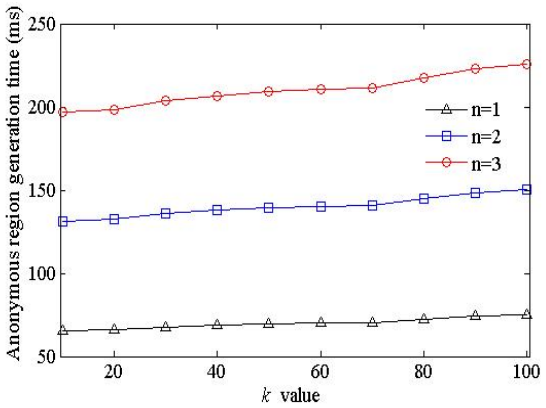


Figure 6: Average generation time of dummy

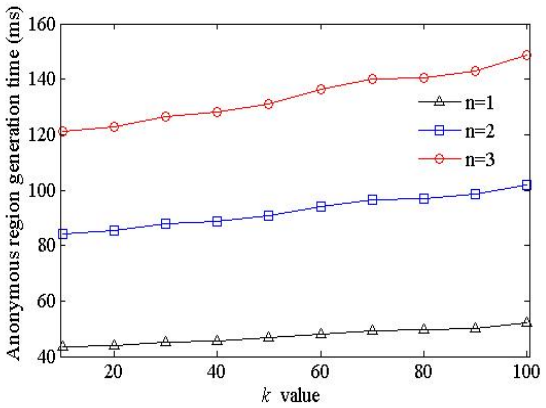


Figure 7: Average generation time of dummy

As can be seen from Figure 6 and Figure 7, when the first round of execution fails to meet the requirements, the second round and the third round will be executed. In contrast, the more the number of execution rounds, the greater the time gap between the two methods, the more obvious the efficiency advantage of the proposed.

5.2 Comparison of Anonymous Area

In the same environment, we compare the area of the anonymous with the grid partition method [1], the circular partition method [26], the rectangle partition method [21], the polygon partition method [19] and the proposed method, as shown in Figure 8.

As we can see from Figure 8, the area of five anonymous region construction methods increases with the increase of k, but the growth rates vary. This is determined by the geometric shape of the above methods. When k is the same, the area of the two polygon methods is the smallest.

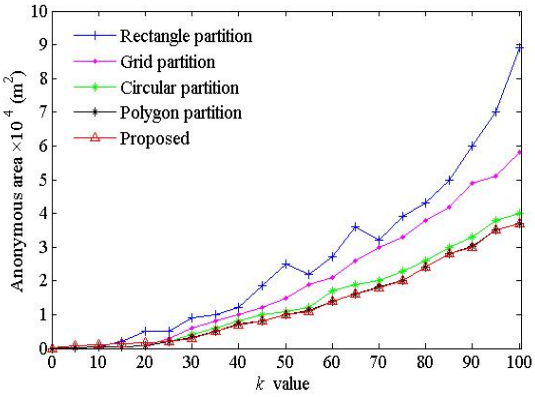
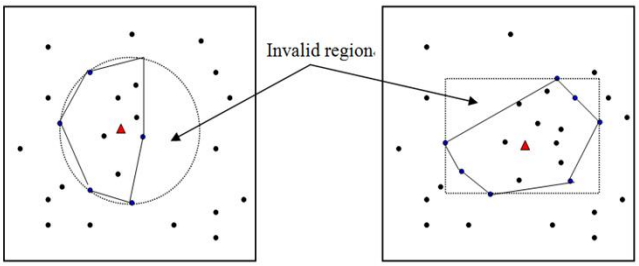


Figure 8: The area of several anonymous regional division methods

As we can see from Figure 8, when k<30, the area of the proposed method is slightly larger than that of the polygon partition method; When k>30, the area growth trend of the two methods is identical. This is because the density threshold is set in the proposed method. When k<30, the polygon region is expanded because it does not meet the anonymity requirement.

5.3 Analysis of Efficiency

In this paper, spatial anonymity is achieved by constructing a polygonal anonymous region. We compare the result of anonymous region construction with circular, rectangular, and polygon, as shown in Figure 9. As can be seen from Figure 9, comparing with the method of polygon construction, the methods of circular and rectangular construction enlarge the area of invalid region, its further reduce the accuracy of query result and privacy protection effect.



(a) (b)

Figure 9: The results of anonymous region construction; (a) Invalid region of circle, (b) Invalid region of rectangle

In other methods of spatial anonymity, if the area of anonymous region is larger than the maximum area threshold, the method is invalid. In the proposed method, if the area of the polygon anonymous region is larger than the maximum area threshold, the polygon anonymous region is expanded further, and $[k - N(Rs)]$ dummy locations are added to the polygon region. As shown in Fig-

ure 10, solid dots represent the neighbor users' locations found, hollow dots represent the added dummy locations, and solid triangle represents the user's current location. K locations including users' locations and dummy locations are sent to LBS server by TTP for query. It is difficult for an adversary to distinguish the user's current location from other k-1 locations. The proposed method is effective.

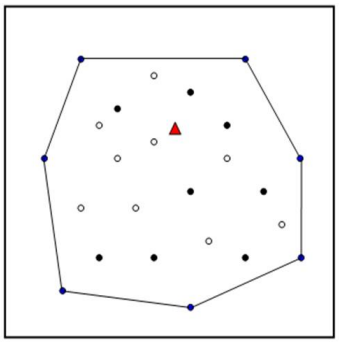


Figure 10: Combination of spatial anonymity and dummy

5.4 Comparison of Entropy

In location privacy protection method of dummy, entropy is usually used to measure effect of the location privacy protection. From the adversary's view, the anonymous set contains user's current location and k-1 dummy locations, and the probability that any location can be used as user current location is p_i. In an anonymous set, the sum of all probabilities is $\sum p_i$. Therefore, the entropy H for distinguishing the user current location in the candidate set is:

$$H = -\sum_{i=1}^{k} p_i \cdot \log_2 p_i \tag{4}$$

In Equation (4), if all the k locations of the candidate set have the same probability, the maximum entropy will be obtained. At this time, the probability of p_i is $1/k$, and the maximum entropy H is $\log_2 k$.

In Figure 11, we compare the entropy with the proposed and other three methods. Random is the method that selects dummy locations at random. Circular dummy and grid dummy are the virtual circle and virtual grid proposed in [15].

As can be seen from Figure 11, entropy of the proposed method is larger than that of the other methods. This is because k-1 dummy locations are all added randomly besides user's current location in the method of grid dummy and circular dummy. These dummy locations are easily distinguishable from the user's current location. In the proposed method, $N(Rs)$ locations are the neighbor users, its are indistinguishable from the user's current location. The remaining $[k-N(Rs)]$ locations are the dummy locations that is added, its are less indistinguishable from the user's current location. So the entropy of the proposed method is larger, and its effect of the privacy protection is better.

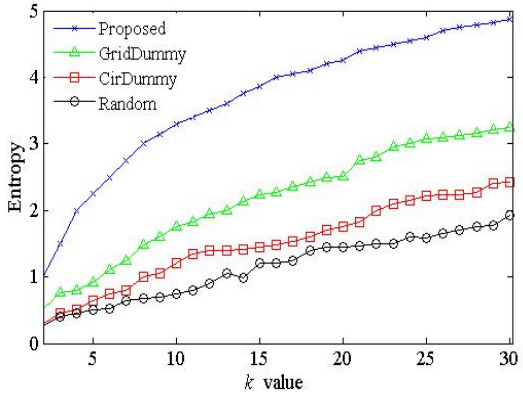


Figure 11: Entropy of the dummy locations

6 Conclusions

In recent years, the application and development of LBS are very fast, the security challenges of location privacy are becoming more and more serious. Location privacy protection has become a research hot spot in the field of information security. In the current widely used model of central server structure, aiming at the deficiency of spatial anonymity method, a k-anonymous location privacy protection method of polygon based on density is proposed. In this paper, according to the idea of k-anonymity, and adapting irregular polygon fast generation algorithm, a polygon anonymous region is constructed quickly, which improves the efficiency of anonymous region generation. At the same time, the area of polygon region is calculated through recursive method. According to the k-density distribution, an ideal and effective anonymous region is constructed. Furthermore, the privacy protection is implemented by combining spatial anonymity and dummy locations according to density parameters. And we evaluate our algorithms through a series of simulations, which show that our algorithm effectively improves the anonymity effect while taking into account query quality.

Acknowledgments

This work is supported by the National Science Foundation of China (No. 61363078, 61762059), Natural Science Foundation of Gansu (20JR5RE634), Innovation Ability Improvement Project of Colleges and Universities in Gansu (2020A-246), and Natural Science Foundation of Tianshui (2020-FZJHK-2664). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with privacy grid," in *Proceedings of the 17th International Conference on World Wide Web*, pp. 237–246, Jan. 2008.

[2] T. Brinkhoff, "A framework for generating network-based moving objects," *GeoInformatica*, vol. 6, no. 2, pp. 153–180, 2002.

[3] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, "Preserving user location privacy in mobile data management infrastructures," *Lecture Notes in Computer Science*, no. 4258, pp. 393–412, 2006.

[4] C. Y. Chow, M. F. Mokbel, and X. Liu, "Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments," *GeoInformatica* vol. 15, no. 2, pp. 351–380, 2011.

[5] R. Dewri, Y. Ray, and Y. Ray, "Query m-invariance: Preventing query disclosures in continuous location-based services," in *The Eleventh International Conference on Mobile Data Management*, pp. 95–104, May 2010.

[6] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," *IEEE Transactions on Mobile Computing*, vol. 7, no. 1, pp. 1–18, 2008.

[7] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services*, pp. 31–42, May 2003.

[8] Y. Huang and Z. P. Cai, "Bourgeois a g. search locations safely and accurately: A location privacy protection algorithm with accurate service," vol. 103, pp. 146–156, 2018.

[9] R. H. Hwang, Y. L. Hsueh, J. J. Wu, and F. H. huang, "Social hide: A generic distributed framework for location privacy protection," *Journal of Network & Computer Applications*, no. 76, pp. 87–100, 2016.

[10] J. Jia and F. Zhang, "K-anonymity algorithm using encryption for location privacy protection," *International Journal of Multimedia & Ubiquitous Engineering*, vol. 10, no. 9, pp. 155–166, 2015.

[11] Y. Jung and J. Park, "An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services," *International Journal of Information Management*, no. 43, pp. 15–24, 2018.

[12] J. Li, H. Y. Yan, Z. L. Liu, X. F. Chen, X. Y. Huang, and D. S. Wong, "Location-sharing systems with enhanced privacy in mobile online social networks," *IEEE Systems Journal*, vol. 11, no. 99, pp. 1–10, 2015.

[13] L. Li, J. Hua, S. Wan, H. Zhu, and F. Li, "Achieving efficient location privacy protection based on cache," *Journal on Communications*, vol. 38, no. 6, pp. 148–157, 2017.

[14] L. Li, Z. J. Lv, X. H. Tong, and R. H. Shi, "A dynamic location privacy protection scheme based on cloud storage," *International Journal of Network Security*, vol. 21, no. 5, pp. 828–834, 2019.

[15] H. Lu, C. S. Jensen, and L. Y. Man, "Pad: Privacy-area aware, dummy-based location privacy in mobile services," in *The Seventh ACM International Workshop on Data Engineering for Wireless and Mobile Access*, pp. 16–27, Jan. 2008. DOI: 10.1145/1626536.1626540.

[16] T. H. Ma, J. Jia, Y. Xue, and Y. Tian, "Protection of location privacy for moving KNN queries in social networks," *Applied Soft Computing*, no. 66, pp. 525–532, 2018.

[17] T. Peng, Q. Liu, G. J. Wang, and Y. Xiang, "Multidimensional privacy preservation in location-based services," *Future Generation Computer Systems*, no. 93, pp. 312–326, 2019.

[18] M. B. Xie, Q. Qian, and S. Ni, "Clustering based k-anonymity algorithm for privacy preservation," *International Journal of Network Security*, vol. 19, no. 6, pp. 1062–1071, 2017.

[19] P. S. Xie, J. Guo, and Q. Wang, "A-anonymous polygon area construction method and algorithm based on LBS privacy protecting," *Journal of Information & Computational Science*, vol. 12, no. 15, pp. 5713–5724, 2015.

[20] J. Xu, X. Tang, H. Hu, and J. Du, "Privacy-conscious location-based queries in mobile environments," *IEEE Transactions on Parallel & Distributed Systems*, vol. 21, no. 3, pp. 313–326, 2010.

[21] Y. Yang and R. Wang, "Rectangular region k-anonymity location privacy protection based on LBS in augmented reality," *Journal of Nanjing Normal University(Natural science)*, vol. 39, no. 4, pp. 44–49, 2016.

[22] A. Y. Ye, L. Y. Cheng, J. F. Ma, and L. Xu, "Location privacy-preserving method of k-anonymous based on service similarity," *Journal of Communications*, vol. 35, no. 11, pp. 162–169, 2016.

[23] C. Yin, R. Sun, and J. Xi, "Location privacy protection based on improved k-value method in augmented reality on mobile devices," *Mobile Information Systems*, vol. 2017, no. 12, pp. 1–7, 2015.

[24] U. Yuji, M. Natsume, and Y. shota, "Private similarity searchable encryption for euclidean distance," *IEICE Transactions on Information and Systems*, vol. 100, no. 10, pp. 2319–2326, 2017.

[25] S. B. Zhang, X. Li, Z. Y. Tan, and T. Peng, "A caching and spatial k-anonymity driven privacy enhancement scheme in continuous location-based services," *Future Generation Computer Systems*, vol. 94, no. 2019, pp. 40–50, 2019.

[26] Z. Zhao, H. Hu, and F. Zhang, "A k-anonymous algorithm in location privacy protection based on circular zoning," *Journal of Beijing Jiaotong University*, vol. 37, no. 5, pp. 13–18, 2013.

Biography

Yong-bing Zhang is currently a Ph.D. student in Lanzhou University of Technology, and worked at school of Gansu Institute of Mechanical & Electrical Engineering. He received his master degree in electronic and communication engineering from Lanzhou University of Technology, Gansu, China, in 2015. His research interests include network and information security, privacy protection.

Qiu-yu Zhang Researcher/PhD 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.

Yan Yan associate professor. received her master degree in communication and information systems from Lanzhou University of Technology, Gansu, China, in 2005. She is currently a Ph.D. student in Lanzhou University of Technology. Her research interests include privacy protection, multimedia information security, uncertain information processing.

Yi-Long Jiang Professor, graduated from Shanghai Technology university in 1989, and then worked at school of Gansu Institute of Mechanical & Electrical Engineering. His research interests include embedded control technology, intelligent manufacturing intelligent, manufacturing technology.

Mo-yi Zhang associate professor. received her doctorate degree in manufacturing information systems from Lanzhou University of Technology, Gansu, China, in 2019. Her research interests include artificial intelligence, image processing and pattern recognition.

Applying Permutations and Cuckoo Search for Obtaining a New Steganography Approach in Spatial Domain

Dieaa I. Nassr and Sohier M. Khamis

(Corresponding author: Dieaa I. Nassr)

Computer Science Division, Department of Mathematics, Ain Shams University
11566 Cairo, Egypt
(Emails: dieaa.nassr@sci.asu.edu.eg)

(Received July 29, 2020; revised and accepted Nov. 10, 2020)

Abstract

Video Steganography is an art and science of embedding secret information into a carrying video file in such a way that others cannot observe the embedded information. Cuckoo Search (CS) is a meta-heuristic algorithm which has been developed by Xin-She Yang and Suash Deb in 2009. CS is very effective in solving many optimization problems that have been found in previous literature. In this paper, a new efficient approach for embedding a secret image in a digital video is proposed. Generally, any colored image consists of three color components (Red, Green, and Blue). So, an image's pixel has three bytes; each of which belongs to one different color component. For security purposes, each secret image's color component is embedded separately into a selected cover video's frame. The proposed approach is based on the permutations on 3 sections of a secret byte, 3-3-2 bits. These three sections are permuted to obtain five different patterns of a specified secret byte. Then, the population of five different pairs is built; each pair consists of one different pattern repeated twice. Good pixels are so chosen via using CS algorithm to achieve the minimum distortion in carrier pixels due to embedding. The sum of absolute values of sectional differences is used as an objective function to compare all the distances between the 3-3-2 Least Significant Bit (LSB) values of a cover frame's pixel and the generated different patterns of a specified secret byte. Experimental results show that the efficiency of the suggested approach is successful since the Peak Signal to Noise Ratio (PSNR) is above 52 decibels.

Keywords: Cuckoo Search; Lévy flights; LSB; PSNR; Video Steganography

1 Introduction

Due to the rapid growth in Internet usage, a lot of information has been shared and transferred through it [29]. The importance of reducing the risk of information being detected during transmission is increasingly important among research topics nowadays. Steganography has become one of the most robust techniques for transmitting confidential messages between parties [18]. Steganography is an art and science of invisible communication, which is used to embed secret data into modern cover types such as text, audio tracks, digital images, and video files. Due to the increased transmission rate of video files on websites such as Facebook, Twitter, and YouTube, video files now pay more attention to steganography.

Video steganography is the process of embedding some secret information within a video [4]. It can be presented as an extension of image steganography. Basically, a video stream is a set of frequent images and audio. Therefore, many researchers have applied image steganographic methods on the video to yield video steganography similar to image steganography, *e.g.*, [2, 10, 23, 24] Video file is a moving stream of images in which a large amount of data can be embedded inside it without being observed. The advantage of using video files in hiding information is the added security against the attack of hackers due to the relative complexity of the structure of video compared to image files. Video-based steganographic techniques are broadly classified into the frequency domain and spatial domain [6,27]. In the frequency domain, frames are transformed to frequency components by using Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), or Discrete Wavelet Transform (DWT), and then, messages are embedded in some or all of the transformed coefficients. Embedding may be at bit level or at the block level. Moreover, in the spatial domain, the bits of a message can be inserted directly in intensity pixels of a video in LSB positions. However, most LSB techniques are prone to attack as described as in [6, 25, 27]. This makes researchers interested in designing new methods. In (2015, [25]), a new idea in video-based steganography has been given, where secret message bits are embedded

in a cover file by using the LSB technique. For embedding, the selection of cover file RGB pixels is done on the basis of its color intensity value. LSB technique is used to embed bits in a specified cover file. This approach leads to a very high capacity with low visual distortions.

In the next, the following terms and notations are used. Cover-video refers to a video file that is used for embedding secret information. A secret-message refers to confidential data that is embedded in a specified cover-video. Stego-video is obtained from combining the cover object with embedded data [12]. Embedding Efficiency (EE) and Embedding Payload (EP) are two important factors that every successful steganography system should take into consideration. EE means good quality of the stego-video and fewer amounts of changed data in a cover-video. While EP means higher capacity allocated for concealing a secret-message inside a cover-video [16]. There is a trade-off between EP and EE. When the capacity of hidden information is increased, the quality of the stego-object is decreased [11, 20, 21].

In fact, the underlying problem for selecting good pixels locations for embedding data can be viewed as an optimization problem [30]. Cuckoo Search (CS) is one of the most intelligent algorithms that can be chosen as a comprehensive search method in many optimization problems. The proposed approach in this paper is a kind of video steganography in the spatial domain. This approach is based on trying to hide large data with minimal distortion in the host video stream. It depends on the concept of permutations on secret bits and then, CS is used for finding good embedding pixels locations in which a secret message can be embedded. A secret-message is concealed in RGB components of the founded carrier pixels using the 3-3-2 LSB technique. A specified secret byte is permuted according to five different pre-indexed patterns before embedding. Finally, these permuted secret bytes are embedded randomly in certain video's frame pixels. So, it is difficult for the attacker to retrieve secret information from a given stego-video. The rest of this paper is organized as follows. Section 2 gives an overview of video steganography. In Section 3, some selected related works are presented. Section 4 introduces the Cuckoo Search algorithm. In Section 5, the suggested CS-based video steganography approach is described. Experimental results and concluded remarks are given in Sections 6 and 7, respectively.

2 Video Based Steganography

Steganography is the process of embedding secret information inside a host medium such as text, audio, image, and video [16]. Its ultimate objectives are un-detectability and robustness of embedded data. Video consists of stream of frames (images) and audio. Any frame of a video can be selected for embedding sent data [14]. The quality of a video depends on a set of parameters; three of them are considered in this paper, namely; the number of pixels in a frame, the number of frames per second (fps), and the frame's size. The number of fps is often standard (between 24 and 30 fps) in most of common video formats. But, the other two parameters vary from one video standard format to another. Each frame consists of pixels having three or four color components such as RGB (Red-Green-Blue) or CMYK (Cyan-Magenta-Yellow-Black) [15]. The basic model of video based steganography consists of five basic elements as illustrated in Figure 1. Some information of these elements is given in the following:

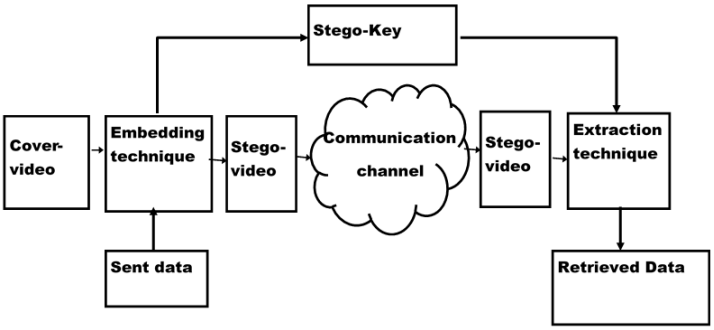


Figure 1: A generalized block diagram of video steganography procedure [15]

- *Cover-video:* An input video used for data concealing.
- *Sent data:* A given data that is to be hidden.
- *Embedding technique:* A technique to conceal a sent data behind cover-video.
- *Stego-video:* A digital video that has a secret-message hidden inside.
- *Stego-key:* The key is built during the embedding stage and then, used for extracting purpose.
- *Extraction technique:* A technique to retrieve the secret-message behind stego-video.
- *Retrieved data:* The obtained data after applying the extraction technique.

Least Significant Bit (LSB) is a popular technique used for embedding information in a cover file [7,8,25]. The basic step of LSB technique is to replace LSB values which are necessary for embedding a secret-message. This message is decomposed and embedded into LSBs of a cover frame so that hackers cannot detect it.

In the classic LSB, the size of a secret-message that can be embedded is equal to 12.5% of the cover image's size. Thus, it is considered a small storage capacity. Consequently, some researchers have used the base technique 3-3-2 for embedding a secret-message [8]. Figure 2 illustrates 3-3-2 method in which the first 3 bits of a byte from a given message are embedded into the last 3 bits of

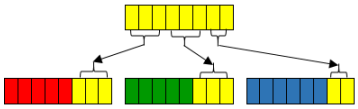


Figure 2: A sketch of embedded one byte of a secret-message in 3, 3, 2 bit position of LSB of R, G, and B components respectively of a cover frame (For interpretation of the colors in this figure and Figure 3, the reader is referred to the web version of this article)

the Red component; the second 3 bits are embedded into the last 3 bits of the Green component, and the last 2 bits of the message are embedded into the last 2 bits of the Blue one. Since the variation in blue is perceptible more than both Red and Green to the human eye, researchers choose to put only 2 bits in the Blue component. This means that byte can be hidden in each pixel of the color image (24-bit), as shown in Figure 2. So, this method increases the embedding capacity up to 33.3% from the size of a cover file.

Video steganography can be classified into two main types. The first one embeds data in uncompressed video, which is compressed later [19, 28]. The second type tries to embed data directly in compressed video stream [6]. In this paper, the authors simply consider the uncompressed video steganography in spatial domain using 3-3-2 LSB replacement technique for embedding a secret-message.

3 Related Works in Steganography

In the last decades, the number of meta-heuristics algorithms that are used to optimize the steganography process in the spatial domain, is growing rapidly. In [7], 3-3-2 LSB based technique has been enhanced using Genetic Algorithm (GA) to get an optimal imperceptibility of hidden data. The obtained results have shown that PSNR lies between 20 and 40 decibels (dBs). An algorithm for optimizing the payload capacity subject to minimal visual degradation has been proposed in [5]. In that algorithm, Logistic Maps have been used for the random selection of pixels. The randomness of selected pixels has been improved by GA subjected to the less distortion of a cover-image. Experimental results have shown the robustness of the proposed algorithm. A technique that can be used to conceal a secret-message into the LSBs of a cover-image and to overcome the level of security issues has been described in [9], which is adopted Ant Colony Optimization (ACO) algorithm to find the optimal LSB substitution matrix. The obtained results have shown that the efficiency of ACO and the PNSR value of stego-image goes beyond 35 dBs. Cat Swarm Optimization (CSO) algorithm has been adopted to achieve an optimal or near-optimal solution of stego-image quality problems in [26]. Each individual cat has four attributes, namely; its own position composed of k-dimensional, velocity for each dimension, a fitness value based on a given fitness function, and a flag to specify whether a cat is in seeking mode or tracing mode. Experimental results have shown that the proposed CSO based scheme can achieve a good solution with less computation time. In (2013, [22]), a new image steganography method has been introduced. This method is based on combining Particle Swarm Optimization (PSO) and Simulated Annealing (SA) together in order to select an optimal LSB substitution matrix for embedding. Comparing the simulation results of both PSO and SA algorithms with their combination (PSO-SA) in terms of PSNR values, it can be shown that the stego-image yielded by the combined PSO-SA has a higher quality than each of the two algorithms.

4 Cuckoo Search

Cuckoo Search (CS) is a nature-inspired metaheuristic algorithm developed by Xin-she Yang and Suash Deb in [30]. It was inspired by the breeding behavior of cuckoos. A cuckoo breeding can be illustrated as an act of parasitism by laying its egg in a random nest of other host birds (of other species) [3]. Sometimes, a host bird discovers the alien egg and throws the alien egg away or simply abandons its nest. A cuckoo might have the characteristic of shape, size, and color of the host eggs to protect his own egg from being discovered. A cuckoo may take aggressive action by removing other native eggs from the host nest to increase the hatching probability of its own eggs. A hatched cuckoo chick may even throw other eggs away from the nest to improve its feeding share. CS depends on Lévy flights to determining a random walk. Lévy flights, named by the French mathematician Paul Lévy, represent a model of random walks characterized by their step lengths which obey a power-law distribution. It has a characteristic of an intensified search around a solution, followed by big steps in the long run. In CS, a random walk is used to produce a new solution (a host nest) from the current solution according to Equation (1).

$$x_i^{(t+1)} = x_i^{(t)} + \alpha \oplus Lévy(s, \lambda), \tag{1}$$

Where $x_i^{(t+1)}$ is the i^{th} Cuckoo at instance $t+1; \alpha > 0$ is the step size; λ is the Lévy distribution coefficient; and the product $\oplus$ means entrywise multiplication. The Lévy flight essentially provides a random walk while the random step length is drawn from a Lévy distribution which is given by Equation (2).

$$Lévy(s, \lambda) \sim s^{-\lambda}, \text{ where } 1 < \lambda \leq 3. \tag{2}$$

The incidental walk via Lévy flights is more efficient in exploring a search space, as its stride length is much longer in the long run. In [30], Yang and Deb have discovered that the random-walk style search is better performed via using Lévy flights rather than a simple random walk. The idealized rules of CS can be summarized as follows [30].

Each cuckoo lays one egg at a time and dumps its egg in a randomly chosen nest. The best nests with high-quality eggs would carry over the next generations. The number of available host nests is fixed and the probability of discovering the laid egg by the host bird can be calculated as $p_a \in]0,1[$. The fraction p_a of the n nests is replaced by new ones.

A pseudo-code of CS is outlined in the following steps:

Algorithm 1 CS

Input: n is the number of nests, p_a is the fraction of n nests.

Output: The best solution.

1: Begin
2: Randomly initialize population of n host nests $X_i = (x_i^1, \ldots, x_i^d)$ for $i = 1, 2, \cdots, n$, and d dimensional problem.
3: Define objective function: $f(X)$; where $X = (x^1, \cdots, x^d)$; {the goal is to maximize the objective function}
4: $G \leftarrow 1$
5: **while** ($G <$ MaxGeneration) or (stop criteria) **do**
6: **for** $i = 1$ to n **do**
7: Randomly get a new Cuckoo X_i using Lévy flights Equation (1);
8: Evaluate its quality/fitness: $f(X_i)$;
9: Choose randomly a nest, say, j, among n host nests;
10: **if** $f(X_i) > f(X_j)$ **then**
11: Then update j^{th} nest by the new solution;
12: **end if**
13: **end for**
14: The worst nests are abandoned with a probability (p_a) and new one are built;
15: $G = G + 1$;
16: **end while**
17: Find the best solution by ranking the values of n host nests;
18: End

5 Solving the Video Steganography Problem with CS

In this section, a new approach to solve video-based steganography problem in spatial domain is proposed. The key of this approach is based on creating five different pattern of each byte of a given secret message. Subsection 5.1 gives the detailed description of generating the different pattern while Subsection 5.2 is devoted to combine this approach with CS. It is used for seeking about optimal (or nearest optimal) pixels for embedding the given secret-bytes inside its RGB component values to obtain the stego-object. The suggested steganography approach is described in Subsection 5.3. Finally, Subsection 5.4 contains the extracting process.

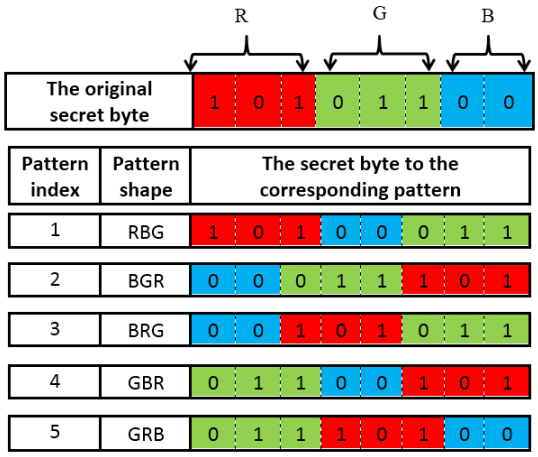


Figure 3: The 5 different patterns of (10101100)

5.1 Generating the Different Patterns

In the suggested approach, any secret message is entered byte by byte. First, each byte is divided into 3-3-2 bit sections noted as R, G, and B, respectively. Then, these three sections are permuted to construct the five different patterns for a specified byte. For instance, suppose that the current secret byte is (10101100), the constructed different patterns are shown in Figure 3. The main aims of these permutations are to increase the security level of the information to be hidden and the chance of matching the secret byte with carrier pixel's LSB.

5.2 Matching Between the Video-Steganography and CS Terminologies

Once the 5 different patterns of a given secret byte are generated and a carrier-video is accomplished, CS algorithm can be applied. The CS algorithm is structured upon five main elements: egg, nest, search space, objective function, and Lévy flights. These elements have the following meaning in treating this problem.

i *Egg:* As usual, a cuckoo lays a single egg in one nest, eggs have the following properties: An egg in a nest is considered a feasible solution adopted by one individual in the population. An egg of a cuckoo is a new solution that candidates for a place in the population. In the steganography problem, we can say that an egg is equivalent to one of the secret byte's patterns.

ii *Nest:* As in CS algorithm, the following characteristics can be imposed regarding to a nest:

- The number of nests is fixed.
- A nest is an individual of the population and the number of nests equals to the size of the population.
- An abandoned nest involves the replacement of an individual of the population by a new one.

By the projection of these features on the suggested video-based steganography approach, a nest has shown as an individual pixel in the population (as mentioned in the next, the size of the population is equal to ten) that is used to carry the current secret byte in the shape of its own pattern.

Furthermore, on the discovery of alien eggs in its nest, a host bird would either get rid of these eggs or quit its nest altogether in quest of setting up a new one elsewhere. Hence, some nests might be removed which is in line with the host bird's attitude. To simulate this behavior, a fraction of p_a, 20% from the population's individuals, are removed from the current iteration, and hence, new ones at new locations are created by Lévy flights.

iii *Search Space:* Generally, every digital video file consists of a set of frames and audio. So, both audio and frames can be used to embed the secret data. In the present work, a carrier video file is decomposed to a set of frames (images) and audio. Hence, according to the size of a secret-message, a suitable number of frames are selected and given as input to the suggested approach. A digital frame is considered as a two-dimensional matrix of elements, in which each element corresponds to a single pixel in a frame and each pixel has two coordinates, x, and y. A secret-message can be either embedded in a single frame of a video or in multiple frames, to guarantee security and hard-detect.

iv *Objective Function:* The current secret byte will be embedded into the selected pixel's RGB 3-3-2 LSB components. As mentioned in Subection 5.1, a secret byte is divided into 3-3-2 bit sections. Also, as explained in Section 2, the pixel's 3-3-2 LSB sections are extracted. During the search, the cost is calculated for each candidate solution (nest) by calculating the sum of absolute differences between the decimal value of the 3-3-2 LSB sections and the corresponding decimal value of the secret byte sections. This summation of absolute Differences, D, is used as objective function which is determined by Equation (3). In this equation, CP-LSB is the current pixel's 3-3-2 LSB; SB is the current Secret Byte; each of which has three sections; and x_z is the decimal number of z's binary number.

$$D(CP-LSB,SB)=\sum_{section=1}^{3}|x_{CP-LSB_{section}}-x_{SB_{section}}| \quad (3)$$

For instance, suppose that the candidate pixel's RGB components and the secret byte are given as follows.

	section1	section2	section3
CP-LSB	10001101 (5)	10101110 (6)	10000010 (2)
SB	010 (2)	011 (3)	01 (1)

The objective function is determined by

$$D(CP-LSB,SB)=|5-2|+|6-3|+|2-1|=7.$$

Evidently, the goal is to minimize the suggested objective function. This means that the least cost value is called a best solution or equivalently a best nest, otherwise is called a worst nest.

v *Lévy flights:* One of the most powerful features of CS is the use of Lévy flights to generate a position of a new candidate solution. And according to [17], in some optimization problems, the search for a new best solution is more efficient via applying Lévy flights. In the given approach, the Lévy flight term is associated with the step lengths to improve the quality of search as outlined in CS.

5.3 New Steganography Approach

In this work, the data required for each nest is gathered in a record called Nest Structure abbreviated by (NStruct). As shown in Figure 4, each nest structure consists of five fields. The first one, byte's order, contains K which is an integer number refers to the order of the current secret byte in a secret-message. While the second field, SB, is the current secret byte to be hidden. The third field, Pattern, contains the pattern's index which corresponds to the pattern shape of the current secret byte. The fourth field, Location, contains the location of candidate pixel for embedding. The last one, D, is the sum of absolute values of sectional distance between the current secret byte and the current pixel. It is clear that the contents of the first three fields are fixed. But the last two fields are updated in the process of generating a new solution in the same iteration. This is done by performing a random walk via using Lévy flights.

At the beginning (the preparing step), the Binary-byte Stream array, BinStr, for the given RGB image is constructed. This array consists of three consecutive parts, each of which has the same number of bytes. The first one contains the red component of the image; The second part has the green component; while the last part contains the blue component. This is done because the suggested approach is based on embedding each color component (R, G, and B) in one frame chosen arbitrarily from the cover video.

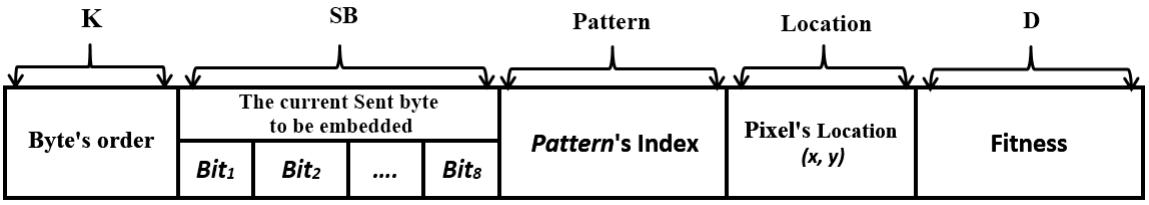


Figure 4: A nest structure (NStruct)

Now, a description of the suggested steganography approach for embedding a specified RGB image within three video frames is given. The main idea depends on repeated each pattern of a secret byte twice which is collected in a pair. So, we deal with each pair of a similar pattern as two distinct eggs. This leads to the current population has 10 individuals, each pair of individuals are compared together to decide the best nest and the worst nest using the suggested objective function. Each pair has two copies of the pattern and all of these patterns should be unchanged over all iterations until the best location of the current byte is obtained and then get the next new byte. Hence, it is well-known that the Elitism process is based on the best solution that is kept unaltered and automatically will be carried over to the next generations unless a more favorable solution is found. In this approach, the Elitism process is applied for each pair separately. So, the suggested population has 5 elitists' solutions and this considers a modification of our previous work [26] which kept one elitist solution.

The steganography algorithm works iteratively as follows. In any iteration, the candidate pixel for each nest is evaluated by the objective function. Once this process is completed for all five pairs of nests, the best individual of each pair is determined and stayed at its current pixel (location). These best nests are carried over to the next generation. After that, the location of the worst individual of each pair is updated by performing a random walk via applying Lévy flights. Then, the sectional differences between each updated nest and its corresponding pattern are evaluated.

Next, for each pair, compare each new nest with its corresponding best nest to update its rank. A fraction p_a, 20% of the population ($\equiv$ two worst nests in our approach) is removed and new nests are created by using Lévy flights. A new generation consists of five new pairs. This process is repeated until the termination condition is achieved, *i.e.*, the maximum number of iterations is reached or an acceptable result has been found depending on a sectional differences threshold value (stop criteria). When the termination condition is satisfied, the best five nests from the last generation are ranked and the lowest-cost individual (best nest) is determined. Then, the secret byte is embedded by its pattern inside the RGB component values of the selected carrier pixel in 3, 3, 2 order as described in Section 2. After the secret byte is embedded in the selected pixel, the three fields (1, 3, and 4) values of the NStruct are saved as a stego-key. Then, the stego-key and the frame numbers contained in the hidden secret RGB-image will be sent to a receiver to be used in the decoding stage. The aforementioned suggested solution would be consecutively repeated to embed each secret byte from the desirable RGB image in the chosen three cover frames. The outlines of the proposed approach are formulated in Steganography (SG) Algorithm 3

Algorithm 2 SG

Input: H, W; the height and width of the given RGB image. BinStr; The Binary-byte Stream is a one-dimensional array having consecutively HW-byte R-component, HW-byte G-component, and then HW-byte B-component of the given RGB image. Nest; 5×2 array of 10 NStruct to save the information of the current feasible solutions. F_1, F_2, F_3; three cover-video frames, where (F_1, F_2, and F_3) are arbitrary chosen to embed R, G, and B components of RGB image, respectively.

Output: Three stego-frames, Stego-key.

1: Begin
2: Define the objective function $D(CP - LSB, SB)$ as given in Equation (3); { where $CP - LSB$, SB are the current pixel's 3-3-2 LSB and underlying secret byte, respectively.}
3: $Z \leftarrow H \times W$; {the number of pixels in the given RGB image}.
4: **for** i=1 to 3 **do**
5: $Z_{first} \leftarrow (i-1)Z + 1$, $Z_{last} \leftarrow iZ$;
6: **for** $J = Z_{frist}$ to Z_{last} **do**
7: **for** p =1 to 5 **do**
8: Nest[p, 1].K = Nest [p,2].$K \leftarrow J$;
9: Nest [p, 1].SB =Nest [p,2].$SB \leftarrow$ BinStr[J];
10: **end for**
11: $G \leftarrow 1$; stop criteria $\leftarrow$ true;
12: Generate the five different patterns corresponding to five eggs named by
$X_1, X_2, \ldots, X_5$ for BinStr[J];
13: **for** k=1 to 5 **do**
14: Duplicate the egg X_k to produce the related pair (X_k, X'_K);

Choose randomly two non-flagged pixels (host nests) (L_k, L'_K) for embedding (X_k, X'_K), respectively;
Evaluate $d_k = D(L_k, X_k)$ and $d'_k = D(L'_k, X'_k)$;
if $d_k < d'_k$ **then**
Keep index of X_k ,L_k and d_k in three fields (Pattern,Location,and D)of Nest[k,1],respectively;
Keep index of X'_k ,L'_k and d'_k in three fields (Pattern,Location,and D)of Nest[k,2],respectively;
else
Keep index of X'_k ,L'_k and d'_k in three fields (Pattern,Location,and D)of Nest[k,1],respectively;
Keep index of X_k ,L_k and d_k in three fields (Pattern,Location, and D)of Nest[k,2],respectively;
end if
if Nest[k,1].$D \leq$ sectional differences - threshold **then**
stop criteria ← False; go to 45
end if
end for
while ($G <$ Maxieteration) or (stop criteria) **do**

Stay(Nest[1,1],Nest[2,1],... ,Nest[5,1]) in the current iteration;
for k=1 to 5 **do**
Update Nest[k,2].Location by using Equation (1) to get new non-flagged (L'_k);
Evaluate $d'_k = D(L'_k, X'_k)$;
Nest[k,2].D ← d'
if Nest[k,1].D $> d'_k$ **then**
Swap Nest[k,1] and Nest[k,2];
if Nest[k,1].D $\leq$ sectional differences - threshold **then**
stop criteria ← False; go to 45
end if
end if
end for
Choose randomly two nests (Nest[m,2] and Nest[n,2]) ; where m,n are any two different numbers from 1 to 5 { to achieve the probability of discovering the laid egg by the host bird (p_a= 0.20)};
Execute steps from 31 to 36 twice for $k = m$ and $k = n$; {execute for each chosen nest};
$G \leftarrow G + 1$;
end while
Determine q at which Nest[q,1].D ($1 < q \leq 5$) has lowest value (best nest) from the current iteration;
Embed X_q into Nest[q,1].Location inside F_i using 3-3-2 LSB as described in Section 2;
Mark embedding pixel Nest[q,1]s.Location as Flagged pixel;
Save Nest[q,1].K , Nest[q,1].Patern, and Nest[q,1].Location in the stego-key;
end for
end for
End

After the embedding process is finished, the stego-frames are formed and then merged with the remaining frames and audio to build a stego-video

Lemma 1. *Algorithm SG is a polynomial-time algorithm for solving the video steganography problem with low visual distortions by using CS.*

Proof. It is easy to show that steps from 6 to 49 of algorithm SG are repeated 3 $(H \times W)$ times where $H \times W$ is the number of pixels in the given RGB image that want to be secret; each pixel has 3 SB. In two outer For loops, there exist inner two loops, namely For-loop from Steps 13 to 27 and While-loop starts from step 28 and ends at step 44.

Clearly, Steps from 14 to 26 inside the For loop are repeated 5 times. Since each operand has only 8 bits except d_k and (d'_k) (small integer numbers) and all operations such as assignments, calculating objective function, and comparison between small numbers are taken unit-time execution so this loop does not affect the running time of the algorithm except step 15 depends on the size of a suggested frame, say M (hight)$times N$ (width), of cover-video, *i.e.*, is not exceed than $5.O(c_1 + M \times N)$, where c_1 is a some constant. As a result, the complexity of this loop is $O(M \times N)$. While-loop contains For-loop (from steps 30 to 40). Evidently, this For-loop has simple mathematical operations and assignments, so the time of this part is not exceeding than $5.O(c_2 + M \times N)$, where c_2 is a constant. Also, this takes $O(M \times N)$. It is not difficult to consider the running time of While-loop depends only on its condition and the size of the cover-videos frame, *i.e.*, $O($ number of iterations $\times M \times N)$. All steps that are not mentioned explicitly are considered to be a limited number of unit-time of execution. Based on the above, the whole complexity time of Algorithm SG is in O(the size of the given image *times* the size of cover video's frame), since the condition of While-loop executed via a limited number of iterations (from 50 up to 100). □

It is worthy to say that the size of the given image $H \times W$ and the size of cover-video's frame $M \times N$ are both limited integer numbers, so the suggested algorithm SG is an efficient one and runs fast in practice.

5.4 Extracting Process

The process of hiding any secret message into a cover-video to produce a stego-video is successful when the receiver able to retrieve the secret message. Via using stego-key and stego-video, the receiver can extract the specified image. For decoding or extracting process, one can follow these steps:

Algorithm 3 SG

Input: Stego-video, stego-key;
Output: Retrieved secret RGB-image.

1: Begin
2: Unplug frames from stego-video;
3: Use stego-key to select the three frames F_1, F_2,and F_3 that contains R, G, and B components of the required secret-image;
4: Create the row image named by retrieved secret RGB -image with dimension $H \times W$ pixels, each pixel contains 3 bytes corresponding to RGB components;
5: BinStr $\leftarrow$ 0; { 1-dimentinal array for saving the retrieved secret-message that has 3HW bytes;}
6: $Z \leftarrow H \times W$;
7: **for** $i = 1$ to 3 **do**
8: $Z_{first} \leftarrow (i-1)Z + 1$, $Z_{last} \leftarrow iZ$;
9: Use F_i to retrieve HW secrets bytes hidden behind it;
10: **for** $k = Z_{frist}$ to Z_{last} **do**
11: Read stego-key [k] to get pixel location and the pattern's index;
12: Retrieve and rearrange 3-3-2 LSB according to pattern's index to obtain Original Byte[k], OB;
13: Save OB in BinStr[k];
14: **end for**
15: **end for**
16: Use BinStr to write its contents on the retrieved RGB-image in the suitable bytes of the corresponding pixels to obtain the correct secret image;
17: End

Obviously, Algorithm Extraction depends on the size of retrieved secret RGB-image, *i.e.*, $O(H.W)$,so it's also an efficient one.

6 Experimental Results

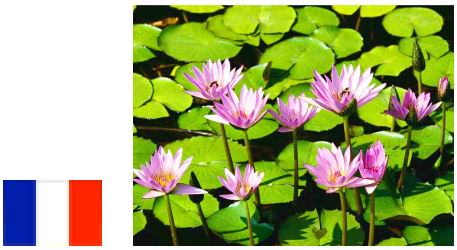
This section provides the experimental results of the suggested SG algorithm applied to the given dataset. Also, it contains a description of the used dataset and illustration of the evaluation criteria, the suggested parameters, and finally the evaluation of results.

6.1 Dataset

To test and evaluate the steganography approach, an uncompressed AVI cover-video file and five different size secret-images are considered. Table 1 shows the detailed information of secret images and cover-video. In this work, a digital color image is used as a secret-image and it is preprocessed before the embedding phase; the whole pixels in the image file are converted into an array of binary bytes. Due to the use of 3-3-2 LSB embedding method, if the carrier-frame has size M (height)$\times N$ (width) , the maximum size of the secret bytes can be embedded at most $\frac{1}{3}(M \times N)$.

Table 1: The detailed information of the secret-images and cover-video

Secret Images information		Cover-Video File information		
Secret-Image (see Figure 5)	Resolution ($H \times W$)	Frame/sec	No. of frames	Resolution ($M \times N$)
A B	30×20 70×70	30	450	240×320



A B

Figure 5: Secret-Images

6.2 Evaluation Criteria

Generally, in steganography, the Peak Signal to Noise Ratio (PSNR) in decibels (dBs) is used as a visual quality metric to evaluate the quality of the stego-object. In order to determine PSNR, the Mean Square Error (MSE) between the cover-frame and the stego-frame is first computed by Equation (4).

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (I_{i,j} - I'_{i,j})^2 \qquad (4)$$

Where $I_(i,j)$ and $I'_(i,j)$ are intensity of pixel located at (i,j) in cover-frame and in stego-frame, respectively, and $M \times N$ is the frame's size.

Depending on MSE value, the PSNR is calculated by Equation (5).

$$PSNR = 10 \log_{10} \frac{L^2}{MSE}, \qquad (5)$$

where L is the peak signal level for an image color component value = 255. The performance of the steganography approach has been evaluated by doing the simulation using MATLAB 7.6 (R2009a) on an Intel Core i7 CPU, 2.67 GHz, 4 GB RAM PC, and windows 8.1 pro.

6.3 Setting up Cuckoo Search Algorithm for Video Steganography

The parameters that we have used in the applied cuckoo search are $n = 10$ nests and the discovery rate of alien solutions$p_a = 0.20$. Due to the Lévy flights, the values used for the Lévy exponent $\lambda = 1.5$ and the step size $\alpha = 1$. As stopping criteria, the maximum number

of generations of the implemented CS is 50 or the specific fitness threshold value. Here, the search space is the cover-frames. So, the lower and upper frame bounds are coordinate $(1, 1)$ and coordinate (frame's width, frame's height), respectively.

6.4 Results

In the experimental implementation, RGB component values are separately extracted. Then, each color component of them is embedded into the selected pixels of a separate cover-frame. Table 2 shows the performance of the suggested approach.

Table 2: Performance of suggested cuckoo search over video steganography

Secret-Image (see Figure 5)	Results obtained using 3,3,2 LSB	Results obtained using algorithm SG
	PSNR	
A	53.2952	65.5863
B	46.9173	59.0799

Generally, when the PSNR value is higher than 30 dBs, the quality of the obtained stego-video is acceptable [13]. As shown in Table II, the proposed method does not cause a significant decrease in video quality. All the results of PSNRs are between 52 and 65 dBs, which are considered good results with regard to the purpose of quality. The present approach is superior to the other pervious one that we introduced in [1].

7 Conclusion

In this paper, an optimized video steganography approach is suggested. This approach, SG algorithm, is based on the concept of using permutations on 3-section of a secret-byte (3-3-2 bits) and cuckoo search algorithm for searching about the suitable pixel locations to applying 3-3-2 LSB embedding method. First, the bits of each secret byte are arranged into five different patterns by using a permutation method. After that, CS algorithm is initialized by a population consists of five different pairs corresponding to the five permuted secret byte patterns and then employed to find a good pixel position. Finally, the 3-3-2 LSB technique is applied to embed the specified secret byte. Experimental results show that the proposed approach attains a high embedding efficiency against security analysis and in retaining stego-video qualities. PSNR and MSE measurements are used to measure the visual quality and all the obtained experimental results have a PSNR above 52 dBs.

In future work, we'll hope to apply other meta-heuristic algorithms such as Simulating Annealing, Elephant Search Algorithm (ESA) , and Cat Swarm Optimization (CSO).

References

[1] S. A. Abbas, T. I. B. E. Arif, F. F. M. Ghaleb and S. M. Khamis, "Optimized video steganography using cuckoo search algorithm," in *IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS'15)*, pp. 572-577, 2015.

[2] A. Ansari, M. T. Parvez, M. S. Mohammadi, "A comparative study of recent steganography techniques for multiple image formats," *International Journal of Computer Network and Information Security*, vol. 11, pp. 11-25, 2019.

[3] W. M. Aly, "Evaluation of cuckoo search usage for model parameters estimation," *International Journal of Computer Applications*, vol. 78, no. 11, pp. 1-6, 2013.

[4] R. Balaji and G. Naveen, "Secure data transmission using video Steganography," in *IEEE International Conference on Electro/Information Technology (EIT'11)*, pp. 1-5, 2011.

[5] J. Chandrasekaran, G. Arumugam,and D. Rajkumar, "Ensemble of logistic maps with genetic algorithm for optimal pixel selection in image steganography," in *IEEE 2nd International Conference on Electronics and Communication Systems (ICECS'15)*, pp. 1172-1175, 2015.

[6] K. Dasgupta, J. K. Mandal, and P. Dutta, "Hash based least significant bit technique for video steganography (HLSB)," *International Journal of Security, Privacy and Trust Management*, vol. 1, no. 2, pp. 1-11, 2012.

[7] K. Dasgupta, J. K. Mondal, and P. Dutta, "Optimized video steganography using genetic algorithm (GA)," in *International Conference on Computational Intelligence: Modeling, Techniques and Applications (CIMTA'13)*, vol. 10, pp. 131–137, 2013.

[8] M. E. Eltahir, L. M. Kiah, and B. B. Zaidan and A. A. Zaidan, "High rate video streaming steganography," in *IEEE International Conference on Information Management and Engineering (ICIME'09)*, pp. 550-553, 2009.

[9] C. S. Hsu and S. F. Tu, "Finding optimal LSB substitution using ant colony optimization algorithm," in *IEEE Second International Conference on Communication Software and Networks (ICCSN'10)*, pp. 293-297, 2010.

[10] S. D. Hu and K. T. U, "A novel video steganography based on non-uniform rectangular partition," in *IEEE 14th International Conference on Computational Science and Engineering (CSE'11)*, pp. 57-61, 2011.

[11] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T.S. Ho, and K. H. Jung, "Image steganography in spatial domain: A survey," *Signal Processing: Image Communication*, vol. 65, pp. 46-66, 2018.

[12] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26–34, 1998.

[13] N. M. S. Kafri and H. Y. Suleiman, "Bit-4 of frequency domain-DCT steganography technique,"

in *The First International Conference on Networked Digital Technologies, Ostrava, Czech Republic*, pp. 286-291, 2009.

[14] Y. Kakde, P. Gonnade, and P. Dahiwale, "Audio-video steganography," in *International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS'15)*, pp. 1-6, 2015.

[15] H. M. Kelash, O. F. A. Wahab, O. A. Elshakankiry, and H. S. El-sayed, "Hiding data in video sequences using steganography algorithms," in *International Conference on ICT Convergence (ICTC'13)*, pp. 353-358, 2013.

[16] R. J. Mstafa and K. M. Elleithy, "A highly secure video steganography using Hamming code (7, 4)," in *IEEE Conference on Systems, Applications and Technology (LISAT'14)*, pp. 1-6, 2014.

[17] A. Ouaarab, B. Ahiod, and X. S. Yang, "Discrete cuckoo search algorithm for the travelling salesman problem," *Neural Computing and Applications*, vol. 24, no. 7-8, pp. 1659–1669, 2014.

[18] R. Paul, A. K. Acharya, V. K. Yadav, and S. Batham, "Hiding large amount of data using a new approach of video steganography," in *The Next Generation Information Technology Summit*, pp. 337-343, 2013.

[19] M. Pazarci and V. Dipcin, "Data embedding in scrambled digital video," *IEEE Eighth International Symposium on Computers and Communication (ISCC'03)*, vol. 1, pp. 498-503, 2003.

[20] J. Qin, Y. Luo, X. Xiang, Y. Tan, and H. Huang, "Coverless image steganography: A survey," *IEEE Access*, vol. 7, pp. 171372-171394, 2019.

[21] A. J. Raphael and Dr. V. Sundaram, "Cryptography and steganography - A survey," *International Journal of Computer Technology and Applications (IJCTA'11)*, vol. 2, no. 3, pp. 626–630, 2011.

[22] F. Sadeghi, M. K. Rafsanjani, and F. Z. Kermani, "Hiding information in image by compound metaheuristic algorithm PSO-SA," *International Journal of Computer Science and Artificial Intelligence*, vol. 3, no. 4, pp. 125-133, 2013.

[23] Y. Shang, "A new invertible data hiding in compressed videos or images," in *IEEE Third International Conference on Natural Computation (ICNC'07)*, vol. 5, pp. 576-580, 2007.

[24] A. P. Sherly and P. P, Amritha, "A compressed video steganography using TPVD," *International Journal of Database Management Systems (IJDMS'10)*, vol. 2, pp. 67-80, 2010.

[25] M. Shrivastava, R. Ranjanand, and S. Kumari, "Video steganography using pixel intensity value and LSB technique," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 3, no. 2, pp. 287– 290, 2015.

[26] Z. H. Wang, C. C. Chang, and M. C. Li, "Optimizing least-significant-bit substitution using cat swarm optimization strategy," *Information Sciences*, vol. 192, pp. 98–108, 2012.

[27] K. Wang, H. Zhao, and H. Wang, "Video steganalysis against motion vector-based steganography by adding or subtracting one motion vector value," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 741-751, 2014.

[28] C. Xu, X. Ping, and T. Zhang, "Steganography in compressed video stream," in *IEEE First International Conference on Innovative Computing, Information and Control (ICICIC'06)*, vol. I, pp. 269-272, 2006.

[29] P. Yadav, N. Mishra, and S. Sharma, "A secure video steganography with encryption based on LSB technique," in *IEEE International Conference on Computational Intelligence and Computing Research (ICCIC'13)*, pp. 436-440, 2013.

[30] X. S. Yang and S. Deb, "Cuckoo search via Lévy flights," in *World Congress on Nature and Biologically Inspired Computing (NaBIC'09)*, pp. 210-214, 2009.

Biography

Dieaa I. Nassr He is a lecturer at Ain Shams University and received Ph. D. in cryptography from Ain Shams University in 2016. His research interests include cryptography, information security, DNA-based coding, discrete mathematics, finite fields, Boolean functions, lattice-based cryptography, and computational number theory.

Sohier M. Khamis She is a professor of computer science at Ain Shams University. Her research interests include various fields such as algorithms, graph theory, artificial intelligence, information hiding, and machine-learning.

Detection and Prevention of Jellyfish Attacks Using kNN Algorithm and Trusted Routing Scheme in MANET

Zulfiqar Ali Zardari[1], Jingsha He[1,2], Muhammad Salman Pathan[1], Sirajuddin Qureshi[1], Muhammad Iftikhar Hussain[1], Fahad Razaque[1], Peng He[2], and Nafei Zhu[1]

(Corresponding author: Nafei Zhu, Peng He)

Faculty of Information Technology, Beijing Engineering Research Center for IoT Software and Systems[1]
Beijing University of Technology, Beijing 100124, China
College of Computer and Information Science, China Three Gorges University[2]
Yichang, Hubei 443002, China
(Email: znf@bjut.edu.cn, hpeng@ctgu.edu.cn))

(Received Sept. 17, 2019; Revised and Accepted Jan. 6, 2020; First Online Feb. 15, 2020)

Abstract

Mobile ad hoc networks (MANETs) are surrounded by various vulnerabilities and attacks due to open medium, dynamic topology, limited energy, and absence of central control. In MANET, each attack has different behavior and aftermaths. DoS attack is one of the serious attacks in MANET, which disturbs the normal routing process. Jellyfish (JF) attack is a type of DoS attack in MANET, whose dynamic behavior makes it quite difficult to detect such attacks. In this paper, we propose a technique to detect the jellyfish attack in MANET. The proposed technique combines the authentication and trustworthiness of nodes and the kNN algorithm for the identification of jellyfish attacks in which each and every node calculates the primary and secondary trust values to detect the attacking node by the recommendation of neighboring nodes and trust metrics. The kNN algorithm separates the jellyfish nodes from other legitimate nodes based on the differences in their behavior. The proposed technique would then pick reliable nodes by the hierarchical trust assessment property of nodes to perform packet routing. The experiment shows that the proposed technique could decrease delay and increase the throughput of the network by avoiding jellyfish nodes.

Keywords: Jellyfish Attack; kNN Algorithm; MANET; Trusted Node; Trust Value

1 Introduction

Significant advances in the accessibility of wireless networks in some handheld devices such as laptops, smartphones, personal digital assistants, tablets, and wearable devices have been noted over the previous few years [2,26]. Wireless communication technology is available everywhere, *i.e.*, hotels, railway stations, bus stops, even small stores and shops where individuals surf the internet. In MANET, these portable devices connect with the internet wirelessly and provide a fast and easy way of commination. MANETs are considered as a communication network in which nodes are communicating with each other without fixed infrastructure [18]. It operates without any centralized server or base station. In MANET, all mobile nodes operate in a self-organized manner and nodes are connected through radio waves and communicate in an open medium. Nodes have full freedom to move arbitrarily in the network, so the topology of the network is highly dynamic. Nodes continuously cooperate to create a dynamic path to transfer data packets. When the mobile nodes are not in the same communication range the intermediates nodes play a key role in transmitting data packets to the destination node [22, 24]. Each node should be responsible for receiving and forwarding data packets therefore; data packets can reach their destination without hiccups in MANET. During the communication of nodes, routing information can be modified by the attacker node. In MANET, different parameters are changed (*e.g.*, due to the movement of nodes topology changes rapidly, link failure, absence of central control, and limited memory space) are the currents problems in the normal working circumstances. The above-mentioned parameters are challenging and intimidating tasks for routing protocols of MANET. Some parameters, *i.e.*, delay and movement of nodes (mobility) ignored [17, 25]. Under certain conditions, some nodes may move from the communication range, and the newly joining node can be part of the routing process. Since the transmission range of nodes is short, the communication of nodes depends on multi-hops fashion. MANET can intelligently manage all

kinds of topological modifications as well as faulty routing issues by the network re-configuration method. As any node can leave the network any time, which causes link breakage and communication stops. In which case nodes immediately sends a request for a new routing path to continue the communication. During communication, when a node leaves the network causes link breakage, impacted nodes can quickly request for fresh routes within seconds to continue network transmission. This problem may trigger some delay, but the network stays operational and usually works [11,13]. Generally speaking, MANETS are extremely susceptible to many malicious attacks due to the following reasons.

1) In the absence of centralized management for authenticating newly joining nodes and no central mechanism is authorizing the nodes to enter or leave the network.

2) The communication of nodes depends on multi-hop fashion.

3) The topology frequently changes because of the mobility of nodes.

4) Nodes have very limited resources in terms of battery and memory [4,7,8,10,12,16].

A critical issue in MANET is relying on intermediate nodes when functioning in a highly dynamic environment. A malicious node can easily eavesdrop into the network, particularly in wireless communication scenarios, and capture the data packets or even delay the communication. All layers, particularly the network and transport layer, are susceptible to severe attacks that influence the general MANET operational situations without rigorous safety methodologies. Video conferencing, HTTP, FTP are the applications of TCP, and UDP relies on end to end communication, but the performance affected by jellyfish attack during transmission. On the other hand, TCP doesn't perform well because nodes are changing their positions in the network [1].

1.1 Jellyfish Attack

Jellyfish attack lies in the category of Denial of Service (DoS) attack in MANET [23]. Like a black hole attack, it is also considered a passive attack. Detection Jellyfish attack is difficult because it obeys all rules of protocol. Jellyfish attack introduces at the network layer, but it interrupts the process of the transport layer. Jellyfish attacker node monitors both path-finding and packet sending, but it attacks in the packet sending process. Closed-loop, *i.e.*, TCP, is the main target of the Jellyfish attack. Jellyfish attack keeps compliance with control and information protocols to enable extremely difficult duties of detection and prevention to perform. Jellyfish attack creates a delay between data packets in the network [21].

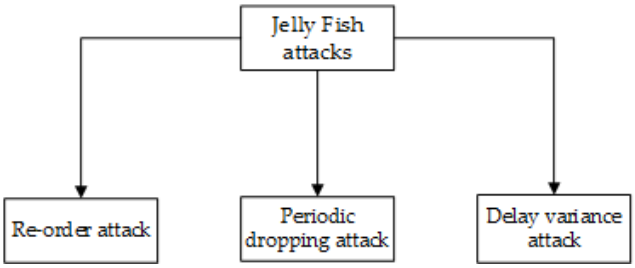


Figure 1: Types of jellyfish attacks

1.1.1 Jellyfish Reordering Attack

Due to multipath routing and route changes in MANET, such type of attacks frequently happens as the name implies that Jellyfish attacker (JF) node re-order the packets instead of FIFO before forwarding to the targeted node. Due to this acknowledgment of re-ordered packets receive late, and source node retransmits the packets again, which degrades the network throughput.

1.1.2 Jellyfish Periodic Dropping Attack

In this dropping attack, an attacker node might discard all data packets or some portion, *e.g.*, ten packets from 100 packets for a certain period during communication. As a consequence, the target node does not receive the data packets on time and not in proper shape. Because of congestion network throughput decreases, the reason is the jellyfish node drops data packets.

1.1.3 Jellyfish Delay Variance Attack

In this attack, an attacker node egotistically introduces a delay in packets that are transmitted over in particular intervals without changing the packet orders. Due to this collision occurs in the network. As a result, it affects the network performance through congestion [9].

In this paper, we propose a defense mechanism against the jellyfish Attack, which depends on trusted base routing and machine learning classifiers. Because of its malicious behavior, the jellyfish attack is difficult to identify as compared to another wireless attack. Such type of attacks causes a delay which degrades the throughput of the network. In the proposed method, node property-based trust calculations being performed. As a consequence, it is largely protected by selecting reliable routes and trusted node before transmitting packets in MANET. The proposed technique is extremely effective in detecting and preventing jellyfish attacks.

1.2 Problem Statement

It is a complex task to identify the solution to the Jellyfish attack in MANETs. The jellyfish attack decreases network performance in terms of all metrics due to its malicious behavior. That's why machine learning comes to solve this issue. The proposed technique uses a kNN

algorithm-based method in our paper to identify malicious nodes observing by the quality of packets delivered at the targeted node. Also, observing complicated actions of the nodes, protocols acquires and becoming effective in periodic intervals is a truly practical approach. In MANE, it is essential to provide a secure route to all nodes for the transformation of data packets. Meanwhile, if the attacker node comes and disturbs the network operations and the network efficiency will be degraded are presented follows:

1) Jellyfish (JF) attacking node re-orders packets to cause enormous delay, which disturbs the legitimate nodes to get access from other nodes on the communication channel.

2) The JF node creates delays during transmission of data packets, causing the network throughput to decrease.

3) The JF node drops data packets in a particular time interval, which causes loss of information so that important information may not reach the destination on time.

1.3 Contribution/Novelty

Our contributions in this paper are summarized as follows:

1) We propose a prominent technique for the detection of jellyfish nodes using machine learning classification kNN algorithm and trusted nodes in the network. The proposed technique identifies the malicious nodes by observing their behavior in MANET.

2) In the proposed technique, only trusted nodes participate in the routing process so that there is very little chance for delay or for packet drop. Furthermore, no extra computation, processing or hardware is required for the network except communicating with neighboring nodes.

3) The proposed technique is different from existing solutions [21, 22] in that it provides accurate detection of jellyfish in the dense network. The difference between the proposed technique and other mechanisms is that the new technique uses the kNN algorithm to identify jellyfish nodes, and only legitimate (trusted) nodes can participate in the routing process.

4) Simulation results show that the proposed technique achieves high accuracy rate in the detection of jellyfish nodes, making it efficient according to the requirement of MANET. This initiative could enhance packet delivery, reduce average delay, reduce packet loss, and enhance the general efficiency of MANET.

The rest of the paper is organized as follows. Section 2 presents related work. Section 3 describes the proposed technique in detail. Section 4 presents the experiments work and an analysis of the results as compared to other similar techniques. Finally, Section 5 concludes this paper.

2 Related Work

DoS attacks have remarkable consideration by the researcher community in recent years. Numerous solutions presented by various researchers, but most of the solutions concentrate solely on the path discovery or information transmission phase to mitigate the jellyfish attack. Many solutions produce high routing overhead and complexity in the network. Also, many mechanisms did not use any attacking model to assess the network's efficiency. Some previous works and their drawbacks are presented as follows:

Kumar *et al.* [15] proposed an algorithm based on the friendship of the nodes for the detection and prevention of jellyfish attacks in MANET. The friendship algorithm is an extended version of the direct trust detection (DTD) algorithm. In this algorithm, every node maintains a friendship, malicious, and monitoring tables of the neighbor nodes. Each node shares the information of their friend node and malicious nodes with their friend nodes to assess the behavior of nodes correctly. The friendship algorithm blacklists and isolates those mobile nodes from the network that execute malicious operations deliberately. The friendship algorithm decreases the probability of blacklist legitimate nodes.

Garg *et al.* [5] proposed an improved version of the AODV routing protocol to detect the malevolent node in MANET. This protocol works in such a way that after several time intervals each node sends a standard broadcast packet and checks which node is between its adjacent nodes delays the packet's threshold value by more than one time. This threshold value relies on the parameters of the network, such as node processing time, connection delay, etc., as well as considering delay owing to the large quantity of channel traffic. The drawback of this protocol is its broadcast (JFPkt) packets, which increase routing overhead in the network.

Bhawsar *et al.* [3] proposed a technique based on watcher nodes in MANET. The authors have analyzed the AODV routing protocol's efficiency with and without the JF attacker node. In the network, there are some watcher nodes deployed to sense the rushing packets sent by the JF node. Watcher nodes identify the JF attacker node and sink the rushing packets and prevent these packets in the network. Simulation results compared with AODV, AODV with JF attack, and AODV with prevention from JF attack. The drawback of this proposed is watcher nodes energy. Due to the deployment of extra nodes (watcher nodes) in the network, the overhead routing increases, ultimately, the efficiency of the network decreases.

Kumar [14] presented a simulation-based study of JF delay variance attacks for video streaming in MANET.

The simulation performed with many scenarios using AODV and OLSR routing protocols. In both protocols, the number of nodes varies (25-50 nodes) to show the performance of delay, throughput, and network load in the simulation. In the simulation, the JF attack affects MANET performance. It observed that the OLSR routing protocols have less effect as compared to AODV routing protocols. The drawback of the proposed study is, it is a pure simulation-based solution with assumptions for video streaming, and there is no attack model is used in the simulation.

Priyanka *et al.* [20] proposed an algorithm to detect the jellyfish attack in MANET. In this algorithm, only trusted nodes are considered in the network. Every node calculates trust in a specific time to identify the behavior of the neighboring node or legitimate node. The proposed uses the DTD algorithm; trust values (0-1) are stored and monitored in the routing table. These trust values are used to detect neighboring node behavior. If any node is not transmitted, the data packets will be added to the blacklist, in particular, the time interval. If a particular node exceeds the threshold value in blacklisted, then a former node of the JF node starts a path discovery that eliminates previously detected JF node from the path discovery process. The drawback of this proposed is the validation process; it increases delay and creates computational complexity in the network.

Pooja *et al.* [19] proposed an approach to detect and prevent the JF attack based on network load, sending, receiving time of data packets. In the proposed approach, if the sending and receiving time exceeds the threshold value, then delay happens because of the jamming of packets. If the network load if it exceeds the threshold value, then it confirms the JF node is present somewhere in the route. Simulation results are deployed for 25 nodes to check the network metrics. The main drawback of this approach is legitimate node didn't respond in a particular time interval due to a link failure or battery power, then the proposed approach mark that node as JF attacker node. Additionally, there is no attack model used in the simulation.

Gayathri *et al.* [6] proposed a solution to mitigate the JF attack and black hole attack in MANET. This approach depends on five factors signal strength (SS), packet success rate (PSR), packet failure rate (PFR), energy level (EL), time factor (TF). The node is having the highest trust value among all the neighbors chosen after the assessment of these variables. This happens until it reaches the destination. Once the neighbors assessed, the AODV routing protocol uses a trusted node network to move the packets to the location. The drawback of this proposed solution is assumptions, and trust calculation is very complex to understand

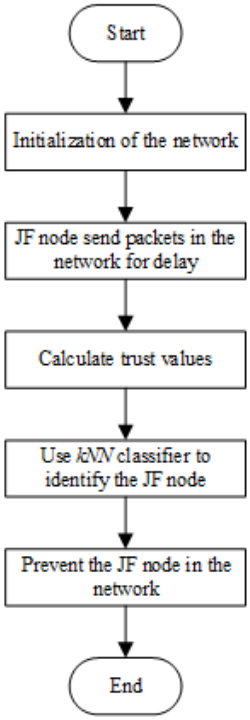


Figure 2: Flowchart of the proposed technique

3 The Proposed Methodology

To combat the jellyfish attack, we proposed a technique that detects and prevent jellyfish attack based on trust evolution and trusts nodes. Consequently, the JF attack selects reliable nodes during the path discovery phase. The proposed technique depends on two main factors, *i.e.*, trust and behavior of the nodes. To evaluate packet-forwarding behavior, the proposed technique uses the kNN algorithm. Meanwhile only trusted nodes can participate in the routing process and if any JF node is present in the network kNN algorithm identify by their trusted metrics. In order to detect the JF attack proposed technique utilizes trust calculation, trust metrics values. The proposed technique detects the JF attack with high accuracy with minimum routing overhead.

3.1 Trust Calculation

Trust calculation is a very important factor in detecting and prevention JF node because during transmission, JF node changes in its behavior. Trust calculation depends on the trust metrics of the node. Every node determines the trust values of the adjacent node if they are the same radio range in the network. Moreover, time is also a very important factor because of the behavior of nodes changes with time when the communications occur among the nodes. Trust supplied by adjacent nodes is calculated by prior node previous experience and endorsements. The previous experience here refers to the node's behavior that depends on various elements, which are primary trust (PT) and secondary trust (ST). PT is

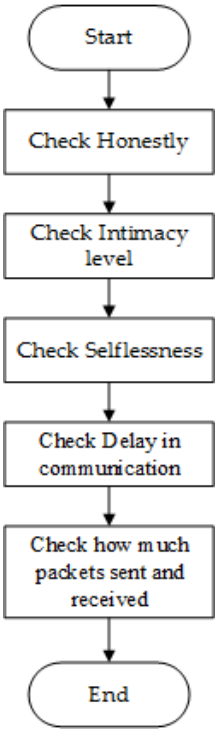


Figure 3: Flowchart of the primary trust

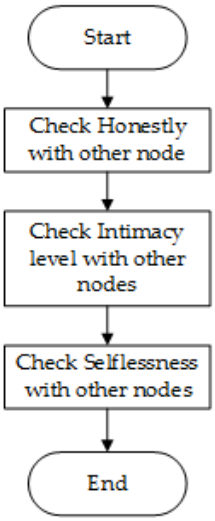


Figure 4: Flowchart of secondary trust

directly involved with the source and the corresponding node whereas secondary trust (ST) is calculated by the recommendations of neighboring nodes.

Primary trust (PT): At this stage, trust is directly involved between source and corresponding node depend on the PT trust metrics. When a source node sends RREQ packet to the corresponding node to checks honestly, intimacy level, selflessness with it, additionally, how much delay created, packets sending, and receiving time of that corresponding node.

Secondary trust (ST): At this stage, trust is calculated by recommendations from other nodes based on the previous history of nodes. When a source wants to know the secondary trust evaluations of a particular node, it asks the recommendations of other nodes. It checks the honestly, intimacy level, selflessness with other nodes.

In the proposed technique, PT and ST trust values are calculated by the following figure. Here node 1 is a source node that has primary trust with node two and secondary trust with remaining nodes and so on.

3.1.1 Node Behavior using kNN Algorithm

In this paper, we have used a machine learning well know algorithm called kNN. The reason for selecting kNN is to differentiate the JF nodes from the network. kNN algorithm is dependent on supervised learning and is very helpful for predicting of attacks and vulnerabilities in any data set [36] In our proposed kNN applies to every node

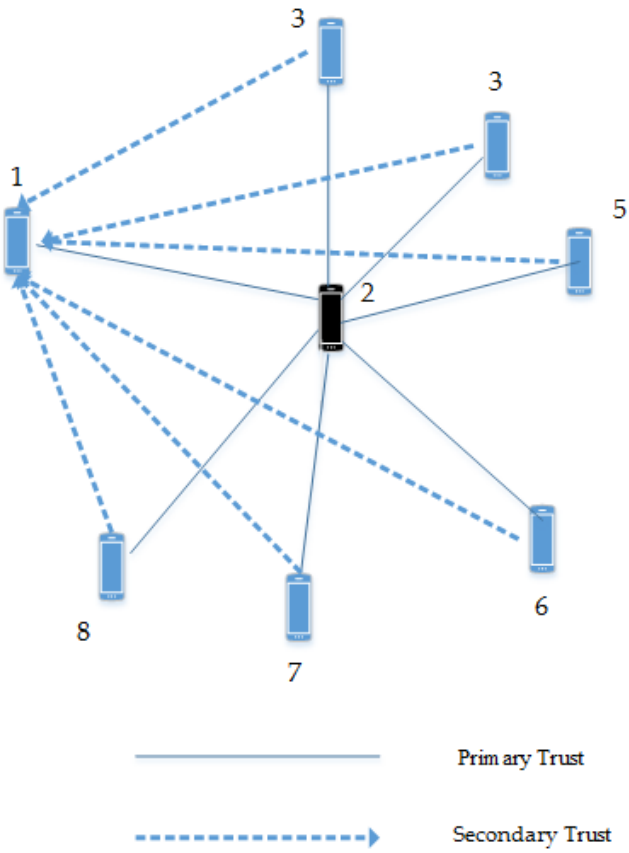


Figure 5: Primary and secondary trust

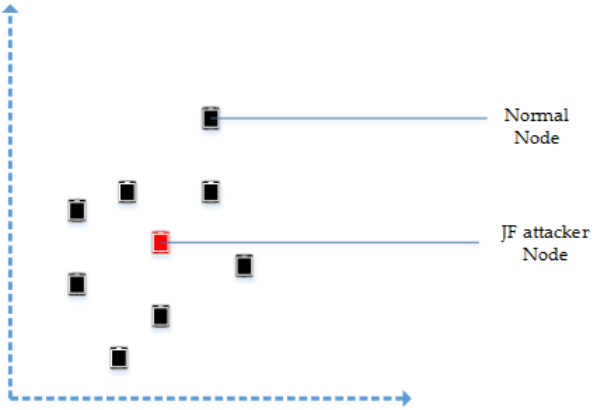


Figure 6: Identification of JF using kNN algorithm

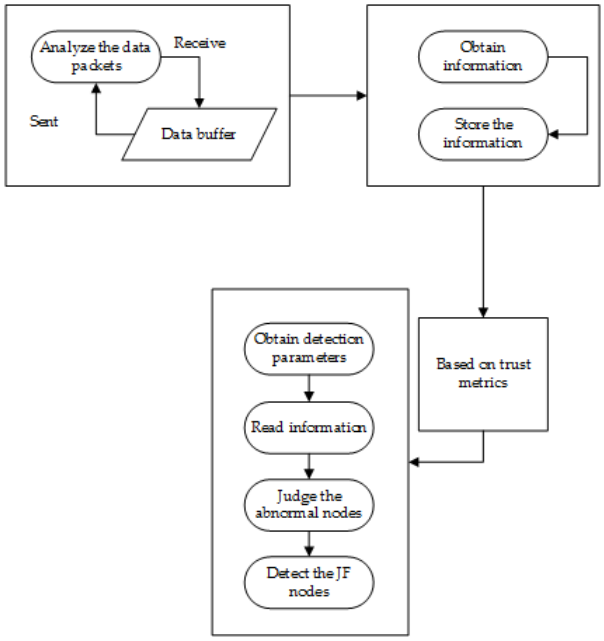


Figure 7: Schematic diagram of the kNN

in the network to classify the JF attack, which is less complex. In kNN, nodes are unable to alter their behavior, and if any changes occur, it notified instantly, and the node will leave the routing route. The basic idea is if, in the network, most of the nodes having the same type and behavior belongs to the same category (normal nodes). If the nodes having malicious behavior and are not satisfies the trust metrics are treated as malicious nodes. In general, the JF attacker node creates a delay or drop and rearranged packets to disturb the communication; as a result, the performance of the network decreases. If the JF attacker node creates such type of malicious behavior, then the intermediate node notifies about malicious behavior to source node via secondary trust. All activities done by JF attacker nodes are monitored by direct source or intermediate nodes. With the help of kNN, the classifier detects the JF attacker node by their trust metrics. Generally, legitimate nodes have normal behavior and similar features. Therefore attacker node's behavior can easily be distinguished.

3.2 Attack Model

The attack model involves all three kinds of jellyfish attacks. In the JF-reordering attack, some of the packets are reordered by the recipient node. In the JF-periodic drop attack, the intruder node rejects certain packets during the communication phase over a defined period, and the sender will enter the timeout ultimately. As the packet frequency dropped by the attacker node rises, the throughput reduces. The malevolent node delays the packets selfishly in JF- delay variance attack, resulting in more collision and heavier traffic. The congestion will happen in the network owing to the delay variance thereby reducing the throughput of the network owing to delayed congestion detection.

3.3 Detection Model

In order to detect the jellyfish attack, different tests are conducted using the NS-2 simulator. During communication, a disturbance occurs because of jellyfish attacks such as creates delay, drop packets or re-order the packets. Because JF nodes are different from legitimate nodes, such malicious behavior of JF node can easily be identified using kNN algorithm. The kNN algorithm detects the jellyfish nodes using primary and secondary trust values. These trust values are stored in the routing table before sending data packets to the destination. Legitimate nodes receive and send data packets on time and have a good intimacy level (honestly) with source node. Because legitimate nodes deliver data packets on time, doesn't hide their identity and have honest with all node whereas jellyfish nodes are not trustworthiness with the other nodes in the network. First, it observes data packets sending and receiving time if any node takes a long time to deliver the data packets. Then the route is suspicion may be JF attacker node is present in the route. Secondly, the corresponding node observes whether the JF nodes forwarding the data packets to the destination or dropping the data packets. Additionally, check the honestly and selflessness with other nodes if the node is misbehaving during communication then it confirms the JF attack.

Nevertheless, the jellyfish node possesses dishonesty, creates delay, and drop packets during communication. When these all actions are processed by the kNN algorithm it identifies and differentiates the legitimate nodes and jellyfish attacker nodes from the network. In this way, jellyfish nodes can easily be detected and prevented from the network. After the detection of jellyfish nodes, only trusted nodes can be part of the routing process with very little chance of drop and delay.

Table 1: Simulation values

Parameters	Value
Network Simulator	(NS-2.35)
Network area	800*800 m
Normal nodes	80
Mobility model	Random Walk mobility
Simulation time	800 sec
MAC type	802.11
Traffic type	Constant bitrate (CBR)
Traffic Agent	UDP
Packet size	512 bytes
Mobility of nodes	0.5-0.1 m/s
Network density	20,40,60,80 nodes

4 Experiment and Analysis

In this section, simulation results and their metrics values are shown Figures 5, 6, 7, and 8. To check the performance of the proposed technique, a well knows (NS-2.35) simulation is used to carry out the results with of 800*800 m area in the network. AODV routing protocol is used to perform communication between nodes. The following parameters are taken to test the proposed technique on MANETs to determine its viability to detect the jellyfish attack.

4.1 Packet Delivery Ratio

Table 2 shows the PDR values of native AODV, AODV under jellyfish (JF), and proposed technique. The PDR of normal AODV is lowest under attack, especially when the network is dense, *i.e.*, the number of nodes increased. As the number of nodes increases, more false replies rebroadcasted by the malicious node. The PDR result of normal AODV is highest because of no any malicious node in the network. In the proposed technique, PDR is higher than AODV under attack but meager lower than normal AODV.

4.2 Throughput

Table 3 shows the throughput values of native AODV, AODV under JF, and proposed technique. The throughput of AODV under attack is slightly decreasing as the malicious nodes are present in the network and periodically sending false replies. A huge amount of false replies causes congestion in the network. It leads to delay and drop the data packets, which effects the PDR and throughput. The throughput of normal AODV is highest because there are no malicious nodes to disturb the network. The throughput of the proposed technique is less than normal AODV and slightly lower than AODV under attack.

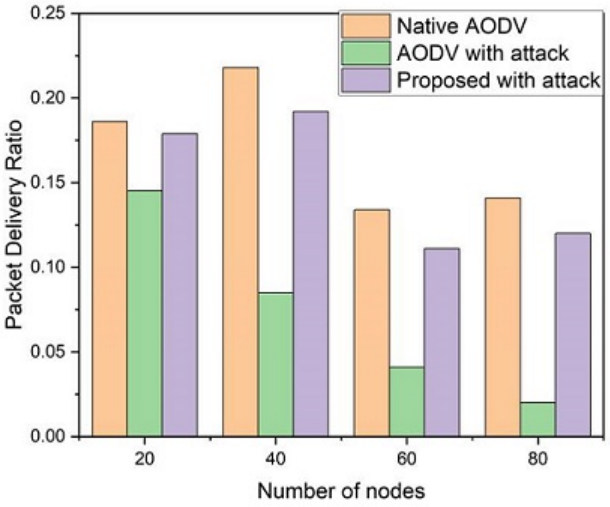


Figure 8: Packet delivery ratio

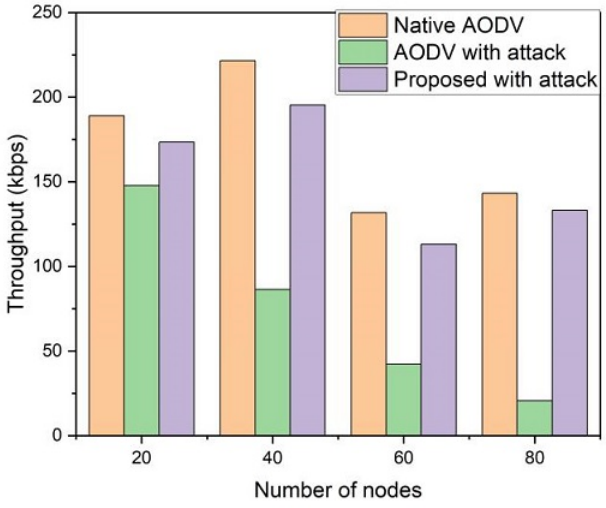


Figure 9: Throughput

Table 2: The packet delivery ratio values

Number of nodes	Native AODV	AODV under JF	Proposed under JF
20	0.186	0.145	0.179
40	0.218	0.085	0.192
60	0.134	0.041	0.111
80	0.141	0.020	0.125

Table 3: Throughput values

Number of nodes	Native AODV	AODV under JF	Proposed under JF
20	189.2	147.8	173.4
40	221.5	86.35	195.4
60	131.8	42.21	113.1
80	143.2	20.64	133.2

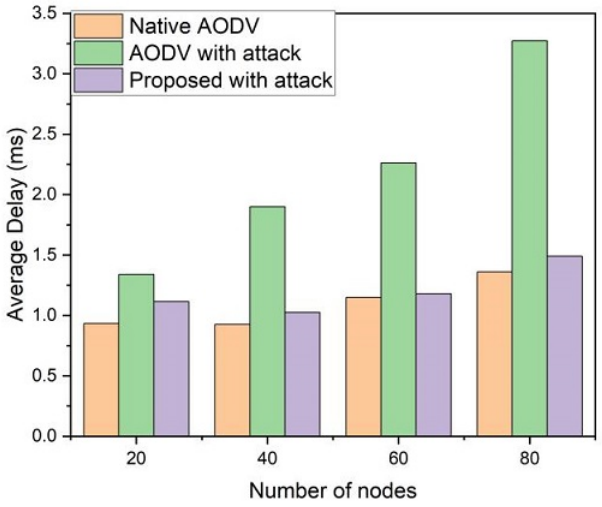


Figure 10: Average delay

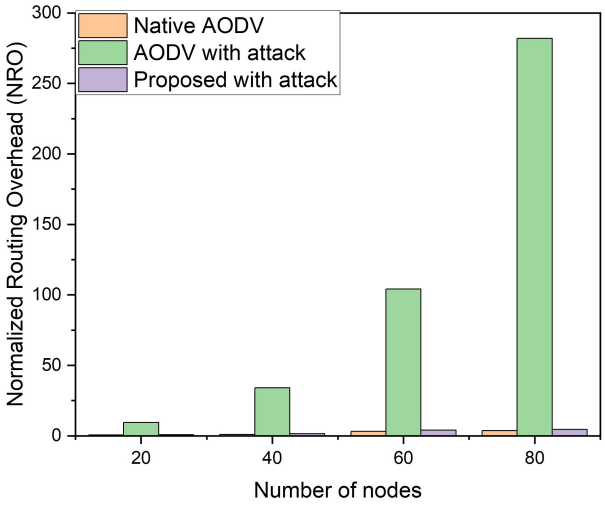


Figure 11: Normalized routing overhead

4.3 Average Delay

Table 2 shows the Average delay values of native AODV, AODV under JF, and proposed technique. The delay of AODV under attack is increasing as the number of nodes are increasing. Malicious nodes create congestion in the network. Therefore packets are delayed to reach the destination, which increases the delay. In normal AODV, there is the lowest delay found because there are no malicious nodes in the network. In the proposed technique, the delay is lower than ADOV under attack; the reason is it detects the malicious node and mitigates from the network. But as compared to the normal ADOV delay of the proposed technique is slightly high because in normal AODV it finds the short for communication.

4.4 Normalized Routing Overhead

Table 2 shows the routing overhead values of native AODV, AODV under JF, and proposed technique. The routing overhead of normal AODV under attack increases as the nodes increases in the network. The reason is malicious nodes send more false replies, which increase the number of routing packets as the number of nodes increases in the network. The routing overhead of normal AODV is lowest because there are no malicious nodes. The routing overhead of the proposed technique is lower than AODV under attack and slightly higher than normal AODV.

5 Conclusion

In this paper, we presented a new technique to detect and combat the jellyfish attack in MANET. In general, MANETs are facing various attacks; each attack has dis-

Table 4: Average delay values

Number of nodes	Native AODV	AODV under JF	Proposed under JF
20	0.934	1.339	1.104
40	0.926	1.899	1.024
60	1.149	2.262	1.18
80	1.361	3.272	1.49

Table 5: Average delay values

Number of nodes	Native AODV	AODV under JF	Proposed under JF
20	0.61	9.42	0.88
40	0.92	34.14	1.49
60	3.13	104.2	4.08
80	3.67	281.9	4.61

tinct behaviors and consequences. The jellyfish attack is considered one of the most dangerous attacks in MANET, which degrades the efficiency of the network. In our proposed technique, the source node seeks the trust from neighboring nodes. The trust assessment based on the node's intimacy with the corresponding nodes. Two types of trusts are calculated in the proposed technique of primary trust and secondary trust. In primary trust, the source node checks direct trust with the corresponding node. While in the secondary trust, the source node asks for recommendations from neighboring nodes for the corresponding node. After the calculating of trust, based on that trust the kNN algorithm identifies the jellyfish attacker node from the behavior of the node calculated in terms of the trust. The proposed technique was validated using the NS-2 simulator and compared with other techniques, *i.e.*, native AODV, AODV with jellyfish attack by different metrics such as throughput, PDR, dropped packet proportion, and delay. The simulation results showed that the proposed technique is better than AODV under jellyfish attack in all metrics throughput, PDR, average delay, and routing overhead. Whereas in simple AODV routing protocol, there is no attack, so the performance of native AODV better than AODV under attack and proposed technique.

For upcoming research, this can be enhanced by incorporating profound deep learning technology and some more parameters to the detection of another type of attacks and improve the efficiency of the network in MANET.

Acknowledgment

The work in this paper has been supported by the National Natural Science Foundation of China (61602456).

References

[1] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh, and F. AlTamimi, "Security challenges and attacks in dynamic mobile ad hoc networks manets," in *IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT'19)*, pp. 28–33, 2019.

[2] Z. Ali-Zardari, J. He, N. Zhu, K. H. Mohammadani, M. S. Pathan, M. I. Hussain, and M. Q. Memon, "A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in manets," *Future Internet*, vol. 11, no. 3, p. 61, 2019.

[3] D. Bhawsar and A. Suryavanshi, "Collaborative intrusion detection and prevention against jellyfish attack in manet," *International Journal of Computer Applications*, vol. 129, no. 13, pp. 37–42, 2015.

[4] A. M. Desai and R. H. Jhaveri, "Secure routing in mobile ad hoc networks: A predictive approach," *International Journal of Information Technology*, vol. 11, no. 2, pp. 345–356, 2019.

[5] S. Garg and S. Chand, "Enhanced aodv protocol for defence against jellyfish attack on manets," in *International Conference on Advances in Computing, Communications and Informatics (ICACCI'14)*, pp. 2279–2284, Sep. 2014.

[6] D. Gayathri and S. J. Raman, "Pltrust AODV: Physical logical factor estimated trust embedded AODV for optimised routing in manets," in *The 4th International Conference on Advanced Computing and Communication Systems (ICACCS'17)*, pp. 1–5, 2017.

[7] S. Gurung and S. Chauhan, "A dynamic threshold based approach for mitigating black-hole attack in manet," *Wireless Networks*, vol. 24, no. 8, pp. 2957–2971, 2018.

[8] S. Gurung and S. Chauhan, "Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in manet," *Wireless Networks*, vol. 25, no. 3, pp. 975–988, 2019.

[9] R. Kapoor, R. Gupta, S. Jha, R. Kumar, *et al.*, "Adaptive technique with cross correlation for lowering signal-to-noise ratio wall in sensor networks," *Wireless Personal Communications*, vol. 105, no. 3, pp. 787–802, 2019.

[10] D. Khan and M. Jamil, "Study of detecting and overcoming black hole attacks in manet: A review," in *International Symposium on Wireless Systems and Networks (ISWSN'17)*, pp. 1–4, 2017.

[11] A. T. Kolade, M. F. Zuhairi, E. Yafi, and C. L. Zheng, "Performance analysis of black hole attack in manet," in *Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication*, pp. 1, 2017.

[12] V. K. Kollati, "IBFWA: Integrated bloom filter in watchdog algorithm for hybrid black hole attack detection in manet," *Information Security Journal: A Global Perspective*, vol. 26, no. 1, pp. 49–60, 2017.

[13] V. H. Kshirsagar, A. M. Kanthe, and D. Simunic, "Trust based detection and elimination of packet drop attack in the mobile ad-hoc networks," *Wireless Personal Communications*, vol. 100, no. 2, pp. 311–320, 2018.

[14] S. Kumar, "Implementation of delay variance attack using video streaming in manet," *Optik-International Journal for Light and Electron Optics*, vol. 127, no. 6, pp. 3303–3307, 2016.

[15] S. Kumar, K. Dutta, and A. Garg, "FJADA: Friendship based jellyfish attack detection algorithm for mobile ad hoc networks," *Wireless Personal Communications*, vol. 101, no. 4, pp. 1901–1927, 2018.

[16] M. Mistry, P. Tandel, and V. Reshamwala, "Mitigating techniques of black hole attack in manet: A review," in *International Conference on Trends in Electronics and Informatics (ICEI'17)*, pp. 554–557, 2017.

[17] F. Muchtar, A. H. Abdullah, S. Hassan, and F. Masud, "Energy conservation strategies in host centric networking based manet: A review," *Journal of Network and Computer Applications*, vol. 111, pp. 77–98, 2018.

[18] M. S. Pathan, J. He, N. Zhu, Z. A. Zardari, M. Q. Memon, and A. Azmat, "An efficient scheme for detection and prevention of black hole attacks in AODV-based manets," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 1, pp. 243–251, 2019.

[19] B. P. Pooja, M. P. Manish, and B. P. Megha, "Jellyfish attack detection and prevention in manet," in *The Third International Conference on Sensing, Signal Processing and Security (ICSSS'17)*, pp. 54–60, 2017.

[20] R. Priyanka and P. Ramkumar, "Trust based detection algorithm to mitigate the attacker nodes in manet," in *International Conference on Computing Technologies and Intelligent Data Engineering (ICCTIDE'16)*, pp. 1–6, 2016.

[21] D. J. Rahman, F. Ahmed, and S. Rashid, "An analysis on security threats of black-hole and jellyfish attacks in mobile ad-hoc network using http traffic," *International Journal Of Research And Engineering*, vol. 6, no. 2, pp. 575–579, 2019.

[22] D. K. Sharma, A. Sharma, J. Kumar, *et al.*, "Knnr: K-nearest neighbour classification based routing protocol for opportunistic networks," in *Tenth International Conference on Contemporary Computing*, pp. 1–6, 2017.

[23] G. Suseendran, E. Chandrasekaran, and A. Nayyar, "Defending jellyfish attack in mobile ad hoc networks via novel fuzzy system rule," in *Data Management, Analytics and Innovation*, pp. 437–455, 2019.

[24] M. Umar, A. Sabo, and A. A. Tata, "Modified cooperative bait detection scheme for detecting and preventing cooperative blackhole and eavesdropping attacks in manet," in *International Conference on Networking and Network Applications (NaNA'18)*, pp. 121–126, 2018.

[25] S. Yadav, M. C. Trivedi, V. K. Singh, and M. L. Kolhe, "Securing AODV routing protocol against black hole attack in manet using outlier detection scheme," in *The 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON'17)*, pp. 1–4, 2017.

[26] Z. A. Zardari, J. He, N. Zhu, M. S. Pathan, M. Q. Memon, M. I. Hussain, P. He, and C. Chang, "A scheme for finding and blocking black hole nodes in mobile ad hoc networks," *International Journal of Network Security*, vol. 21, no. 6, pp. 1021–1030, 2019.

Biography

Zulfiqar Ali Zardari received his B.E. and M.E degree from Mehran University of Engineering and Technology Jamshoro in Sindh, Pakistan 2011 and 2015 respectively. Currently, he is doing PhD in Faculty of Information Technology, Beijing University of Technology, China. He has published more than 10 research papers as a first and co-author in international journals. His research interest area is Mobile ad hoc networks, Wireless Communications, Information Security, sensor network security, Computer Networks and Network Security.

He Jingsha received his B.S. degree from Xi'an Jiaotong University in Xi'an, China and his M.S. and PhD degrees from the University of Maryland at College Park in the USA. He is currently a professor in the School of Software Engineering at Beijing University of Technology in China. Professor He has published over 170 research papers in scholarly journals and international conferences and has received nearly 30 patents in the United States and China. His main research interests include information security, network measurement, and wireless ad hoc, mesh and sensor network security.

Muhammad Salman Pathan received his PhD the Faculty of Information Technology, Beijing University of

Technology, China. He received his B.E. and M.E degree from Mehran University of Engineering and Technology, Pakistan in 2011 and 2014 respectively. Currently, he is doing Post Doc at the Faculty of Information Technology, Beijing University of Technology, China. His research interest is Wireless Communications, Information Security, sensor, network security.

Sirajuddin Qureshi did his bachelor's degree in Computer Sciences from Quaid-e-Awam University of Engineering, Science & Technology, Pakistan. Afterwards, he pursued his Master's in Information Technology from Sindh Agricultural University Tandojam, Pakistan. Currently he is pursuing PhD in Information Technology at Beijing University of Technology, China. He has nine research publications to his credit as main author and co-author, which featured national and international journals and conferences. His research areas include but not limited to Network Forensics Analysis, Digital Forensics, Cyber security, Computer Networks and Network Security.

Muhammad Iftikhar Hussain is currently doing PhD at Faculty of Information Technology, Beijing University of Technology, China. His Research interests include Information Security, Hybrid Cloud Computing Security and Hybrid Cloud Computing Infrastructure and Design. He did his MS Computer Science from Superior University Lahore with distinction. He served as Senior System Engineer in Television and Media Network (Express-News) for four years, one year as System Administrator in 92NEWSHD and two years as Lecturer / Advisor IEEE SUL in Superior University Lahore.

Fahad Razaque received his B.S from Sindh University Jamshoro and M.S degree from Indus University Karachi in Sindh, Pakistan 2011 and 2017 respectively. Currently, he is doing PhD in Faculty of Information Technology, Beijing University of Technology, China. He has published six research papers as a 1st and co-author in national and international journals. His research interest area is Mobile ad hoc networks, Wireless Communications, Information Security, sensor network security, Computer Networks and Network Security in machine learning.

Peng He is currently a professor in the College of Computer and Information Technology, China Three Gorges University. He graduated from Hefei University of Technology in 1986 with a bachelor's degree in computer application and from Xi'an Jiaotong University in 1989 with a Master's degree in computer software. He worked in National Time Service Center, Chinese Academy of Sciences (CAS) and participated in 30 research projects, including the seventh national 5-year-plan, the rehearsal of 'eight-five' project from the State Bureau of Surveying and Mapping, CAS youth fund project, Hubei technology research-program, etc. Prof. He won the western young scientist's achievement award and the third class award of technology advancement by CAS and the Hubei teaching research achievement award, etc. and has been an Education Information Expert of Ministry of Education and a Standing Director of Education Information Technology, Hubei. Prof. He has published over 50 journal papers, some of which have been indexed by EI and ISTP. His research focuses on transmission protocols and information security based on network time synchronization.

Nafei Zhu received her B.S. and M.S. degrees from Central South University, China in 2003 and 2006, respectively, and her PhD degree in computer science and technology from Beijing University of Technology in Beijing, China in 2012. From 2015 to 2017, she was a postdoc and an assistant researcher in the Trusted Computing and Information Assurance Laboratory, State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences in China. She is now on the Faculty of Information Technology at Beijing University of Technology. Dr Zhu has published over 20 research papers in scholarly journals and international conferences (16 of which have been indexed by SCI/EI/ISTP). Her research interests include information security and privacy, wireless communications and network measurement.

Detect Fast-Flux Domain Name with DGA through IP Fluctuation

Hongling Jiang[1] and Jinzhi Lin[2]
(Corresponding author: Hongling Jiang)
School of Information Management, Beijing Information Science and Technology University[1]
No. 12 Xiaoying East Qinghe Road, Haidian District, Beijing, 10092, China
Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences[2]
Shenzhen, 518055, China
(Email: hellojhl@163.com)
(Received July 28, 2019; Revised and Accepted Dec. 6, 2019; First Online Apr. 8, 2020)

Abstract

Many malicious networks use the DNS domain names to protect their networks. One of the techniques is the fast-flux, which maps many IP addresses to a domain name and uses recruited hosts to redirect users' requests. Fast-flux is powerful in concealing the malicious networks, thus it is widely used by attackers. Although diverse approaches have been proposed to detect the fast-flux domain names, they still suffer from limitations like either having heavy computations or be easy to be noticed by attackers. According to our research, the IP addresses of the fast-flux domain name are unstable. In this paper, we design a metric called domain score to measure the IP fluctuation. Meanwhile, we consider the feature of the domain name itself. A system called FluDD is proposed to detect the fast-flux domain name with DGA (Domain Generation Algorithm). Experimental results show that FluDD can achieve good performance and the true positive rate reaches to 99.6% and the minimal false positive rate is 0.

Keywords: DGA; DNS; Domain Name; Fast-Flux; IP Fluctuation

1 Introduction

In the early stage, malicious codes usually contained the IP addresses of the C&C servers. Once the IP addresses are detected, the whole malicious network could be shut down. Nowadays DNS (Domain Name System) plays an important role in the Internet [14]. Many internet applications depend on DNS. At the same time, many attacks leverage DNS to be more resilient [29], such as botnet, APT (Advanced Persistent Threat), spam, phishing sites and so on [12, 22, 28]. Attackers use DNS to obtain the IP addresses of their servers. In this way, the attackers can hide their Command and Control (C&C) servers [16].

Recently, many attackers use the so-called fast-flux technique to protect their networks. The fast-flux technique maps a set of IP addresses to a domain name. When a client query a domain name, a set of different IP addresses will be returned. These IP addresses are corresponding to host agents, which redirect the client's requests to the real C&C servers. Ordinary, the IP set includes hundreds and thousands of IP addresses, which can be changed rapidly. Even some of them could be detected as malicious and blocked, many others can still provide services. The fast-flux technique makes it hard to detect the malicious networks. Besides, some attackers use DGA (Domain Generation Algorithm) to generate domain names. The fast-flux combined with DGA makes it more difficult to detect the malicious domain names.

Many solutions have been proposed to detect the fast-flux domain names, but they still face different problems. Existing approaches can be divided into two categories: passive and active. For example, the passive DNS traffic based approaches suffer from heavy computations and privacy concerns [10]. Some of the active approaches may be noticed by attackers as they send requests to the servers regularly. Meanwhile, some approaches would be escaped by attackers [13].

To detect fast-flux with DGA, in this paper, we propose a lightweight approach without causing the attacker's attention. Our paper makes the following contributions.

1) We propose an approach to detect fast-flux with DGA, called FluDD. The approach not only focuses on the fast-flux technique but also pays attention to domain names generated by DGA.

2) We put forward an idea of using IP fluctuation to detect the fast-flux domain names. We propose a metric called domain score to measure the IP fluctuation.

3) Our approach does not need to analysis a large amount of DNS traffic data and the cost of compu-

tation is low. It does not send messages to rival's servers, so it's hard to be found by attackers.

The remainder of this paper is organized as follows. Section 2 introduces the background. Section 3 gives the related work. Section 4 describes our approach in detail. Section 5 shows experimental evaluations and results. Section 6 concludes the paper.

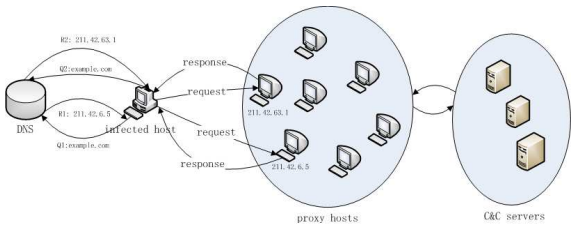


Figure 1: The fast-flux service network

2 Background

2.1 Legitimate Dynamic DNS

Dynamic DNS maps a domain name to a set of IP addresses. Some applications, such as RRDNS (Round-Robin DNS) and CDN (Content Delivery Network), utilize dynamic DNS for various purposes.

RRDNS uses dynamic DNS for load balancing, load distribution and fault tolerance [27]. RRDNS is usually utilized in large networks where the traffic is hard to be managed by a single server. DNS servers are used to distribute traffic to different physical servers. Each time a DNS request is made, one of the IP addresses is returned in a Round Robin fashion. In this way, the traffic will be distributed among the different IP addresses. Round Robin DNS depends on the TTL (Time to Live) values. The smaller the TTL is, the faster these IP addresses are rotated.

CDN utilizes dynamic DNS to serve content to end-users with high availability and high performance [11]. CDN is a globally distributed network consisting of a lot of servers. When an end-user requests the content of CDN, some algorithms are used to choose a server providing the content with high performance. When optimizing for performance, the location may be chosen for serving content. In CDN, small TTL value is required for changing the IP addresses.

2.2 Fast-Flux Service Network

Attackers use the fast-flux service network to organize their compromised hosts, improve their networks availability and hide their service infrastructures. The schematic diagram of the fast-flux service network is shown in Figure 1. In the fast-flux service network, hundreds of IP addresses are mapped to a domain name [3]. When the fast-flux domain name is inquired, different IP addresses are returned, and the IP addresses change frequently. These IP addresses act as agents to redirect the communication between the infected hosts and the C&C servers [19]. If one of the IP addresses is blacklisted, the C&C server can continue to serve through other IP addresses. It's easy to add new C&C servers by adding new IP addresses to the set of IP addresses. This dynamic DNS technique makes it difficult for intrusion detection systems to find the C&C servers hiding behind proxy hosts. To change the IP addresses for a certain fast-flux domain name, the TTL (Time To Live) in the DNS response record is usually small.

2.3 DGA (Domain Generation Algorithm)

Domain Generation Algorithm (DGA) is based on seeds to create a pseudo-random string [7]. DGA can generate a large number of domain names periodically. These domain names can be used to contact the C&C servers [8, 26]. Malware can generate thousands of domain names and contact a few of them every day, which makes them difficult to be eliminated. To be more robust, a malware can use lots of DGAs.

3 Related Work

As many attackers use the fast-flux domain name to protect their networks, it is important to detect fast-flux domain names for preserving network security. Many researchers proposed a lot of fast-flux domain name detection approaches. These approaches can be divided into two categories: Passive and active.

The passive approaches firstly collect DNS traffic including DNS requests and responses and then analyze DNS traffic to recognize the behavior features of the fast-flux domain name.

Ammar [2] presented a fast-flux hunter system to detect the fast-flux service network. The system used an evolving fuzzy neural network algorithm. It collected DNS traffic and analyzed features of the fast-flux service network. The algorithm depends on 14 features, including the number of DNS queries, average packet size, average TTL, the number of TLDs, duration, and so on.

Zhou *et al.* [30] collected DNS traffic of a real campus network. They used Passive DNS to detect the fast-flux domain. Passive DNS constructs 18 domain name features, which are categorized into diversity, time, growth and relevance. They trained a random forest to detect fast-flux domain name.

Leyla *et al.* [15] designed an EXPOSURE system to detect malicious domain names. They extracted 15 features grouped into 4 categories. The feature set includes time-based features, DNS answer based features, TTL based features, and domain name based features. They trained the J48 decision tree algorithm using different combina-

tions of feature sets. The trained classifier is used to detect malicious domain names.

The active approaches query the domain names for their IP addresses. Domain names are obtained from various sources, such as spam, social networks. For each domain name, the detection system queries DNS to get the records of the domain name information. By analyzing the answers, the detection system will judge whether a domain name is benign or malicious.

Hsu *et al.* [10] proposed a fast-flux domain detector (FFDD), which depends on the response time differences. It is based on the observation that the response time of subsequent requests to the same flux bot should be more fluctuating. The FFDD firstly obtains the IP addresses of a domain name, then sends requests to the same client host and measures their response time. The domain name with more fluctuating response time will be judged as the fast-flux domain name.

Davor *et al.* [5] presented a method which measures the network delay, document fetch delay and processing delay of the hosts related to a domain name. The method is based on the observation that the compromised network could have a larger delay than normal one.

Zang *et al.* [27] proposed a fast-flux service network detection scheme which identifies fast-flux botnet with DGA domain names. To detect fast-flux botnet, they measured the features of domain names, such as entropy of location, attribution of the resolved IP, the spatial service relationship. Meanwhile using a machine learning algorithm, the scheme could detect fast-flux service with DGA domain names.

Shi *et al.* [25] proposed a malicious domain name detection approach based on extreme learning machine (ELM). They apply ELM to classify domain names based on multiple features. These features can be divided to four categories, including construction-based, IP-based, TTL-based, and WHOIS-based.

4 Principle and Architecture of FluDD

This section introduces the differences between malicious and benign domain names, and then presents the IP fluctuation of the fast-flux domain name. A new metric called domain score is designed. Besides, this section describes the architecture of FluDD.

4.1 Differences Between Malicious and Benign Domain Names

Attackers use malicious domain names to hide their C&C servers. Malicious domain names use the fast-flux technique, meanwhile, the domain names are generated through DGA. In the fast-flux service network (FFSN), a domain is mapped to a lot of different IP addresses. Each IP address corresponds to a distinct bot. The attackers recruit these bots continually. Each time a client queries the fast-flux domain name, different IP addresses will be returned. In this way, the real malicious servers are hard to be detected.

However, some benign applications also use dynamic DNS techniques, such as RRDNS and CDN. Both of the fast-flux service networks and the benign networks use dynamic DNS, they have similar features, such as small TTL value. However, the difference between the fast-flux and the benign domain name is obvious. In the fast-flux service network, the bots are compromised hosts. The connections between bots and C&C servers are unreliable. To solve this problem, attackers recruit lots of bots and frequently change the mapping between the fast-flux domain names and IP addresses [13]. On the other hand, RRDNS and CDN have their own servers. These servers are used for load balancing. The IP addresses mapping to the benign domain name are stable.

To demonstrate the IP fluctuation of benign and malicious domain names in practice, we select a benign domain name "microsoft.com" and a malicious domain name "2e22e99ot9oofkkkf.000webhostapp.com" randomly from our dataset described in Section 5. We use the "dig" command to obtain the IP addresses from type "A" response of the domain name. Figure 2 and Figure 3 are "dig" command results of "microsoft.com" and "2e22e99ot9oofkkkf.000webhostapp.com", respectively. For each domain name, "dig" command is executed twice. The second "dig" command is executed after the TTL of the response expires. From the results, we can see that the IP addresses of "microsoft.com" are stable, and the IP addresses of "2e22e99ot9oofkkkf.000webhostapp.com" change after TTL expires.

Furthermore, some fast-flux domain names also use DGA to generate domain names. For the fast-flux with DGA domain names, we focus on the features of the domain name itself. Because the domain names are generated automatically and usually not readable, they are different from benign ones in many ways. One of the most obvious features is the length of the domain name. Benign domain names are short to be remembered by users easily, while DGA domain names are not. So the length of DGA domain names usually longer than benign ones. To reduce the computational complexity, we only compute one feature of the domain name, the length.

4.2 IP Fluctuation and Domain Score

The above analysis shows that the IP fluctuation is the main distinction between the fast-flux and the benign domain names. The IP addresses of fast-flux domain names are more fluctuating than benign ones.

Figure 4 illustrates the IP fluctuation of benign domain and fast-flux domain, respectively. The horizontal axises represent the time elapses since the domain name is queried. In the benign network, there are more IP overlaps in different time windows. On the contrary, in the fast-flux service network, there is less or even no IP over-

```
jhl@senslot2:~$ dig microsoft.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> microsoft.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10019
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1024
;; QUESTION SECTION:
;microsoft.com.                 IN      A

;; ANSWER SECTION:
microsoft.com.          1008    IN      A       13.77.161.179
microsoft.com.          1008    IN      A       40.76.4.15
microsoft.com.          1008    IN      A       40.112.72.205
microsoft.com.          1008    IN      A       40.113.200.201
microsoft.com.          1008    IN      A       104.215.148.63

;; Query time: 44 msec
;; SERVER: 125.31.58.114#53(125.31.58.114)
;; WHEN: Sat Jul 20 12:49:59 CST 2019
;; MSG SIZE  rcvd: 122
jhl@senslot2:~$ dig microsoft.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> microsoft.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30968
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1024
;; QUESTION SECTION:
;microsoft.com.                 IN      A

;; ANSWER SECTION:
microsoft.com.          1562    IN      A       13.77.161.179
microsoft.com.          1562    IN      A       40.76.4.15
microsoft.com.          1562    IN      A       40.112.72.205
microsoft.com.          1562    IN      A       40.113.200.201
microsoft.com.          1562    IN      A       104.215.148.63

;; Query time: 45 msec
;; SERVER: 125.31.58.114#53(125.31.58.114)
;; WHEN: Sat Jul 20 15:31:20 CST 2019
;; MSG SIZE  rcvd: 122
```

Figure 2: "dig" command results of "microsoft.com"

```
jhl@senslot2:~$ dig 2e22e99ot9oofkkkf.000webhostapp.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> 2e22e99ot9oofkkkf.000webhostapp.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11967
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1024
;; QUESTION SECTION:
;2e22e99ot9oofkkkf.000webhostapp.com. IN        A

;; ANSWER SECTION:
2e22e99ot9oofkkkf.000webhostapp.com. 3583 IN CNAME us-east-1.route-1.000webhost.awex.io.
us-east-1.route-1.000webhost.awex.io. 57 IN A   145.14.145.196

;; Query time: 47 msec
;; SERVER: 125.31.58.114#53(125.31.58.114)
;; WHEN: Sat Jul 20 15:41:27 CST 2019
;; MSG SIZE  rcvd: 130
jhl@senslot2:~$ dig 2e22e99ot9oofkkkf.000webhostapp.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> 2e22e99ot9oofkkkf.000webhostapp.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25214
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1024
;; QUESTION SECTION:
;2e22e99ot9oofkkkf.000webhostapp.com. IN        A

;; ANSWER SECTION:
2e22e99ot9oofkkkf.000webhostapp.com. 3490 IN CNAME us-east-1.route-1.000webhost.awex.io.
us-east-1.route-1.000webhost.awex.io. 31 IN A   145.14.144.171

;; Query time: 234 msec
;; SERVER: 125.31.58.114#53(125.31.58.114)
;; WHEN: Sat Jul 20 15:43:01 CST 2019
;; MSG SIZE  rcvd: 130
```

Figure 3: "dig" command results of "2e22e99ot9oofkkkf.000webhostapp.com"

lap in different time windows.

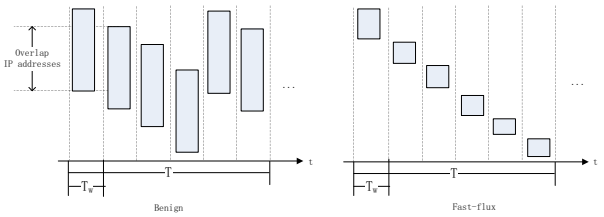


Figure 4: IP fluctuation of benign and fast-flux domain name

To measure the IP fluctuation, we design a metric, called domain score. Assume that during the total time T, a domain name d is queried several times in each time window. Denote T_w as the size of time window. For a time window t_i, the IP addresses set P_i^d is mapped to domain name d. Assume two adjacent time windows, t_i and t_j, the IP addresses sets are P_i^d and P_j^d. The similarity $J(P_i^d, P_j^d)$ between P_i^d and P_j^d is calculated using the Jaccard coefficient [20], shown as Equation (1).

$$J(P_i^d, P_j^d) = \frac{|P_i^d \cap P_j^d|}{|P_i^d \cup P_j^d|} \tag{1}$$

The domain score $S(d)$ is the average $J(P_i^d, P_j^d)$ during T. $S(d)$ is calculated as Equation (2).

$$S(d) = \frac{\sum_{i=1,j=i+1}^{i=L-1,j=L} J(P_i^d, P_j^d)}{L * (L-1)/2} \tag{2}$$

Where L is the number of time windows during T. We use domain score $S(d)$ of a domain name d as a feature to decide whether the domain name d is a benign domain name or a fast-flux one. A domain name with a low domain score is more likely to be a fast-flux domain name.

Moreover, compared to fast-flux domain names, most benign domain names are mapped to less distinct IP addresses during a period of time. Thus, in our system, if a domain name with distinct IP addresses less than 5, we judge it as a benign domain name.

We compute the domain score in two steps. Firstly, we extract the DNS response records periodically. Every T_p time, each domain name is queried for their response records(T_p is less than or equal to T_w). The total time of the DNS querying process is T. In this way, we could obtain the IP addresses mapped to each domain name in different times. It is shown in Algorithm 1. Secondly, we assign a time window ID $twID$ for each record and compute the domain score of each domain name, according to Equation (2). It is shown in Algorithm 2.

Algorithm 1 Extracting DNS response records

Input:

1) *domainList* (the list of domain names)
2) T (the total time of the DNS querying process)
3) T_p (the time interval between two consecutive DNS queries)

Output: *responseList* (DNS response records)
Begin
$starttime$ = current time
$nowtime$ = current time
while $nowtime - starttime \leqslant T$ **do**
  $qtime$ = current time
  for each d in *domainList*: **do**
    $responseList$ = response records of d
    for each r in $responseList$: **do**
      store the $r(d, IP, TTL, queryTime, \dots)$
    end for
  end for
  $nowtime$ = current time
  $qduration = nowtime - qtime$
  sleep$(T_p - qduration)$
  $nowtime$ = current time
end while
End

Algorithm 2 Computing domain score

Input:

1) *domainList* (the list of domain names)
2) $responseList$ ($d, IP, TTL, queryTime, \dots$)
3) T_w (the size of time window)

Output: $S(d)$ of each domain d in *domainList*
Begin
for each d in *domainList* **do**
  sort the $responseList$ of d by $queryTime$
  $twID = 1$
  t_1 = mininum $queryTime$ of all the records
  $t_2 = t_1 + T_w$
  for each r in $responseList$ **do**
    if $queryTime \geqslant t_1$ and $queryTime < t_2$ **then**
      assign $twID$ to r
    else
      update t_1 and t_2
      $twID = twID + 1$
    end if
  end for
  collect all the IP in each time window $twID$
  compute $J(P_i^d, P_j^d)$ between two adjacent time window, t_i and t_j
  compute domain score $S(d)$
end for
End

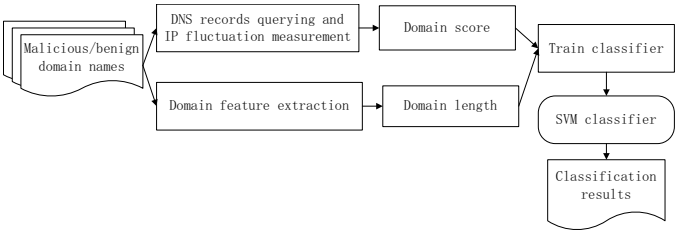


Figure 5: Architecture of FluDD

4.3 FluDD Architecture

Figure 5 gives the architecture of FluDD. Firstly, a set of domain names, which may include malicious and benign domains, are collected. Then, for each domain name, the domain score and length are computed. In order to compute the domain score, a DNS querying process is conducted, as described in Algorithm 1. After that, the IP fluctuation of each domain name is measured, and the domain score is computed according to Equation (2), as described in Algorithm 2. The features of the fast-flux domain names with DGA are quite different from benign domain names as the domain names are generated automatically by algorithm and are not readable. To reduce the cost of calculation, we only extract the length of domain names as a feature. Finally, the SVM (Support Vector Machine) classifier is trained. In the detection phase, we use the trained SVM classifier to detect malicious domain names.

5 Experimental Design and Results

5.1 Datasets

We use two datasets. One is the benign domain names according to Alexa top 500 sites on the web [1]. The other is the malicious domain names collected from sources [9, 17, 23]. After obtaining the malicious domain name datasets, for each domain name, we compute its number of distinct IP addresses. The first 500 malicious domain names with the largest number of different IP addresses are selected.

5.2 Experimental Environment

The proposed approach was implemented in Python3.5.2. The experiments were performed on a server with 4 cores Intel (R) Xeon (R) CPU @ 2.60 GHz. The operating system is 64 bit Ubuntu16.04. The database used is MySQL5.5.55.

5.3 Experimental Settings

1) The parameters for extracting DNS response records.

The total time of the DNS querying process, T in Algorithm 1, is 10 days. The time interval between two DNS queries, T_p in Algorithm 1, is 1 hour.

2) The parameters for computing domain score.

Because the number of distinct IP addresses of the benign domain name is usually small, in our experiments, we filter the domain name with distinct IP addresses less than 5. Thus lots of benign domain names will not be analyzed and the computation is reduced. The size of time window, T_w in Algorithm 2, is a variable parameter. In the following experiments, we first set T_w to 24 hours to see the distribution of features. Then, T_w is set to 1, 6, 12, 18 and 24 hours respectively to evaluate the performance of FluDD.

5.4 Performance Measurement

The performance of FluDD is evaluated using the following metric: True Positive Rate (TPR), False Positive Rate (FPR), Precision (Pr), F-Measure (Fm) [4,18,21]. TPR, FPR, Pr, and Fm are calculated as shown in Equations (3), (4), (5), and (6) respectively.

$$TPR = \frac{TP}{TP+FN} \quad (3)$$

$$FPR = \frac{FP}{FP+TN} \quad (4)$$

$$Pr = \frac{TP}{TP+FP} \quad (5)$$

$$Fm = \frac{2*Pr*TPR}{Pr+TPR} \quad (6)$$

Where TP (True Positives) is the number of malicious domain names recognized as malicious ones correctly, TN (True Negatives) is the number of benign domain names recognized as benign ones correctly, FP (False Positives) is the number of benign domain names recognized as malicious ones incorrectly and FN (False Negatives) is the number of malicious domain names recognized as benign ones incorrectly.

Fm is the weighted average of TPR and Pr. The higher the values of TPR, Pr, and Fm are, the lower the value of FPR is, the better the performance of FluDD is.

5.5 Performance Evaluation

5.5.1 Distributions of Features

In this experiment, we analyzed the distributions of features of domain names, including domain score and length. The size of time window T_w is configured as 24 hours in this experiment.

There are two approaches to obtain the distribution of samples. One is the parametric approach and the other is non-parametric approach [6]. Parametric approaches, such as GMM (Gaussian Mixture Model), LE(Likelihood Estimate), need the pre-defined model and parameter estimation [24], so we use a non-parametric approach in our experiments. The representative method of the non-parametric approach is the Kernel Density Estimation (KDE). KDE use all the sample information to approximate the target probability distribution, shown as Equation (7):

$$f(x) = \frac{1}{nh}\sum_{i=1}^{n} K(\frac{x-x_i}{h}). \quad (7)$$

Where n is the number of samples. h is the smoothing parameter that controls the size of the neighborhood around x. The larger the value of h, the smoother the probability density function curve, and vice versa [6]. K is the kernel controlling the weight given to the observations x_i at each point x based on their proximity. The kernel function $f(x)$ can make the probability density function by summing all these kernel functions and dividing them by n [24].

Firstly, we analysis the Kernel Density Estimation (KDE) distribution of the single-dimensional feature, domain score and length, respectively. In our experiments, K is a Gaussian kernel function. To gain the probability density curves with different smoothness, we set h to 0.02, 0.08, 0.1 and 0.2 respectively. The KDE distributions of domain score are shown in Figure 6. The x-axises are the domain score, and the y-axises are the density of KDE. The malicious domain scores are much smaller than the benign ones, and the peak domain score is about 0.3. The domains scores of benign domain names are larger, and most of them are more than 0.4. The peak domain score of benign ones is about 0.7. As indicated in previous, the large domain scores mean small IP fluctuation. Compared to malicious domain names, the IP addresses of benign domain names are more stable.

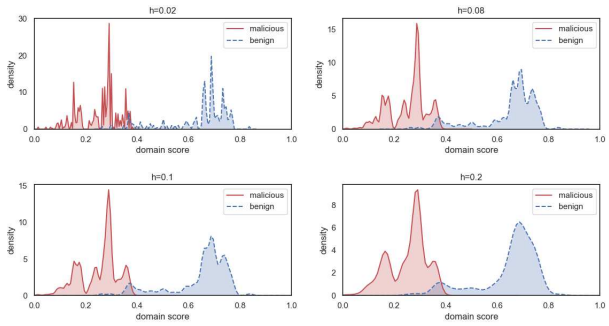


Figure 6: KDE distribution of domain score

The KDE distribution of length is given in Figure 7. The x-axises are the length, and the y-axises are the density of KDE. From Figure 7, we can see that the lengths of benign domain names are less than 20, and most of them are less than 10. However, the lengths of most malicious domain names are much larger than benign ones.

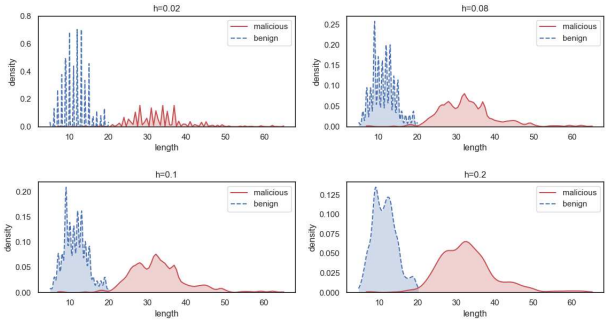


Figure 7: KDE distribution of length

Secondly, we analyze the distribution of both the two features in two-dimensional, as shown in Figure 8. As it can be seen, most of the benign and malicious domain names can be separated by the SVM classifier.

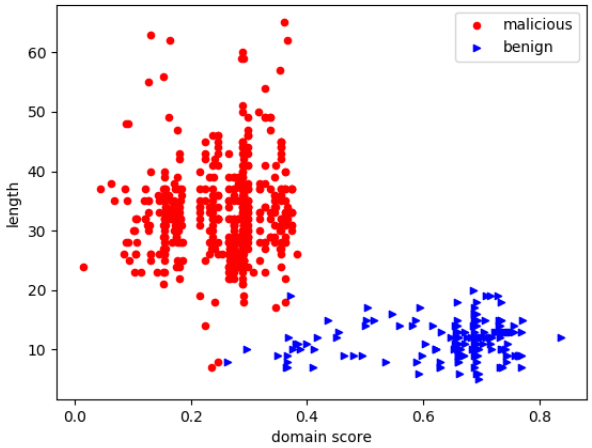


Figure 8: The distribution of two-dimensional features

5.5.2 Performance of FluDD

To achieve the best performance, we try different values of T_w. N-fold cross-validation is used to estimate the performance of the SVM classifier. In N-fold cross-validation, the dataset is partitioned randomly into N samples. The evaluations are run by N times. In each time, $N-1$ samples are selected for training and the remaining samples are used to evaluate the accuracy of the classifier. Finally, the mean value of all the results is calculated. In this experiment, N is 10 and T_w is set to 1, 6, 12, 18 and 24 hours respectively.

We analysis the Pr, Fm, and TPR in different time windows size T_w. As shown in Figure 9, all the Pr and Fm are more than 98%. When the time window size T_w is 6 and 12 hours, the Pr, Fm, and TPR achieve the maximum value, in which Pr is 100%, Fm is 99.8% and TPR is 99.6%.

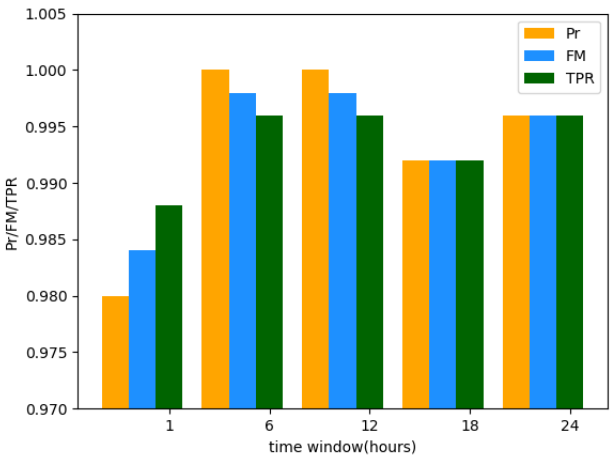


Figure 9: Pr, Fm, and TPR in different time windows sizes

FPR in different time windows size T_w are also analyzed. As shown in Figure 10, when the time window size T_w is 6 or 12 hours, the FPR is zero. From Figure 9 and Figure 10, we can see that when the time window size T_w is 6 and 12 hours, FluDD achieves the best performance.

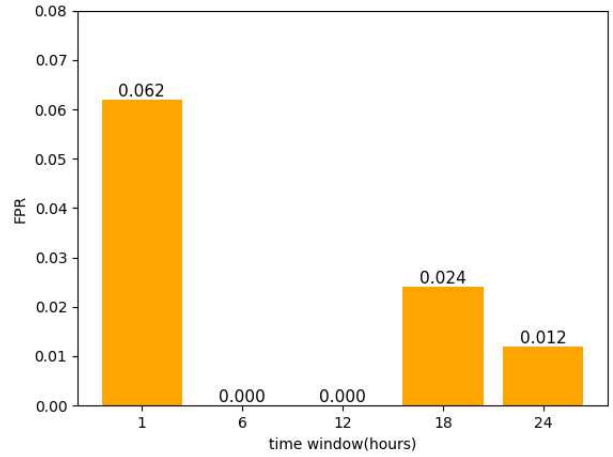


Figure 10: FPR in different time windows size

5.5.3 Discussion and Comparison

Passive fast-flux domain detection approaches need to parse and process the DNS traffic, and this brings heavy computations. While some active approaches send messages or requests to malicious servers and will attract the attention of attackers. Instead, we concern about the stability of IP addresses mapping to a domain name. IP addresses of fast-flux domain names are unstable than benign ones. Our approach utilized this phenomenon.

It is difficult for attackers to bypass the detection of FluDD. A way for attackers to escape the detection of FluDD is to make the domain score large. To do so, a

Table 1: Comparisons of different fast-flux domain detection approaches

Targets	**Hsu *et al.* [10]**	**Zeng *et al.* [27]**	**Shi *et al.* [30]**	**FluDD**
No message sending to malicious servers	No	Yes	Yes	Yes
Can detect domain name generated by DGA	No	Yes	Yes	Yes
No need of domain names generated by the same DGA	Yes	No	Yes	Yes
Fewer features to analysis	Yes	No	No	Yes

lot of stable hosts, which are Internet-connected, without anti-virus software installed and always powered on, are required. Furthermore, attackers could not recruit new hosts to scale up the fast-flux service network during the running time of the detection system. However, all the hosts used in the fast-flux service networks are controlled by dedicated persons, not attackers. It's hard for attackers to ensure most of the hosts are available. To make the fast-flux service network robust, attackers must constantly recruit new hosts to join the network. Thus, it is difficult for the attackers to make the domain score large on purpose.

Three typical related approaches for detecting fast-flux domain names are chosen to make comparisons with FluDD. As shown in Table 1, our approach is different from others and has some excellent features.

6 Conclusion

In this paper, FluDD, a system for detecting the fast-flux domain name with DGA, is proposed. We utilize the phenomenon that the IP addresses mapping to the fast-flux domain name are unstable. A new metric called domain score is designed to measure the IP fluctuation. Meanwhile, to counter the DGA domain name, the length of the domain name is considered. It is convinced that FluDD can be used to detect the fast-flux domain name with DGA. Experiments show that the true positive rate, F-measure and precision of our approach are high, and the false positive rate is low. Our approach is lightweight and requires fewer computations. Furthermore, since no information is sent to the malicious servers, it is impossible for the attacker to notice the detection. Finally, we analyze the advantages of FluDD, the possible evasion methods of attackers and make comparisons of different detection approaches. In the future, we continue to discover the features of the fast-flux domain name and combat attackers' evasion strategies.

7 Acknowledgments

This study was supported by the School Funds of Beijing Information Science and Technology University (No. 1925023).

References

[1] Alexa Internet, *The Top 500 Sites on the Web*, 2019. (`https://www.alexa.com/topsites`)

[2] A. Ammar, "Fast-flux hunter: A system for filtering online fast-flux botnet," *Neural Computing and Applications*, vol. 29, no. 7, pp. 483–493, 2018.

[3] B. Andreas, D. Alessandro, G. Wilfried, and P. Antonio, "Mining agile dns traffic using graph analysis for cybercrime detection," *Computer Networks*, vol. 100, pp. 28–44, 2016.

[4] C. Daiki, Y. Takeshi, A. Mitsuaki, S. Toshiki, M. Tatsuya, and G. Shigeki, "Domainprofiler: Toward accurate and early discovery of domain names abused in future," *International Journal of Information Security*, vol. 17, no. 6, pp. 661–680, 2018.

[5] C. Davor, S. Vlado, and D. Ivica, "Fast-flux botnet detection based on traffic response and search engines credit worthiness," *Tehnički vjesnik*, vol. 25, no. 2, pp. 390–400, 2018.

[6] Q. L. Deng, T. Y. Qiu, F. R. Shen, and J. X. Zhao, "Adaptive online kernel density estimation method (in Chinese)," *Journal of Software*, 2019. (doi: 10.13328/j.cnki.jos.005674)

[7] T. Duc, M. Hieu, T. Van, T. H. Anh, and N. L. Giang, "A LSTM based framework for handling multiclass imbalance in dga botnet detection," *Neurocomputing*, vol. 275, pp. 2401–2413, 2018.

[8] Y. Fu, L. Yu, O. Hambolu, I. Ozcelik, B. Husain, J. X. Sun, K. Sapra, and D. Du, "Stealthy domain generation algorithms," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1430–1443, 2017.

[9] hpHosts, 2019. (`http://hosts-file.net`)

[10] F. Hsu, C. Wang, C. Hsu, C. Tso, L. Chen, and S. Lin, "Detect fast-flux domains through response time differences," *IEEE Journal on Selected Areas in Communications*, vol. 32, pp. 1947–1956, Oct. 2014.

[11] L. Jeffrey, F. Qiang, and M. Tim, "Using SDN and NFV to enhance request rerouting in ISP-CDN collaborations," *Computer Networks*, vol. 113, pp. 176–187, 2017.

[12] A. Kamal, A. Ammar, and M. Ahmad, "A survey of botnet detection based on dns," *Neural Computing & Applications*, vol. 28, no. 7, pp. 1541–1558, 2017.

[13] M. Knysz, X. Hu, and K. G. Shin, "Good guys vs. bot guise: Mimicry attacks against fast-flux detection systems," in *Proceedings IEEE INFOCOM*, pp. 1844–1852, Apr. 2011.

[14] J. Kwon, J. Lee, H. Lee, and A. Perrig, "Psybog: A scalable botnet detection method for large-scale dns traffic," *Computer Networks*, vol. 97, pp. 48–73, 2016.

[15] B. Leyla, S. Sevil, B. Davide, K. Engin, and K. Christopher, "Exposure: A passive DNS analysis service to detect and report malicious domains," *ACM Transactions on Information and System Security (TISSEC'14)*, vol. 16, no. 4, p. 14, 2014.

[16] Z. Y. Liu, Y. F. Zeng, P. F. Zhang, J. F. Xue, J. Zhang, and J. T. Liu, "An imbalanced malicious domains detection method based on passive dns traffic analysis," *Security and Communication Networks*, vol. 2018, pp. 1–8, 2018.

[17] Malc0de database, 2019. (`http://malc0de.com/rss/`)

[18] S. Matija, P. J. Myrup, D. Alessandro, and R. Stefan, "A method for identifying compromised clients based on DNS traffic analysis," *International Journal of Information Security*, vol. 16, no. 2, pp. 115–132, 2017.

[19] M. Muhammad, N. Manjinder, and M. Ashraf, "A survey on botnet architectures, detection and defences.," *International Journal of Network Security*, vol. 17, no. 3, pp. 264–281, 2015.

[20] N. Natrajan and P. Suresh, "A comparative scrutinization on diversified needle bandanna segmentation methodologies," *International Journal of Electronics and Information Engineering*, vol. 10, no. 2, pp. 65–75, 2019.

[21] W. N. Niu, X. S. Zhang, G. W. Yang, J. N. Zhu, and Z. W. Ren, "Identifying APT malware domain based on mobile DNS logging," *Mathematical Problems in Engineering*, vol. 2017, pp. 9, 2017.

[22] O. Pomorova, O. Savenko, S. Lysenko, A. Kryshchuk, and K. Bobrovnikova, "Anti-evasion technique for the botnets detection based on the passive DNS monitoring and active DNS probing," in *The 23rd International Conference on Computer Networks (CN'16)*, pp. 83–95, June 2016.

[23] Risk Analytics, *Malware Domain Blocklist by Riskanalytics*, 2019. (`http://www.malwaredomains.com`) 2019.

[24] S. Sanghyun and K. Juntae, "Efficient weights quantization of convolutional neural networks using kernel density estimation based non-uniform quantizer," *Applied Sciences*, vol. 9, no. 12, pp. 2559, 2019.

[25] Y. Shi, G. Chen, and J. Li, "Malicious domain name detection based on extreme machine learning," *Neural Processing Letters*, vol. 48, no. 3, pp. 1347–1357, 2018.

[26] T. S. Wang, H. T. Lin, W. T. Cheng, and C. Y. Chen, "DBod: Clustering and detecting DGA-based botnets using DNS traffic analysis," *Computers & Security*, vol. 64, pp. 1–15, 2017.

[27] X. Zang, J. Gong, S. Mo, A. Jakalan, and D. Ding, "Identifying fast-flux botnet with AGD names at the upper DNS hierarchy," *IEEE Access*, vol. 6, pp. 69713–69727, 2018.

[28] X. D. Zang, G. Jian, and X. Y. Hu, "Detecting malicious domain names based on AGD," *Journal on Communications*, vol. 39, no. 7, pp. 15–25, 2018.

[29] Y. Zhauniarovich, I. KHALIL, T. Yu, and M. Dacier, "A survey on malicious domains detection through dns data analysis," *ACM Computing Surveys*, vol. 1, no. 1, pp. 1–35, 2018.

[30] C. L. Zhou, K. Chen, X. X. Gong, P. Chen, and H. Ma, "Detection of fast-flux domains based on passive DNS analysis (in chinese)," *Acta Scientiarum Naturalium Universitatis Pekinensis*, vol. 52, no. 3, pp. 396–402, 2016.

Biography

Hong-Ling Jiang received her Ph.D in the Computer Science College of Nankai University, Tianjin, China, in 2013. She is currently a lecturer in the School of Information Management at Beijing Information Science and Technology University, China. Her research interest focuses on Network Security, Artificial Intelligence, and the Internet of Things. She has published more than ten papers in recent years.

Jin-Zhi Lin received the Ph.D. degree in computer application from Nankai University, Tianjin, China, in 2015. Currently, he works as an assistant professor in Shenzhen Institute of Advanced Technology (SIAT), Chinese Academy of Sciences (CAS), Shenzhen, China. His research interests include cyber physical system, embedded system, internet of things and wireless communication. He has also published several peer-reviewed journal and conference papers in recent years.

An Electronic Voting Scheme Based on LUC Secret System and Secret Sharing

Hongquan Pu[1,2,3], Zhe Cui[1,2], Ting Liu[1,2,3], Zhihan Wu[1,2] and Hongjiang Du[1,2]
(Corresponding author: Hongquan Pu)

Chengdu Institute of Computer Applications, Chinese Academy of Sciences[1]
No.9, South Renmin Road, Sec.4, Chengdu 610041, China
School of Computer and Control Engineering, University of Chinese Academy of Sciences[2]
No.19(A), Yuquan Road, Shijingshan District, Beijing 100049, China
Guangxi Key Laboratory of Hybrid Computation and IC Design Analysis[3]
No.188, East University Road, Nanning 530006, China
(Email: 774149765@qq.com)
(Received Aug. 31, 2019; Revised and Accepted Dec. 6, 2019; First Online Apr. 8, 2020)

Abstract

The security of electronic voting systems is an essential factor restricting its development. This paper proposes an electronic voting scheme based on LUC secret system and secret sharing. This scheme uses LUC to verify and identify voters' identities. Furthermore, it adopts Shamir's secret sharing to divide votes into multiple secret sharings, which are shared with all vote counters. The vote counters use the homomorphism of secret sharing to perform additional operations on the secret sharings received and then recover the final result of the voting. The proposed scheme meets the security requirements of anonymity, no receipt, verifiability and fairness, and so on. At the same time, it can obtain the final result without restoring the vote of each voter and there is an optimum number of vote counters, which guarantees the efficiency of the voting process. At last, it performs the voting process hierarchically. These advantages make our method suitable for electronic voting of different scales.

Keywords:Electronic voting; LUC; Secret share; Homomorphism; Vote counters

1 Introduction

With the development of information technology, voting has been changed from paper voting to electronic voting. The security of electronic voting has always been the bottleneck restricting its development. The privacy protection in electronic voting systems has attracted more and more attention from scholars and engineers. The most important feature of electronic voting based on cryptography is to provide end-to-end verifiability. All submitted votes are published in the ciphertext. Trusted third parties can verify the results of the voting, and different voters can also verify and supervise the whole voting process. These advantages are not available to non-cryptographic electronic voting.

After Chaum [1] presented the first electronic voting scheme based on an anonymous letter channel in 1981, a large number of electronic voting schemes based on cryptography have been proposed, which can be divided into the following four categories.

The first kind of electronic voting scheme is based on a hybrid network. Encrypted votes are confused through the hybrid network, which can shield the correlation between output and input, thus achieving the purpose of protecting the vote information. Chaum's scheme [1] uses an anonymous channel to transmit votes, which is a typical voting scheme based on the hybrid network. Sako and Killian [2] proposed an obfuscation scheme based on reencryption and random permutation for voting. Neff [3] proposed a mathematical structure to shuffle the votes, which is only suitable for ElGamal encryption. Groth [4] gived a scheme to extend Neff's scheme to general homomorphic encryption in public key cryptosystem. Electronic voting scheme based on the hybrid network usually requires multiple confusion calculations, encryption and decryption operations and zero-knowledge proof. Therefore, the implementation efficiency is generally low, and it is difficult to be applied to large-scale voting activities.

The second kind of electronic voting scheme is based on homomorphic encryption. Cohen [5] in 1985 proposed the first electronic voting scheme based on homomorphic encryption, which requires all voters to vote at the same time. Cramer et al. [6] proposed a 1-out-of-many electronic voting scheme based on ELGamal encryption and zero-knowledge proof. This method needs an exhaustive search when decrypting, and it leads to a high computational cost. Damgard et al. [7] proposed a many-out-of-many electronic voting scheme based on Pailier encryp-

tion [8]. When the set of possible votes contains a large number of elements, the efficiency of this scheme is reduced sharply. Damgard, Groth and Solomonsen [9] designed a scheme to code votes by using homomorphic commitment and homomorphic encryption, which is more efficient. Chen et al. [10] proposed a receipt-free homomorphic encrypted electronic voting scheme based on semi-trust model. This scheme achieves the result of confidentiality, generalized verifiability and fairness. However, it has high requirements for the voters which is difficult to be used in practice.

The third kind of electronic voting scheme is based on the blind signature. In 1992, Fujiaka et al. [11] proposed the famous electronic voting scheme based on the blind signature (FOO scheme). This scheme achieves the security goal in large-scale electronic voting activities. However, it still exists some problems, such as the voters cannot abstain and the votes collision. The proposed scheme makes electronic voting enter a practical stage. Some electronic voting systems developed later are basically based on FOO scheme, e.g., the Sensus system of the University of Washington [12]. Shilbayeh et al. [13,14] proposed EVAPS scheme based on the blind signature and improved the scheme, both of which are based on REVS[15] and Evox-MA [16]. Fenfen Luo et al. [17] proposed a receipt-free electronic voting scheme based on FOO, which theoretically solved the problems of ballot collision and non-abstention, but still failed to achieve overall verifiability.

Shamir [18] proposed the first secret sharing scheme in 1979. This scheme is based on Lagrange difference polynomial, which is easy to implement and has high security. Many improved versions, such as the multi-stage secret sharing scheme (MSS) [19-20], have emerged to realize multiple secret sharing. The secret sharing scheme [21-22], introducing the one-way function, solves the problem of secret share reuse and improves the practicability. Benaloh et al. [23-24] began to use secret sharing in electronic voting. There are two main types of electronic voting schemes based on secret sharing: one is based on the difference method in Shamir's (t, n) threshold [25-27], the other is based on the Chinese Remainder Theorem [28-29].

This paper applies the LUC secret system to authenticate voters and Shamir's (t, n) secret sharing technology to realize the voting process. Finally, based on the homomorphism of Shamir secret sharing, the final results of voting are counted, and the feasibility and the security of our scheme are compared with other methods through security analysis.

The organizational structure of this paper is as follows. The second part introduces the information of the LUC secret system, secret share, and homomorphism of secret sharing.The third part introduces the security requirements, the composition and the form of the electronic voting system. The fourth part presents our proposed scheme. The fifth part carries on the security analysis to the proposed scheme. The last part concludes this paper.

2 Preliminaries

This part mainly introduces the knowledge needed in this paper, including: the Shamir's (t, n) secret sharing, the LUC cryptosystem, and the homomorphism of secret sharing.

2.1 Shamir's (t, n) Secret Sharing

Shamir's (t, n) secret sharing is based on Lagrange interpolation polynomials, which consists of three phases [18].

Initialization Phase

Secret Distributor (SD) randomly selects n different non-zero elements $x_1, x_2, \ldots, x_n$, Identifies each participant $P_r \in \{P_1, P_2, \ldots, P_n\}(r = 1, 2, \ldots, n)$, orders $P = \{P_1, P_2, \ldots, P_n\}$, SD and assigns x_r to the corresponding $P_r(r = 1, 2, \ldots, n)$, where the value of x_r is public.

Secret Distribution Phase

If SD intends to have a participant $P_r \in P(r = 1, 2, \ldots, n)$ sharing secret $s \in \mathbb{Z}_m(m$ is a large prime), SD randomly chooses t-1 elements $a_1, a_1, \ldots, a_n$ in $GF(q)$ and constructs t-1 polynomial, by the formula as follows:

$$f(x) = (s + \sum_{i=1}^{t-1} a_i x^i) \ mod \ q \tag{1}$$

where $q > s$ and $s = f(0)$. Then SD generates secret shares for all participants:

$$s_r = f(x_r) = (s + \sum_{i=1}^{t-1} a_i x_r^i) \ mod \ q \tag{2}$$

SD sends s_r to the corresponding participant P_r through the secure channel.

Secret Recovery Phase

Any t participants in the n participants may be set as $P_1, P_2, \ldots, P_t$, showing their secret shares, which can reconstruct polynomial $f(x)$.

$$f(x) = (\sum_{i=1}^{t} f(x_i) \prod_{j=1, j\neq i}^{t} \frac{x - x_j}{x_i - x_j}) \ mod \ q \tag{3}$$

By Ordering $x = 0$, the following formulas is obtained.

$$s = (\sum_{i=1}^{t} f(x_i) \prod_{j=1, j\neq i}^{t} \frac{-x_j}{x_i - x_j}) \ mod \ q \tag{4}$$

In Shamir'(t, n) secret sharing scheme, any secret shares of not less than t can recover secret s, and no information of s can be obtained if less than t secret shares. This secret share scheme is a one-time scheme and can only be used once in the process of secret share, because after t participants give secret shares, the secret share can be disclosed at the same time. The polynomial $f(x)$ constructed by D is also made public. This feature just meets the characteristics of electronic voting. The electronic voting scheme should be a one-time scheme; otherwise, the scheme itself will be questioned.

2.2 LUC

LUC is a double cryptosystem proposed by P.Smith [30-32]. This method uses Lucas sequence to realize encryption and decryption.

Lucas Sequence

Definition: choosing two non-negative integers P and Q, Constructing quadratic equation $x^2 - Px + Q = 0$, the two roots of the equation are:

$$x_1, x_2 = \frac{P \pm \sqrt{P^2 - 4Q}}{2} \tag{5}$$

If $P^2 - 4Q \neq 0$, then the Lucas sequence can be defined as:

$$U_n(P,Q) = \frac{x_1^n - x_2^n}{x_1 - x_2},\ n \geqslant 0 \tag{6}$$

$$V_n(P,Q) = x_1^n + x_2^n,\ n \geqslant 0 \tag{7}$$

LUC cryptosystem is only interested in $V_n(P,Q)$ sequences, Lucas sequence has the following properties:

- Let a and b be arbitrary positive integers, $V_{ab}(P,1) = V_a(V_b(P,1),1)$; The proof is available in reference [30].
- Let a and b be arbitrary positive integers, $V_b(V_a(P,1),1) = V_a(V_b(P,1),1)$.

  Proof: $V_b(V_a(P,1),1) = V_{ba}(P,1) = V_{ab}(P,1) = V_a(V_b(P,1),1)$.

LUC Cryptosystem

Let $N = pq$, for the product of two odd prime numbers, we choose an integer e and let$(e, \phi(N)) = 1$, then $(e, \phi(N)) = 1$ is an Euler function, which determines another integer d by $ed \equiv 1\ mod\ \phi(N)$. The construction method is as follows:

- Public key: N, e;
- Private key: d;
- Plaintext: P is an integer less than N;
- Ciphertext: $C = V_e(P,1)\ mod\ N$;
- Decrypt: $P = V_d(P,1)\ mod\ N$.

This paper implements voter authentication through the LUC cryptosystem.

2.3 Homomorphism of Secret Sharing

The concept of homomorphism of secret sharing is given in [33]. S is the main secret space and T is the secret sharing space corresponding to the main secret. The function $F_I : T \to S$ is the induced function of (t,n) secret sharing. This function defines the secret s based on any subset of $\{s_1, s_2, ..., s_t\}$ containing t secret shares as $s = F_I(s_1, s_2, ..., s_t)$, where $\{I = s_1, s_2, ..., s_t\}$. Definition: suppose $\oplus$ and $\otimes$ are two functions on set S and T elements, respectively. For any subset I, if there exists $s = F_I(s_1, s_2, ..., s_t)$, $s' = F_I(s'_1, s'_2, ..., s'_t)$ satisfies $s \oplus s' = F_I(s_1 \otimes s'_1, s_2 \otimes s'_2, ..., s_t \otimes s'_t)$, then it is considered that a $(t,\ n)$ secret sharing scheme has $(\oplus,\ \otimes)$ homomorphism.

According to the above definition, Shamir's $(t,\ n)$ is $(+,\ +)$ homomorphic.

The proof is as follows: suppose two participants A and B share the secret s_A and s_B with Shamir's $(t,\ n)$, For A, the secret s_A can be decomposed into multiple secret shares by the following polynomial $s_A = F_I(a_1, a_2, ..., a_t)$; for B, the secret s_B can be decomposed into multiple secret shares by the following polynomial $s_B = F_I(b_1, b_2, ..., b_t)$. The following formulas can be obtained through mathematical variations:

$$s_A + s_B = F_I(a_1 + b_1, a_2 + b_2, ..., a_t + b_t) \tag{8}$$

This indicates that Shamir's $(t,\ n)$ share sharing is $(+,\ +)$ homomorphic.

3 Electronic Voting System

This part includes the security requirements of electronic voting, the form of electronic voting and the composition of electronic voting.

3.1 Security Requirements for Electronic Voting

Fujioka et al.[11] defined seven security requirements of electronic voting, which are considered as the basic security requirements of electronic voting schemes.

1) Completeness: All legitimate and valid votes should be counted correctly.
2) Soundness: Illegal or malicious voters cannot affect or disrupt the voting process.
3) Privacy: The identity and voting information of all voters must be kept confidential.
4) Unreusability: All voters can vote only once, not many times.
5) Eligibility: All voters need to be authenticated before voting. If the authentication fails, they are not allowed to vote.
6) Fairness: Voting is fair to all, and nothing can affect the fairness of voting.
7) Verifiability: The voting results are verifiable, and no one can change the voting results.

With the emergence of new network technologies and attack methods, electronic voting needs to meet higher security requirements besides the above seven basic security requirements [34-36]:

8) Receipt-Freeness: Voters cannot prove what they voted for during the voting process.

9) Universal Verifiability: Not only can voters verify that their votes have been counted correctly, but any third parties can also verify that the results are correct

10) Coercion-Resistance: Voters cannot coerce others to prove their voting information during the voting process.

3.2 Electronic voting form

There are usually three forms of electronic voting [37] :(1)voters choose yes or no, which is only suitable for the case of 2 choosing 1; (2)voters choose one candidate from multiple candidates, and the number of candidates should be greater than 2; (3)voters choose multiple candidates from multiple candidates.

3.3 Composition of Electronic Voting

A complete electronic voting system consists of four parts [10,11,35,37-39] : voters, registration agencies, vote issuing agencies and vote counting agencies.

- Voters: Actual Participants in Voting Activities
- Registration agency: To verify the identity of voters, only when the conditions for verification specified by the Registrar are met, can the voter be eligible for voting.
- Ballot issuing agency: issuing blank votes to legitimate voters.
- Vote counting institution: statistics of the total number of votes and verification of the legitimacy of votes.

In the actual electronic voting activities, registration agency, vote issuing agency and vote count agency can merge, but also can be decomposed into multiple institutions.

Generally, a complete voting process is as follows: Voters apply to the registration agency for authentication. After the registration agency receives the application, it examines the voting qualifications of the voter. If satisfied, it will be validated successfully and become a valid voter. Otherwise, the application is rejected. Then the vote issuing agency will send the blank vote to the voter who is a valid voter. The voter fills in the blank vote after received, and then send the filled vote to the vote-counting institution, which counts the vote and publishes the final results.

4 Electronic Voting Scheme Based on LUC Secret System and Secret Sharing

The scheme consists of five agencies: voters $V_1, V_2, ..., V_m$, regulatory agency abbreviated as RA, secret distribution agency abbreviated as DA, vote counting agency abbreviated as CA, including n vote counters $C_1, C_2, ..., C_n$, verification agency recorded as PA, all of the above agencies and entities are credible, p,q are two large enough prime numbers, let $N = pq$, the LUC public key and private key of voter $V_i (i = 1, 2, ...m)$ are $\{N, e_i\}$ and d_i (i = 1, 2,...,m), the LUC public key and private key of RA are $\{N, d_{RA}\}$ and e_{RA}, Q is a randomly selected prime greater than N, ID number is the random identifier of V_i.

4.1 Initial Phase

At this phase, voter identification is verified and voters get blank votes.

Step1: If voter P_i (i=1,2,...,m) authentication is required. P_i firstly forms his or her own private key e_i and public key $\{N, d_i\}$, where e_i is also P_i's identity information and meets the voting requirements. Then, it sends the authentication request Request to RA through anonymous channel.

Step2: After receiving P_i's Request, RA randomly selects an integer g from $(\sqrt{N}, N-1)$ and sends g to P_i via anonymous channel.

Step3: After receiving g, P_i uses his or her own private key e_i to sign g, which is calculated by LUC encryption method, and sends the result of signature to RA through the anonymous channel.

Step4: After receiving P_i's signature, RA uses $\{N, d_i\}$ to verify the validity of $V_{d_i}(g, 1)$ mod N, that is, is $g = V_{d_i}(V_{e_i}(g, 1), 1)$ mod N valid. If it is valid, it randomly selects a unique ID from $(\sqrt{N}, N-1)$. Then it sends the ID number to P_i through anonymous channel, and at the same time, it sends the ID number to each vote counter $C_1, C_2, ..., C_n$, and RA encrypts the blank vote s' with its own private key using the LUC encryption method, as $V_{d_{RA}}(s', 1)$ mod N and sends the encrypted blank vote to P_i through anonymous channel. If not, RA sends a Rejection message to P_i, P_i can re-sign and verify, If P_i authentication fails more than three times, RA refuses to accept P_i's authentication.

4.2 Secret Sharing Phase

This phase includes participants vote and send votes to secret distribution agency (DA), which uses Shamir's (t, n) to decompose votes into multiple secret sharings, and then sends them to n vote counters.

Step1: After receiving the ID number and the encrypted blank vote, the voter P_i decrypts blank vote as $V_{e_{RA}}(V_{d_{RA}}(s', 1), 1)$ mod N, The voter P_i fills in the blank vote s' and gets the vote s_i. After encrypting the s_i and ID number ID with P_i's LUC private key, P_i sends them to the secret distribution agency (DA) through the anonymous channel.

Step2: After DA receives P_i's vote, it decrypts the vote s_i and the corresponding ID with P_i's public key. DA randomly selects n different non-zero elements $x_1, x_2, ..., x_n$ from $GF(q)$ (q is a large prime and

$q > n$), DA exposes $x_i (i = 1, 2, ..., n)$ and assigns to $C_j (j = 1, 2, ..., n)$.

Step3: DA randomly chooses $t-1$ elements $a_{i1}, a_{i2}, ..., a_{in}$ from $GF(q)$. The $t-1$ polynomial is constructed as follows:

$$f_{(P_i)}(x) = s_i + a_{i1}x + a_{i2}x^2 + ... + a_{i(t-1)}x^{t-1} \quad (9)$$

DA calculates $y_j = f_{(P_i)}(x_j)$, $1 \le j \le n$, $1 \le i \le m$.
Step4: DA encrypts y_j and ID number of P_i and PI by LUC and sends them to the corresponding vote counter $C_j (j = 1, 2, ..., n)$.

4.3 Counting Phase

After each vote counter receives the secret sharing and ID number, it decrypts by LUC. Then, it checks whether it has received the secret sharing of the same ID number, discards it if it has received it, and saves it if it has not received it. Because the Shamir's (t, n) method is (+, +) homomorphic, the addition operation is performed after all secret sharings received by each vote counter. The final voting result can be restored directly, which is proved as follows.

Let

$$F(C_j) = \sum_{i=1}^{m} f_{(P_i)}(x_j) \quad (10)$$

It can be written as:

$$F(C_j) = \sum_{i=1}^{m} f_{(P_i)}(x_j) = (s_1 + s_2 + ... + s_m) + (a_{11} + a_{21} + ... + a_{m1})x_j + (a_{12} + a_{22} + ... + a_{m2})x_j^2 + ...+ (a_{1(t-1)} + a_{2(t-1)} + ... + a_{m(t-1)})x_j^{t-1} \quad (j = 1, 2, ..., n) \quad (11)$$

According to the following formula, the final result of voting can be obtained:

$$s_1 + s_2 + ... + s_m = \sum_{j=1}^{t} F(C_j) \prod_{i=1, j \ne i}^{t} \frac{x_i}{x_i - x_j} \quad (12)$$

4.4 Verification Phase

After obtaining the final result of the voting activity directly through the homomorphic nature of secret sharing, if there are voters who doubt whether their voting information is accurately recorded, they can submit their ID number to CA for application verification, and CA can recover the votes through the t in n vote counters according to the ID number by the following formula, where $r = 1, 2, ..., m$.

$$s_r = \sum_{i=1}^{t} f_{(P_r)}(x_i) \prod_{j=1, j \ne i}^{t} \frac{x_j}{x_j - x_i} \quad (13)$$

If existing voters or any third party organizations question the overall results of the voting, CA can recover all the information of the votes through t in n vote counters, and then calculate the final results by the following formula.

$$s_1 + s_2 + ... + s_m = \sum_{i=1}^{t} f_{(P_1)}(x_i) \prod_{j=1, j \ne i}^{t} \frac{x_j}{x_j - x_i} + \sum_{i=1}^{t} f_{(P_2)}(x_i) \prod_{j=1, j \ne i}^{t} \frac{x_j}{x_j - x_i} + ...+ \sum_{i=1}^{t} f_{(P_m)}(x_i) \prod_{j=1, j \ne i}^{t} \frac{x_j}{x_j - x_i} \quad (14)$$

5 Security Analysis

We provide a security analysis of the proposed scheme from the following ten aspects.

- Completeness: In the verification phase, whether the number of ID numbers of the vote counter is equal to the number of successful voters can ensure that all legitimate and valid votes are counted correctly. At the same time, the number of ID numbers received by DA can also ensure the consistency of the number of votes, thus ensuring the integrity of the number of votes in the whole voting process.
- Soundness: This scheme is based on LUC cryptosystem. It combines the introduction of ID number and the use of Shamir'(t, n) secret sharing to ensure the security of voting activities, and to ensure that illegal or malicious voters can not affect and destroy the voting process.
- Privacy: In this scheme, the identity information of voters is used and verified as the LUC private key. Malicious voters and third parties can not obtain the identity information of legitimate voters through illegal channels. Also, the unique ID number generated by RA for voters randomly is also sent to voters through LUC encryption, which ensures that ID number is not leaked, that is, the ID number is not disclosed. Even if the ID number is leaked, it can not bind the ID number to the voter's identity information. At the same time, it can not obtain the correct blank votes, which ensures the privacy of the voter's identity. The voting process uses the LUC encryption and decryption. Although the secret sharing process does not encrypt the secret sharings, the leakage of a certain number of secret sharings will not cause leakage of the vote.
- Unreusability: Voters need to send their ID number when voting. When voting is restored and counted, if the counters receive the secret sharings of the same ID number, they will be discarded and can not be counted normally, which ensures that voters can only vote once legally and effectively.
- Eligibility: In this scheme, voters need to authenticate to RA for obtaining blank votes and their unique

ID number before voting, and don't allow voters who have not been authenticated to vote.

- Fairness: In this scheme, *RA, DA, CA, PA* and n counters are credible, which can guarantee the objectivity and fairness of the whole voting process. As long as the successful voters are verified by *RA*, they will get the only *ID* number and blank votes which can ensure that voters' votes do not tamper.

- Verifiability: If there are voters who doubt whether their voting information is accurately recorded, they can submit their *ID* number to *CA* for application verification, and *CA* can recover the votes through the t in n vote counters according to the *ID* number by the formula 13.

- Receipt-Freeness: In the process of identification, voting and counting, voters can not prove their votes. Even if there are Bribery electors at all phases, voters can not prove their votes to bribery electors. In the later phase of voting verification, voters can only check whether their votes are counted, but can not show their contents of votes to *CA*.

- Universal Verifiability: If existing voters or any third party organizations question the overall results of the voting, *CA* can recover all the information of the votes through t in n vote counters, and then calculate the final results by the formula 14.

- Coercion-Resistance: If voters are coerced to disclose their voting content after voting, because the scheme has receipt-freeness, voters can not prove that their open voting content is the real content of the original voting, and the content obtained by the coerced person may not have any relevance to the actual situation of voting.

The security of electronic voting of our method is compared with the methods in [11] [14] [17] [29]. As shown in Table 1.

Our scheme meets ten security requirements of electronic voting. Scheme [11] does not satisfy receipt-freeness and universal verifiability; scheme [14] does not satisfy Privacy, Receipt-Freeness, universal verifiability and Coercion-Resistance; scheme [17] does not satisfy Privacy, Verifiability, Receipt-Freeness, and Universal Verifiability; scheme [29] does not satisfy Privacy, Receipt-Freeness and Universal Verifiability. Based on the comparison, we can see that our proposed scheme is better than its peer methods.

6 Conclusions

The first part of this paper introduces the current research situation of electronic voting. The second part introduces Shamir's (t, n) secret sharing, the LUC cryptosystem and the homomorphism of secret sharing. The third part illustrates the security requirements and the form and composition of the electronic voting system. The fourth part presents our proposed electronic voting scheme in this paper. The fifth part analyses the security of our scheme and compares it with other similar ones.

This scheme uses the LUC cryptosystem to verify voters' identities. With the voter's identity information as the private key, *RA* cannot obtain the identity information, and the *ID* number generated cannot bind to the voter's identity. It achieves the privacy of voter's identity and guarantees the receipt-free voting process. After voter votes, *SD* uses Shamir's (t, n) secret sharing method to divide vote into several secret shares and send them to n vote counters. Each vote counter adds the secret shares received homomorphically. The vote counter does not need to restore each vote to obtain the final result of the voting. In the verification phase, if someone doubts the voting process or results, the voters'votes need to be restored for verification. This process reachs the security requirements of electronic voting and has high efficiency. Since the number of voters can find the best value according to the scale of voting activities, the scheme in this paper is suitable for electronic voting activities of different scales.

Our scheme does not encrypt the secret sharings, because considering that if an attacker can not get the vote information if he or she obtains a single secret sharing, but if the scale of the voting and the number of vote counters are small, it will inevitably affect the security of voting process, but at the same time it will affect the efficiency of the vote decomposition and counting process, which need to be considered in future research activities. Besides, the scheme can achieve overall verifiability, but all votes must be restored. For large-scale voting activities, the efficiency is low. Whether there are better methods is worthy of attention in future research.

Acknowledgments

This study was supported by the National Natural Science Foundation of China (61501064), Sichuan Technology Support Program (2015GZ0088), the Guangxi Key Laboratory of Hybrid Computation and IC Design Analysis (HCIC201502, HCIC201701). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[2] K. Sako, J. Killian, "Receipt-free mix type voting scheme a practical solution to the implementation of a voting booth," in *International Conference on*

Table 1: Security comparison of electronic voting

Security	Our Scheme	FOO.[11]	Shilbayeh et al.[14]	Luo et al.[17]	Yuan et al.[29]
Completeness	Y	Y	Y	Y	Y
Soundness	Y	Y	Y	Y	Y
Privacy	Y	Y	N	Y	N
Unreusability	Y	Y	Y	N	Y
Eligibility	Y	Y	Y	Y	Y
Fairness	Y	Y	Y	Y	Y
Verifiability	Y	Y	Y	N	Y
Receipt-Freeness	Y	N	N	N	N
Universal Verifiability	Y	N	N	N	N
Coercion-Resistance	Y	Y	N	Y	Y

the Theory and Application of Cryptographic Techniques(EUROCRYPT'95), pp. 393–403, Saint-Malo, France, May 1995.

[3] A. C. Neff, "A verifiable secret shuffle and its application to e-voting," in *Proceedings of the 8th ACM Conference on Computer and Communications Security(CCS 2001)*, pp. 116–125, Philadelphia, Pennsylvania, USA, November 2001.

[4] J. Groth, "A verifiable secret shuffle of homomorphic encryptions," in *6th International Workshop on Practice and Theory in Public Key Cryptography*, pp. 145–160, Miami, FL, USA, January 2003.

[5] J. D. Cohen, M. J. Fischer, "A robust and verifiable cryptographically secure election scheme," in *Proceedings of the 26th IEEE Symposium on the Foundations of Computer Science(SFCS'85)*, pp. 372–382, Washington, DC, USA, October 1985.

[6] R. Cramer, R. Gennaro, B. Schoenmakers, "A secure and optimally efficient multi-authority election scheme," in *International Conference on the Theory and Applications of Cryptographic Techniques(EUROCRYPT'97)*, pp. 103–118, Konstanz, Germany, May 1997.

[7] I. Damgard, M. Jurik, "A generalisation, a simplification and some applications of paillier's probabilistic public-key system," in *International Workshop on Public Key Cryptography(PKC 2001)*, pp. 119–136, Cheju Island, Korea, February 2001.

[8] P. Paillier, "Public-key cryptosystem based on composite degree residuosity class," in *International Conference on the Theory and Applications of Cryptographic Techniques(EUROCRYPT'99)*, pp. 223–238, Prague, Czech Republic, May 1999.

[9] I. Damgard, J. Groth, G. Salomonsen, "The theory and implementation of an electronic voting system," *Secure Electronic Voting*; pp. 77–99, Springer, Boston, MA, 2003.

[10] XiaoFeng Chen, JiLin Wang, YuMin Wang, "Receipt-Free Electronic Voting Based on Semi-Trusted Model," *Chinese Journal of Computers* , vol. 26, no. 5, pp. 557–562, 2003.

[11] A. Fujioka, T. Okamoto, K. Ohta, "A practical secret voting scheme for large scale elections," in *International Workshop on the Theory and Application of Cryptographic Techniques(AUSCRYPT'92)*, pp, 244–251, Gold Coast, Australia, December 1992.

[12] L. F. Cranor, R. K. Cytron, "Sensus: a security-conscious electronic polling system for the Internet," in *Proceedings of the 30th Hawaii International Conference on System Sciences*, pp. 561–570, Hawaii, USA, February 1997.

[13] Reem Al-Saidi, Nidal Shilbayeh, Ebrahim Elnahri, And Khaled alhawiti, "E-Voting Authentication Preparation Scheme (EV-APS) Based on Evox-MA and REVS E-Voting Blind Signature Protocols," *International Journal of Engineering Innovations and Research*, vol. 5, no. 3, pp. 590–596, 2014.

[14] Nidal F. Shilbayeh, Reem Al-Saidi, Sameh T. Khuffash, Ebrahim Elnahri, "Efficient and Secure Operations of the New Secure E-Voting Authentication Preparation Scheme (EV-APS)," *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 5, no. 1, pp. 35–41, 2016.

[15] Rui Joaquim, André Zúquete, Paulo Ferreira, "REVS – a roubst electronic voting system", *IADIS International Journal on WWW/Internet*, vol. 1, no. 2, pp. 47-63, 2004.

[16] B. W. DuRette, "Multiple Administrators for Electronic Voting," *Bachelor's Thesis Mit*, 1999.

[17] Fenfen Luo, ChangLu Lin, Shengyuan Zhang, Yining Liu, "Receipt-freeness electronic voting scheme based on voting protocol" *Computer Science(in Chinese)*, vol. 42, no. 8, pp. 180–184, 2015.

[18] A. Shamir, "How to share a secret," *Commmunications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[19] J. He, E. Dawson, "Multistage secret sharing based on one-way functions," *Electronics Letters*, vol. 30, no. 19, pp. 1591–1592, 1995.

[20] H. X. Li, C. T. Cheng, L. J. Pang, "An Improved Multi-stage(t, n) threshold Secret Sharing Scheme," in *WAIM 2005: Advances in Web-Age Information*

Management, pp. 267–274, Hangzhou, China, October 2005.

[21] L. J. Pang, Y. M. Wang, "A new (t, n) multi-secret sharing scheme based on Shamir's secret sharing," *Apllied Mathematics and Computation* , vol. 167, no. 2, pp. 840–848, 2005.

[22] H. X. Li, C. T. Cheng, L. J. Pang, "A new (t, n)-threshold Multi-secret Sharing Scheme," in*International Conference on Computational and Information Science(CIS 2005)*, pp. 421–426, Xi'an, China, December 2005.

[23] J. Benaloh, M. J. Fischer, "A robust and verifiable cryptographically secure election scheme," in *Proceedings of the 26th IEEE Symposium on Foundations of Computer Science(FOCS'85)*, pp. 372–382, Portland, Oregon, USA, October 1985.

[24] J. C. Benaloh, M. Yung, "Distributing the power of a government to enhance the privacy of voters," in *Proceedings of the 5th annual ACM symposium on Principles of distributed computing(PODC'86)*, pp. 52–62, Calgary, Alberta, Canada, August 1986.

[25] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting," in *Advances in Cryptology-CRYPTO'99*, pp. 148–164, Santa Barbara, California, USA, August 1999.

[26] Y. N. Liu, Q. Y. Zhao, "E-Voting Scheme Using Secret Sharing and K-Anonymit," *World Wide Web*, vol. 22, no. 4, pp. 1657–1667, 2019.

[27] D. G. Nair, V. P. Binu, G. S. Kumar, "An improved E-voting scheme using secret sharing based secure multi-party computation," in *ICCN 2014*, pp. 130–137, 2015.

[28] S. Iftene, "General secret sharing based on the Chinese Remainder Theorem with applications in E-voting," *Electronic Notes in Theoretical Computer Science*, vol. 186, no. 1, pp. 67–84, 2007.

[29] L. F. Yuan, M. C. Li, C. Guo, W. T, Hu, Z. Z. Wang, "A Veriable E-voting Scheme with Secret Sharing," *International Journal of Network Security*, vol. 19, no. 2, pp. 260–271, 2017.

[30] P. Smith, "LUC public-key encryption: A secure alternative to RSA," *Dobb's Journal*, vol. 18, no. 1, pp. 44–49, 1993.

[31] L. J. Pang, Y. M. Wang, "A (t, n) secret sharing scheme based on the LUC cryptosystem," *Journal of Xidian University*, vol. 32, no. 6, pp. 927–930, 2005.

[32] H. X. Li, C. T. Chen, L. J. Pang, "LUC-based secret sharing scheme with access structures," *Journal of Southeast University(English Edition)* vol. 36, no. 1, pp. 43–46, 2006.

[33] J. C. Benaloh, "Secret sharing homomorphisms: keeping shares of a secret secret," in em Conference on the Theory and Application of Cryptographic Techniques(CRYPTO'86), pp. 251–260, Santa Barbara, California, USA, August 1986.

[34] H. G. Rong, J. X. Mo, B. G. Chang, G. Sun, F. Long, "Key distribution and recovery algorithm based on Shamir's secret sharing," *Journal on Communications(in Chinese)*, vol. 36, no. 3, pp. 64–73, 2015.

[35] J. Benaloh, D. Tuinstra, "Receipt-free secret-ballot elections," in *Proceedings of 26th Annual ACM Symposium on Theory of Computing(STOC'94)*, Orlando, FL, USA, May 1994.

[36] J. Groth, "Efficient maximal privacy in boardroom voting and anonymous broadcast," in *International Conference on Financial Cryptography(FC2004)*, pp. 90–104, Key West, FL, USA, February 2004.

[37] Z. Hong, L. S. Huang, Y. L. Luo, "A multi-candidate electronic voting scheme based on secure sum protocol," *Journal of Computer Research and Development*, vol. 43, no. 8, pp. 1405–1410, 2006.

[38] A. Ei-Latif, X. Yan, L. Li, et al, "A new meaningful secret sharing scheme based on random grids, error diffusion and chaotic encryption," *Optics & Laser Technology*, vol. 54, pp. 389–400, 2013.

[39] I. C. Lin, M. S. Hwang, C. C. Chang, "Security enhancement for anonymous secure e-voting over a network," *Computer Standards & Interfaces*, vol. 25, no. 2, pp. 131–139, 2003.

Biography

Hongquan Pu received the M.S. degree in computer application technology from University of Chinese Academy of Sciences in 2014. He is currently a Ph.D. candiadate in University of Chinese Academy of Sciences. His current research interests include Electronic voting, Secret Sharing, LUC Secret System, Secure Multi-Party Computation(SMPC).

Zhe Cui received the degree of Bachelor in Electronic Precision Machinery from University of Electronic Science and Technology of China in 1992. He received the M.S. degree in Computer Application Technology from Chengdu Institute of Computer Applications, Chinese Academy of Sciences in 1995. He received the Ph.D. degree in Computer Software and Theory from Chengdu Institute of Computer Applications, Chinese Academy of Sciences in 2011. He is currently a Ph.D. supervisor at the University of Chinese Academy of Sciences. The main research fields include pattern recognition and information security.

Ting Liu received the M.S. degree in Computer Software and Theory from Xi'an Technological University in 2011. He is currently a Ph.D. candiadate in University of Chinese Academy of Sciences. His research interests include Electronic voting, Blockchain and Secret Sharing.

Zhihan Wu received the degree of Bachelor of Engineering in Information Scecurity from Sichuan University in 2017. She is currently a M.D. candiadate in University of Chinese Academy of Sciences. Her current research interests include Electronic voting, Blockchain, Cryptography.

Hongjiang Du received the degree of Bachelor of Engineering in Computer Science and Technology from

Sichuan University in 2002. He received the degree of Master of Engineering in Computer Science and Technology from Sichuan University in 2006. He is currently a Ph.D. candidate in University of Chinese Academy of Sciences. His current research interests include Electronic voting, coding theory, information security.

Intrusion Detection Method Based on MapReduce for Evolutionary Feature Selection in Mobile Cloud Computing

Emmanuel Mugabo, Qiu-Yu Zhang, Aristide Ngaboyindekwe,
Vincent de Paul Niyigena Kwizera, and Victus Elikplim Lumorvie
(*Corresponding author: Qiu-Yu Zhang*)

School of Computer and Communication, Lanzhou University of Technology
School of Electrical and Information Engineering, Lanzhou University of Technology
No. 287, Lan-Gong-Ping Road, Lanzhou 730050, China
(Email: zhangqylz@163.com)

(Received June 5, 2019; Revised and Accepted Dec. 2, 2019; First Online Feb. 10, 2020)

Abstract

In the last few years, mobile cloud computing (MCC) has developed rapidly and become one of the most useful in different disciplines to communicate and exchange a lot of sensitive information within many types of mobile terminals, and computer devices. The increase of MCC usage in daily life has expanded from ten to thousands of data day by day. Meanwhile, processing and analyzing those huge amounts of data have been a major issue in data mining and machine learning techniques, wherein many traditional methods were not able to cope with a large number of instances and features found in big datasets. To overcome these drawbacks, an intrusion detection method for MCC based on MapReduce for evolutionary feature selection was proposed. In the proposed method, a MapReduce feature selection based on evolutionary computing is used to obtain a small and useful number of instances and features from big datasets. To evaluate the performance of our proposed method, the popular KDD Cup 99 dataset is used and the random forest classifier is used for classifying the normal and abnormal activities in MCC. The experimental results show that our proposed method can detect the intrusions in MCC with high accuracy, detection rate and low false positive rate.

Keywords: Big Dataset; Intrusion Detection; MapReduce for Evolutionary Feature Selection; Mobile Cloud Computing; Random Forest Classifier

1 Introduction

Over the last decade, the constant growth of mobile devices has tremendously changed the lives of our societies, where people rely on them to receive news, emails, biomedical reports and do online marketing anywhere and anytime. However, it has been known that these portable devices are always limited in terms of memory space, disk capacity and processor speed [5]. Aiming at the above challenges of mobile devices, cloud computing can be a good way to improve their capabilities by offloading the computation data from the mobile devices into the cloud.

The integration of mobile terminals, mobile internet, and cloud computing is a new technology called mobile cloud computing (MCC) that uses cloud computing to deliver cloud services to mobile services in a pay-as-you consume principle [21]. Moreover, the recent advances in MCC have made it easy for cyber-attacks by intruders [5, 11, 21]. The confidentiality, integrity and availability of MCC need to be protected from those number of cyber-attacks.

The most recently workflows to counter the security issues in MCC have adopted intrusion detection systems (IDSs) which provide a better solution to the security issues compared to the traditional firewall technologies. Among them, machine learning algorithms such as support vector machine (SVM) [7, 22], genetic algorithm (GA) [18], random forests (RF) [4, 14, 20, 23, 27] and so forth have been used. On the other hand, in the recent contributions in cloud computing field, many researchers have adopted different data mining and machine learning techniques to deal with redundancy, high computing cost and dimensional issues which have also been a serious problem. However, the existing methods lack enough scalability to deal with big datasets and do not provide suitable results.

The term 'Big data' is getting more attention from different disciplines that build massive datasets. Big data is defined as the most popular term used to describe large and complex amounts of data [20]. Due to its simplicity and fault tolerant nature, the MapReduce framework, which is a way of processing large amounts of data in a

parallel manner, has been an effective and robust model to deal with the big dataset analysis [8].

Feature selection methods and other data reduction methods have been used to reduce the input data and also to improve the classification accuracy by removing redundant or irrelevant features. In some of the existing techniques, evolutionary approaches such as ant colony optimization (ACO) [2], particle swarm optimization (PSO) [17, 27, 28] have been adopted by many researchers in big datasets for feature selection methods.

In this paper, we have adopted evolutionary approach-based feature selection (EFS) to reduce the size of dataset and a MapReduce algorithm is used to split the input data in a parallel way to get the most important features to be used for further process. The random forest (RF) classifier is then used to classify our model either in normal or attack.

The rest of this paper is organized as follows. Section 2 outlines the recent related works based on MapReduce for evolutionary feature selection and other methods. The related techniques and other related theories are detailed in Section 3. The proposed MapReduce for Evolutionary feature selection-based RF method for IDS in MCC is presented in Section 4. Section 5 provides the experimental results and performance analysis as compared with other related methods. Finally, we conclude our paper in Section 6.

2 Related Works

In the development of cloud computing environment, processing and analyzing big data have been a hot topic for most of the researchers in the last few years [8]. Feature selection (FS) is an important issue in IDS that can be used to filter out noise, remove redundant and irrelevant feature from the original dataset. On the other hand, FS can be considered as an optimization problem that satisfy a desired measure for an optimal subset of features [2]. In the recent research works, many researchers have adopted FS methods in either dimensional reductions and/or optimization problems, and the evolutionary computation (EC) techniques have shown to be successful when dealing with the feature selection in big dataset.

The main techniques in IDSs and data security challenges in MCC have been analyzed, and the literature survey about machine learning and data mining methods is presented in [5, 6, 11, 18, 21]. The authors in [22] proposed a method that uses rough set theory (RST) and support vector machine (SVM) to detect the intrusions. The RST is used to preprocess the data and reduce the dimensions of the data, while SVM is used to learn and test the selected features from RST. The KDD Cup 99 dataset is used to evaluate the model and the results show that the proposed method can improve the accuracy and shorten the false positive rate. In [14], an improved scalable RF algorithm based on MapReduce model is proposed. The experimental results show that the proposed method is more suitable to classify massive datasets in distributing computing environment and can achieve a higher performance than traditional RF methods. The distributed IDS method based on SVM and ACO that can detect unseen attacks of intrusions with high detection rate and low misclassification is proposed in [23], the experimental results show that the proposed method can perform better than SVM or ACO alone in terms of detection rate and run-time efficiency. The authors in [8] proposed a feature selection based on EC for big data using MapReduce framework and three classifiers (SVM, Logistic Regression and Na?ve Bayes) are used to evaluate the performance of the proposed method. In [2], the authors proposed ant colony optimization (ACO) to address the problem of dimensional reduction in intrusion detection system. The proposed method used the ACO and nearest neighbor classifier to select important features and classify normal or abnormal behavior. Tests and comparisons are performed using KDD Cup 99 and NSL-KDD datasets and the experimental results showed a competitive performance of the proposed method. In [28], a fuzzy c-means clustering (FCM) based on particle swarm optimization (PSO) for IDS is proposed. By using KDD Cup 99 dataset, the experimental results show that the proposed method achieved a higher detection rate, and a lower false positive rate. The hybrid approach of PSO and decision tree (DT) is proposed in [17], where PSO is used to prune a DT and the pruned DT is used for classification of the network intrusions. All the experiments are carried out on KDD Cup 99 dataset, and the results show that the proposed technique performs better than other classifiers in terms of detection rate, accuracy, precision, and false positive rate. The authors in [25, 26] highlights the EC techniques for feature selection in big dataset and in [1] analyses the parallel EC algorithms for FS in big dataset.

In [10], the feature selection based on the cuttlefish optimization algorithm (CFA) which is used as a search strategy to find the optimal subset of features and decision tree (DT) classifier as a measurement on the selected features were used. The KDD Cup 99 dataset was used to evaluate the proposed method and the experimental results showed that the combined method of CFA and DT gives a higher detection rate, accuracy rate and low false positive rate. The two-level hybrid approach of two anomaly detection components and a misuse detection component was proposed in [12] to achieve a high detection rate with a low false positive rate. By using KDD'99 dataset, the experimental results show that the proposed hybrid method can detect known and unknown attacks with high detection rate and low false positive rate. In [13], the authors proposed a distance sum-based support vector machine (DSSVM) to improve the detection accuracy, and after applying DSSVM to the KDD'99 dataset, the experimental results show that the proposed method performs well in both detection performance and computational cost. The hybrid learning of K-means, clustering based density and k-NN classifier was proposed

in [24], and the results show that the proposed method can be effective in intrusion detection. In [15], a k-NN classifier with ant colony optimization (ACO) using KDD Cup 99 dataset was proposed, and the experimental results show that the proposed system provides better accurate results than the existing methods. The hybrid approach of principal component analysis (PCA) and machine learning algorithms was proposed in [9] to develop an effective intrusion detection method, and the result show higher true positive rate and lower false positive rate compared to the existing approaches. In [16], the authors proposed a FAST-ABQGSA-SVM algorithm to improve the effect of network intrusion detection, and the simulation results show that the proposed algorithm achieves better robustness, learning accuracy and detection performance. The authors in [29] proposed a new network intrusion detection method based on hybrid rice algorithm optimized extreme learning machine (HRO-ELM). The KDD Cup 99 dataset is used to evaluate the proposed algorithm and the simulation results show that the HRO-ELM improves the detection accuracy and can meet the requirements of network intrusion online detection.

3 Problem Statement and Preliminaries

The main parts of the proposed method are: big dataset, MapReduce for evolutionary feature selection (MR-EFS) and random forest classifier (RF).

3.1 Big Dataset

Dealing with large datasets has been a major issue for most of the traditional data mining and machine learning algorithms. This issue is commonly known as 'big data', which refers to the deficiencies of processing and analyzing huge amounts of connection records. Due to the enormous stored data in different domains, the term 'big data' has attracted much attention in academia and industry. The recent advances on cloud computing technologies allow for adapting standard data mining techniques in order to apply them successfully over massive amounts of data [3, 8].

In 2001, Gartner analyst Doug Laney introduced the 3Vs concept defining the big data as a high volume, variety and velocity information [20]:

1) The term 'volume' refers to the large amount of data that are being produced every day and have gone from Mega Bytes (MB) and Giga Bytes (GB) to Peta Bytes (PB).

2) The term 'variety' cope with the large number of types of data, both structured and unstructured data.

3) The term 'velocity' refers to how fast the data is coming in and how it needs to be analyzed.

Recently, there are some other additional big data Vs such as veracity, value, validity and volatility that are getting attention day by day.

3.2 MapReduce for Evolutionary Feature Selection (MR-EFS)

Feature selection has been a challenging task in machine learning and data mining due to the large search space and big dimensionality where the total number of possible solutions is 2^n for a dataset with n features, which leads to poor classification performance [25]. As the number of features n is increasing, various heuristic search methods have been proposed for feature selection, but most of existing methods still suffer from stagnation in local optima and high computational cost. Due to the potential search ability, evolutionary computation (EC) methods such as genetic algorithms (GAs), genetic programming (GP), particle swarm optimization (PSO), and ant colony optimization (ACO) have been recently adopted for feature selection and have shown to achieve accurate results for big datasets [1, 25].

The EC algorithms have been originally introduced in 2003 by Eiben and Smith, which are defined as the search algorithms that use principles inspired by natural genetic populations to develop solutions to problems [26]. The main problems when dealing with big datasets for these methods are; the huge amount of computation time since their complexity for feature selection is at least $O(n^2D)$, where n is the number of instances and D the number of features, and the other problem is memory consumption since most methods need to store the whole dataset in memory. Therefore, many researchers use the parallel computation methods such as MapReduce, MPI (Message Passing Interface) to improve the efficiency of the EC methods for feature selection on large datasets [1].

The MapReduce programming model which is used in our proposed method, originally introduced in 2004 by Google, is the effective and robust framework that deals with the analysis of big datasets in a parallel way. Due to its fault-tolerant mechanism and its simplicity, the MapReduce framework is currently taken into consideration in machine learning and data mining, rather than other parallelization schemes such as MPI [8]. Its main approach is to partition the original dataset into small subsets and allocate them into a single map task in parallel manner. The main functions of MapReduce model are Map function and Reduce function are as shown in Figure 1.

As can be seen from Figure 1, the MapReduce model is based on a basic data structure known as *(key, value)* pair where its main goal is to merge the input *(key, value)* pair to another one *(key, value)* list. The map function takes an input pair and generates a list of intermediate *(key, value)* pairs as output. This is represented by the following form:

$$map(key1, value1) \rightarrow \{(key2, value2), ...\}. \quad (1)$$

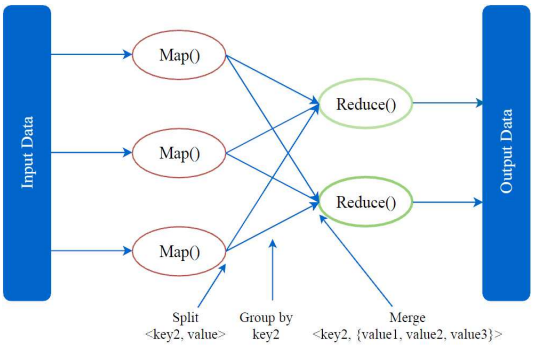


Figure 1: Data flow of MapReduce operation

The reduce function receives and merges together all the intermediate *(key, value)* pairs to form the aggregated pairs and then generates a new *(key, value)* pair as output [7, 26]. This is represented by the following form:

$$reduce(key2, \{value2, ...\}) \rightarrow (key2, value3). \quad (2)$$

MapReduce programming model not only provides an efficient model for processing large datasets, but also is the most parallel model for data processing in cloud computing environment [26]. In our proposed method, we adopted Cross generation elitist selection, Heterogeneous recombination, Cataclysmic mutation (CHC) algorithm [17] with MapReduce framework, a binary-coded genetic algorithm, which combines the conservative selection strategy that produces offsprings that are at the maximum hamming distance from their parents. CHC algorithm is a robust evolutionary algorithm, which often offer promising results in different search problems. The main components of the CHC algorithm are:

Half-uniform crossover (HUX): This produces two offsprings, which are exactly different from their two parents.

An elitist selection: It composes a new generation, the best individuals among parents and offspring are selected.

An incest prevention mechanism: Which prevents the pairs of individuals to mate if the similarity between them is higher than a threshold. This threshold is decreased, as time goes by, to help the population to converge.

A restarting process: Which is applied when the specified population has stagnated, then generates a new population by choosing the best individuals from the old population.

Figure 2 shows the flowchart of the CHC algorithm.

3.3 Random Forest Classifier (RF)

The Random forest (RF) classifier [19], a commonly used method applied to data classification, is an ensemble classifier which consists of many decision trees that uses the randomly selected data features as their input data, and is built by using the bagging method [6, 14]. According to Breiman, each decision tree in the forest is constructed on bootstrapped sample of the original training data. In order to classifier new object from an input vector, the input vector will put down each of the trees in the forest. Every tree cast a vote to indicate the decision of the trees and the forest chooses the classification with the most votes over all the trees in the forest [4, 27].

Random forests are well known to be a good parallel distributed processing, since they are composed of multiple decision trees and each decision tree can be independently trained by ensemble learning techniques [23]. Every tree in the forest is grown as follows:

1) Let the number of instances in the original training data be N and then, draw a bootstrap sample of size N from the original training data. This sample will be a new training dataset for growing the tree. The instances that are in the original training data but not in the bootstrap sample are called out-of-bag (oob) data for the tree.

2) Let the total number of input features in the original training data be M. On this bootstrap sample data, only m features are chosen randomly for every tree where . The features from this dataset creates the best possible split at each node of the tree and the value of m should be constant during the growing of the forest.

Random forest classifier runs efficiently on big datasets with a better classification accuracy when comparing to a single decision tree method. RF combines N decision tree classifiers $Tree(1)$, $Tree(2)$, ..., $Tree(N)$ as shown in Figure 3.

The work steps of RF classification are as follows:

1) Select randomly N samples from the original training dataset by using bagging method.

2) The selected N samples will be the training set for growing N trees in order to achieve the N classification results.

3) Finally, the N classifiers vote to elect the optimal classification with majority votes.

4 The Proposed Method

The MapReduce for evolutionary feature selection (MR-EFS) based RF classifier method is developed with the main goal of increasing the anomaly intrusion detection accuracy, detection rate and decreasing the false positive rate in MCC. Due to the huge amounts of features including redundant and irrelevant features in KDD Cup 99 dataset, processing and analyzing them for data mining and machine learning tasks is a big challenge for most of the researchers. To overcome the above issues, the

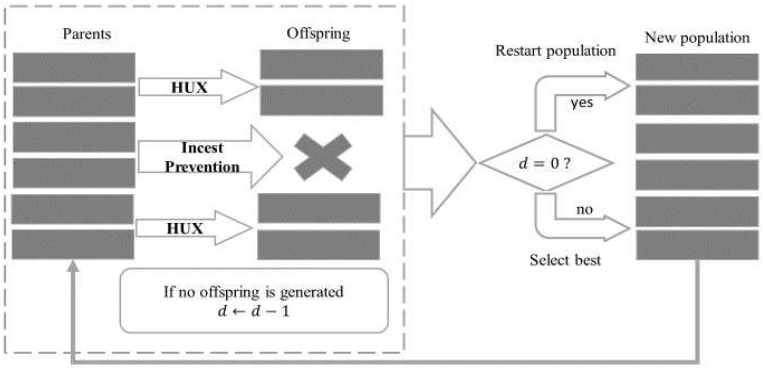


Figure 2: Flowchart of the CHC algorithm

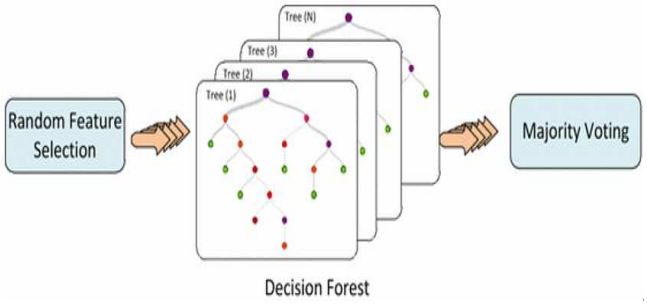


Figure 3: Random forest (RF) classifier

proposed method uses MR-EFS method to extract the optimal features and the optimal features are selected efficiently and are able to reduce the computation time of intrusion detection system and therefore improve the detection rate and accuracy, and reduce the false positive rate using RF classifier.

The RF classifier is then used to classify accurately the malicious attacks wherein the experimental results show that the proposed method can achieve better classification accuracy, detection rate, and low false positive rate compared to the traditional methods applied on big datasets.

The flow diagram of the proposed method is shown in Figure 4.

As can be seen from Figure 4, the proposed method includes three main phases: data preprocessing, feature selection, and anomaly detection and classification.

In KDD'99 dataset, the features in columns 2, 3, and 4 are the protocol type, the service type, and the flag, respectively. The protocol type values are TCP, UDP, or ICMP; the service type values are one of the 66 different network services such as http and smtp; and the flag values are in 11 possible values such as SF or $S2$. Hence, the data preprocessing is done by mapping the categorical features to numerical features. After mapping these features, 115 variables for each samples of the KDD'99 dataset are obtained. The final step of data preprocessing is data normalization wherein the numeric training and testing data are normalized in the range of [0, 1] to make them easier for further steps.

The evolutionary CHC algorithm with MapReduce model is then adopted to find the global optimum feature from the number of numeric features in the dataset. Finally, after selecting the optimal features from the dataset, the RF classifier is used to detect and classify the attacks from normal behavior connections.

The Algorithm 1 shows a basic pseudocode of CHC algorithm.

Algorithm 1 CHC algorithm

Input: A population
Output: An optimized population

```
initialize the population
while termination criteria are not satisfied do
    select the candidates from the population;
    generate offspring by crossing the parents;
    evaluate the offspring with the fitness function;
    select the individuals of the new population
end while
if population is not changed then
    decrease the threshold d
end if
if threshold d ≤ 0 then
    restart population and reinitialize threshold
end if
```

Algorithm 1 explains the process of CHC algorithm that is used to obtain the optimized population from the initial population. Firstly, the initial population is initialized and according to Figure 2, when the termination criteria of the algorithm is not satisfied, the candidates from the initial population are selected and the offspring are generated by crossing the parents. After evaluating the offspring, the individuals of the new population are selected, and if the population is not changed, then the threshold d is decreased to help the population to converge. However, when the threshold $d \leq 0$, then the new population is generated by selecting the best individuals from the old population.

The Algorithm 2 describes the process of MR-EFS algorithm.

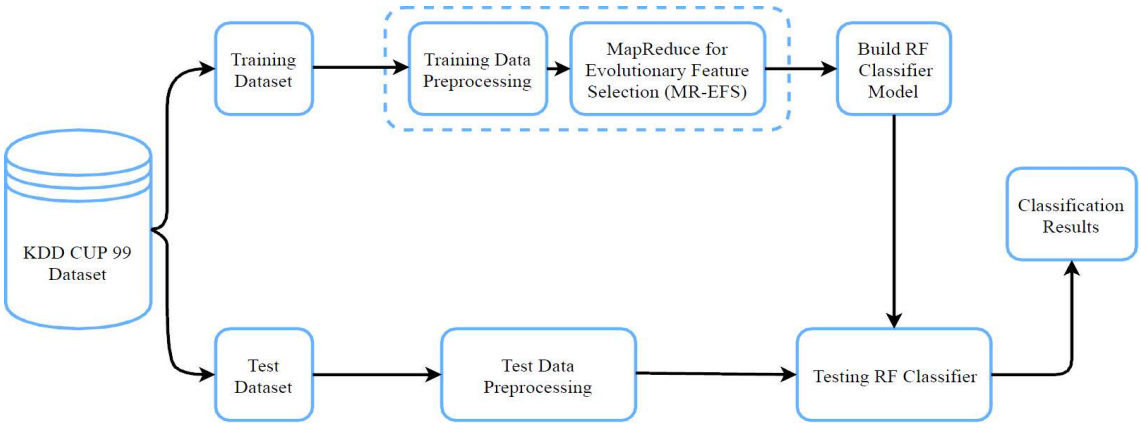


Figure 4: The flow diagram of MR-EFS based RF classifier

Algorithm 2 MR-EFS algorithm

$Map_i \forall i \in \{1, \ldots, T_{isubset}\}$
Input: Training set T corresponding to m number of map tasks
Output: A binary vector $f_i = \{f_{i1}, \ldots, f_{iD}\}$, D is number of features selected by CHC algorithm

1: load training set T
2: split T into m disjoint subsets of instances
3: process each $T_{isubset}$ $i \in \{1, 2, \ldots, m\}$ using corresponding Map_i task

$Reduce_i \quad \forall i \in \{1, \ldots, T_{isubset}\}$
Input: Average of all the binary vectors
Output: Selected features for the reduced dataset

1: average all the binary vectors by obtaining vector $x = \{x_1, \ldots, x_D\}; x_j = \frac{1}{m}\sum_{j=1}^{m} f_{ij}, j \in \{1, 2, \ldots, D\}$
2: calculate and use vector x to build the reduced dataset
3: design an additional MapReduce process to remove less promising features
4: doing so, binarize vector x by using a threshold θ: $b = \{b_1, \ldots, b_D\}; b_j = \begin{cases} 1, & \text{if} x_j \geq \theta \\ 0, & \text{otherwise} \end{cases}$; vector b indicates which features will be selected for the reduced dataset
5: the number of selected features $D' = \sum_{j=1}^{D} b_j$ is controlled with θ
6: **while** a high threshold θ **do**
7: select only few features
8: **end while**
9: **while** a low threshold θ **do**
10: pick more features
11: **end while**

Algorithm 2 presents the process of MR-EFS algorithm that is used to find the optimal features for intrusion detection and classification process using random forest (RF) classifier to detect the normal and abnormal behavior in mobile cloud computing (MCC). First, the training set is split into different subsets in the map phase to get the binary vector f_i that indicates which features were selected by the CHC algorithm. Then, the average of all binary vectors is calculated in the reduce phase to get the best optimal features from the reduced dataset and to be used in the intrusion detection and classification process. The number of selected features D' is controlled with the threshold θ, and if the threshold θ is high, the few features are selected and the performance of the model is improved as well. However, if the threshold θ is small, then more features are picked and the performance of the model is affected.

The algorithmic process of RF classifier for the proposed method is described as follows:

Algorithm 3 Random Forest classifier

Input: Selected features $f_i = f_1, f_2, \ldots, f_n$ from the reduced dataset
Output: Classification accuracy, detection rate and false positive rate

1: load the selected best features
2: the selected features are given to RF classifier for training
3: the test set in then fed to RF classifier for classification
4: execute the accuracy, detection rate and false alarm rate

Algorithm 3 shows the process of random forest (RF) classifier for detecting and classifying the normal behavior and malicious attacks in MCC. The best optimal features are selected from the reduced dataset in Algorithm 2 and then loaded to be given to RF classifier for training process. After that, the test set is fed to RF classifier for classifying the connection in either normal or abnormal. This results to a good classification method with good accuracy, detection rate and low false positive rate.

5 Experimental Results and Analysis

All the experiments of the proposed method were implemented on a computer having window 10 Intel (R) Core (TM) i5-7200U CPU 2.50GHz with 16 GB of RAM and 64-bit OS. The Java programming language under NetBeans IDE 8.2 platform were used to run the whole project and KDD Cup 99 dataset was used to evaluate the performance of the proposed method.

5.1 Dataset Collection and Data Preprocessing

In intrusion detection system (IDS), KDD Cup 99 dataset has been widely used as the benchmark dataset to evaluate the performance of IDS problem. The KDD Cup 99 includes three independent sets: The whole KDD training set, 10% KDD training set, and corrected KDD test set. Each record represents a network connection described by 41 features and a label marked as either normal or one of the 39 specific attack types.

The corrected KDD test set includes 17 new attack types not presented in the training set and excludes 2 types (spy, warezclient) of attack from training set, therefore there are 37 attack types that are included in test set, as shown in Table 1 and Table 2.

Table 1: Attacks in KDD'99 training dataset

Attack types	Name of Attacks
DoS	Neptune, Smurf, Pod, Teardrop, Land, Back
Probe	Port-sweep, IP-sweep, Nmap, Satan
U2R	Buffer-overflow, Load-module, Perl, Rootkit
R2L	Guess-password, Ftp-write, Imap, Phf, Multihop, Spy, Warezclient, Warezmaster

Table 2: Attacks in KDD'99 test dataset

Attack types	Name of Attacks
DoS	Neptune, Smurf, Pod, Teardrop, Land, Back, Apache2, Udpstorm,Processtable, Mail-bomb
Probe	Port-sweep, IP-sweep, Nmap, Satan, Saint, Mscan
U2R	Buffer-overflow, Load-module, Perl, Rootkit, Xterm, Ps, Sqlattack
R2L	Guess-password, Ftp-write, Imap, Phf, Multihop, Warezmaster, Snmpget attack, Named, Xlock, Xsnoop, Send-mail, Http-tunnel, Worm, Snmp-guess

The attack types in KDD'99 can be categorized in four classes, namely remote-to-local (R2L), denial-of-service (DoS), user-to-root (U2R), and Probe. In our experiment, we have used 10% KDD'99 dataset containing 494,021 records for training and corrected KDD dataset consisting of 311,029 records for testing as shown in Table 3.

Data Preprocessing consists of two steps: the first step involves mapping some nominal features to numeric-valued features. Thus, nominal features such as "protocol", "service type" and "TCP status flag" are mapped to binary numeric features. The second step is to normalize the numerical features because the scales of some numerical features in the KDD'99 data are different. For instance, "destination host count" has a range of $0 \backsim 255$, whereas "source bytes" ranges from $0 \backsim 693{,}375{,}640$, therefore the numerical attributes are normalized by projecting their feature value to the range of [0, 1].

5.2 Feature Selection

As KDD Cup 99 dataset includes large amount of relevant, irrelevant and redundant features, and not all of them are useful; the dimensional reduction methods such as feature selection are used to select the most important features and reduce the dimension of the dataset. This results in a simpler and more comprehensible classification model with a low processing time and a better classification performance.

Among the existing methods, the evolutionary approaches have been successfully used for feature selection methods. In our experiment, we adopted CHC evolutionary algorithm for feature selection with MapReduce to be applied on KDD Cup 99 dataset, which splits the training data in parallel in the map phase and then combines the results in the reduce phase to obtain the most important features to be used for classification process.

According to the Algorithm 3 stated above, the number of selected features is set D'=15, which are then used as input for classification process.

5.3 Performance Metrics

The proposed model is evaluated based on three performance metrics: detection rate (DR), false positive rate (FPR), and accuracy rate (ACC).

$$DR = \left(\frac{TP}{TP+FN}\right) \times 100\%$$

$$FPR = \left(\frac{FP}{FP+TN}\right) \times 100\%$$

$$ACC = \left(\frac{TP+TN}{TP+FN+FP+TN}\right) \times 100\%$$

where, TP is the number of attacks that are correctly classified as attack, FP is the number of normal records misclassified as attacks, TN is the number of truly classified normal records and FN is the number of attacks misclassified as normal records. DR is the number of successfully detected intrusive records from the total number

Table 3: 10% KDD'99 training set and corrected KDD test set

Dataset	Instances	Normal	DoS	Probe	U2R	R2L
KDD'99 (10%)	494,021	97,278	391,458	4,107	54	1,124
Corrected	311,029	60,593	229,853	4,166	2,636	13,781

of intrusive records and FPR is the number of misclassified normal records as attacks from the total number of normal records, while ACC is the number of correctly classified records from the total number of the records. The higher values of DR and ACC, and lower values of FPR show better classification performance for IDSs.

5.4 Experimental Result and Discussion

In the proposed method, the random forest classifier was tested with the following parameters: number of trees is 100, minimum node size is 1, and three performance metrics were used for machine learning comparison; classification accuracy (ACC), detection rate (DR) and false positive rate (FPR). After conducting the dimensional reduction process, the relevant features are generated and given as input data to random forest classifier (RF). According to the Algorithm 2, the number of selected features D' is controlled with the threshold θ. Table 4 shows the performance of the proposed method using different threshold values.

Table 4: Performance evaluation using different threshold values

Threshold(θ)	Features	ACC (%)	DR (%)	FPR (%)
0.00	41	90.2	89.01	4.05
0.50	26	91.74	91.35	3.16
0.65	15	93.9	91.9	2
1.00	6	93.83	91.89	2.73

As can be seen from Table 4, with a high threshold value, the fewer number of selected features and with a low threshold value, the larger number of selected features. The zero-threshold value corresponds to the original dataset without using any feature selection method and the threshold value of 0.65 got to improve the performance of the proposed method compared to other threshold values and reducing the size of the dataset with D'=15 as well. The results of classification using the proposed method are compared with other machine learning techniques [9, 10, 12, 13, 15–17, 24, 28, 29] tested on the KDD Cup 99 dataset as shown in Table 5.

As can be seen from Table 5, all the machine learning techniques tested on the KDD Cup 99 dataset provided a good level of accuracy and detection rate as the proposed method, but most of them except the one for k-NN [12] did not have lower false positive rate needed for better classification. At the same time k-NN [12] has a lower ACC and DR compared to the proposed method. The proposed method showed to improve the level of accuracy and detection rate, and shorten the false positive rate compared to the stated above methods. In [29], comparing with HRO-ELM method, the proposed method has improved the detection accuracy (ACC). The proposed method has a high ACC, DR and low FPR compared to that of ADBCC [10], DMNBtext [17], $C4.5$ [13], CFA+DT [10] and SO-DTP [17]. In [9, 16, 28], comparing with PSO+FCM, RS+GA+SVM, MLP methods, the proposed method improved the DR and shortened the FPR.The KNN+ACO [15] method has a good detection rate (DR), but its FPR is high compared to the proposed method. Compared to the CANN [9] method, the detection accuracy (ACC) and false positive rate (FPR) of the proposed method are improved. As the large number of records in the dataset can affect the performance of the machine learning algorithm and its execution time, applying the evolutionary feature selection can be a good method to remove the unimportant features, and select the important ones and improve the classification performance. Therefore, the experimental results of the proposed method based evolutionary feature selection show that a good detection performance has been achieved.

Table 5: Comparison of performance evaluation

Methods	ACC (%)	DR (%)	FPR (%)
HRO-ELM [29]	92.50	N/A	N/A
ADBCC [12]	92.71	91.79	3.5
k-NN+ACO [15]	94.17	N/A	5.82
k-NN [12]	93.29	91.86	0.78
RS+GA+SVM [16]	N/A	88.2	2
DMNBtext [17]	91.394	91.46	8.9
PSO+FCM [28]	N/A	89.46	13.55
C4.5 [13]	92.745	91.7049	2.9558
CFA+DT [10]	92.5	91.5	3.372
CANN [24]	89.79	91.96	4.55
MLP [9]	N/A	88.9	4.6
SO-DTP [17]	91.69	91.765	2.7429
Proposed Method	93.9	91.9	2

6 Conclusion and Future Works

In this paper, we have proposed an intrusion detection method based on MapReduce for evolutionary feature selection in mobile cloud computing. The proposed method addresses the problem of processing and analyzing big datasets by using a MapReduce for Evolutionary Feature Selection (MR-EFS) algorithm based on random forest (RF) classifier. The MR-EFS algorithm is used for dimension reduction and RF classifier is used for classification. The traditional methods have been facing the problem of

features redundancy, high computation cost and not suitable for processing large datasets thus obtaining poor results for intrusion detection. The proposed method uses MR-EFS algorithm to select the most relevant features from the big dataset and RF classifier to identify and classify the attack and normal behavior. The KDD Cup 99 dataset is used to evaluate the proposed method and the experiment results show that the proposed method can achieve better performance of intrusion detection in MCC.

For the future works, the proposed method can be extended to deal with the above issues by adopting the other machine learning techniques and/or hybrid techniques, and Hadoop shall be applied to deploy test cases across multiple nodes.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (No. 61862041, 61363078), the Innovation Ability Improvement Project of Gansu Colleges and Universities of China (2019A-236). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] S. I. Adi, and M. Aldasht, "Parallel evolutionary algorithms for feature selection in high dimensional datasets," *American Journal of Computer Science and Engineering Survey*, vol. 6, no. 1, pp. 013–021, 2018.

[2] M. H. Aghdam and P. Kabiri, "Feature selection for intrusion detection system using ant colony optimization," *International Journal of Network Security*, vol. 18, no. 3, pp. 420–432, 2016.

[3] I. Aljarah, S. A. Ludwig, "MapReduce intrusion detection system based on a particle swarm optimization clustering algorithm," in *IEEE Congress on Evolutionary Computation*, pp. 955–962, 2013.

[4] M. H. R. Al-Shaikhly, H. M. El-Bakry, and A. A. Saleh, "Cloud security using Markov chain and genetic algorithm," *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 96–106, 2018.

[5] T. Bhatia and A. K. Verma, "Data security in mobile cloud computing paradigm: A survey, taxonomy and open research issues," *Journal of Supercomputing*, vol. 73, no. 6, pp. 1–74, 2017.

[6] A. L. Buczak, and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2017.

[7] Y. Chang, W. Li, Z. Yang, and Z. Yang, "Network intrusion detection based on random forest and support vector machine," in *IEEE International Conference on Computational Science & Engineering*. pp. 635–638, 2017.

[8] P. Daniel, D. R. Sara, R. G. Sergio, T. Isaac, M. B. Jose and H. Francisco, "Evolutionary feature selection for big data classification: A MapReduce approach," *Mathematical Problems in Engineering*, vol. 2015, pp. 1–11, 2015.

[9] I. Dutt, S. Borah, I. Maitra, "A proposed machine learning based scheme for intrusion detection," in *IEEE 2nd International Conference on Electronics, Communication and Aerospace Technology (ICECA'18)*, pp. 479–483, 2018.

[10] A. S. Eesa, Z. Orman, A. M. A. Brifcani, "A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems," *Expert Systems with Applications*, vol. 42, no. 5, pp. 2670–2679, 2015.

[11] K. Gai, M. Qiu, L. Tao and Y. Zhu, "Intrusion detection techniques for mobile cloud computing in heterogeneous 5G," *Security and Communication Networks*, vol. 9, no. 16, pp. 3049–3058, 2016.

[12] C. Guo, Y. Ping, N. Liu, and S. S. Luo, "A two-level hybrid approach for intrusion detection," *Neurocomputing*, vol. 214, pp. 391–400, 2016.

[13] C. Guo, Y. Zhou, Y. Ping, Z. Zhang, G. Liu, Y. Yang, "A distance sum-based hybrid method for intrusion detection," *Application Intelligent*, vol. 40, pp. 178–188, 2013.

[14] J. Han, Y. Liu, and X. Sun, "A scalable random forest algorithm based on MapReduce," in *IEEE 4th International Conference on Software Engineering and Service Science (ICSESS'13)*, pp. 849–852, 2013.

[15] S. Jaiswal, K. Saxena, A. Mishra, S. K. Sahu. "A KNN-ACO approach for intrusion detection using KDDCUP'99 dataset," in *IEEE 3rd International Conference on Computing for Sustainable Global Development*, pp. 628–633, 2016.

[16] C. Li, R. Yan, C. Zhu, G. Gao, "Network intrusion detection based on Fast feature selection and ABQGSA-SVM", *Application Research of Computers*, vol. 33, pp. 75–78, 2017.

[17] A. J. Malik, and F. A. Khan, "A hybrid technique using binary particle swarm optimization and decision tree pruning for network intrusion detection," *Cluster Computing*, vol. 21, no. 1, pp. 667–680, 2018.

[18] D. S. A. Minaam, E. Amer, "Survey on machine learning techniques: Concepts and algorithms," *International Journal of Electronics and Information Engineering*, vol. 10, no. 1, pp. 34–44, 2019.

[19] I. Obeidat, N. Hamadneh, M. Al-Kasassbeh, *et al.*, "Intensive preprocessing of KDD cup 99 for network intrusion classification using machine learning techniques," *International Journal of Interactive Mobile Technologies*, vol. 13, no. 1, pp.70–84, 2019.

[20] S. D. Río, V. López, J. M. Benítez, and F. Herrera, "On the use of MapReduce for imbalanced big data using random forest," *Information Sciences*, vol. 285, pp. 112–137, 2014.

[21] R. Sharma, P. Sharma, P. Mishra, E. S. Pilli, "Towards MapReduce based classification approaches for intrusion detection," in *IEEE International Conference on Cloud System & Big Data Engineering*, pp. 361–367, 2016.

[22] Y. Shi, S. Abhilash, K. Hwang, "Cloudlet mesh for securing mobile clouds from intrusions and network attacks," in *IEEE International Conference on Mobile Cloud Computing, Services & Engineering*, pp. 109–118, 2015.

[23] R. Wakayama, R. Murata, A. Kimura, T. Yamashita, Y. Yamauchi, and H. Fujiyoshi, "Distributed forests for MapReduce-based machine learning," in *The 3rd IEEE IAPR Asian Conference on Pattern Recognition*, pp. 276–280, 2016.

[24] X. Wang, C. Zhang, K. Zheng, "Intrusion detection algorithm based on density, cluster centers, and nearest neighbors," *China Communications*, vol. 13, no. 4, pp. 24–31, 2016.

[25] B. Xue, M. Zhang, W. N. Browne, and X. Yao, "A survey on evolutionary computation approaches to feature selection," *IEEE Transactions on Evolutionary Computation*, vol. 20, no. 4, pp. 606–626, 2016.

[26] B. Xue and M. Zhang, "Evolutionary feature manipulation in data mining/big data," *ACM SIGEVOlution*, vol. 10, no. 1, pp. 4–11, 2017.

[27] J. Zhang, "Detection of network protection security vulnerability intrusion based on data mining," *International Journal of Network Security*, vol. 21, no. 6, pp. 979–984, 2019.

[28] Z. Zhang and B. Gu, "Intrusion detection network based on fuzzy C-Means and particle swarm optimization," in *Proceedings of the 6th International Asia Conference on Industrial Engineering and Management Innovation*, pp. 111–119, 2016.

[29] X. Zheng, Z. Ye, J. Sun, *et al.*, "Network intrusion detection based on hybrid rice algorithm optimized extreme learning machine," in *IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS'18)*, pp. 777–781, 2018.

Biography

Mugabo Emmanuel. He is a masters degree graduate from Lanzhou University of Technology. He graduated with a bachelor degree in Electronic Science and Communication from University of Dar-es-salaam (Tanzania) in 2014. His main research focuses on the network and information security.

Zhang Qiu-yu. 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 the 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.

Aristide Ngaboyindekwe. He is currently pursuing his master's degree at Lanzhou University of Technology. He received his Bachelor degree in Electronics and Communication Systems Engineering from the National University of Rwanda in 2012. From 2016, he started his master studies. His research interests are Future Internet Architecture, Security and Privacy in wireless networks and information, and Blockchain Technology.

Vincent de Paul Niyigena Kwizera. He is currently doing his master's degree at Lanzhou University of Technology in Control Theory and Control Engineering. He graduated with a Bachelor degree in Electronics and Communication Systems Engineering from University of Rwanda in 2016. His main research focuses on Intelligent Information Processing, Artificial Intelligence and Internet of Things.

Victus Elikplim Lumorvie. He is currently pursuing his Master's degree at Lanzhou University of Technology. He graduated with a bachelor degree in Computer Science and Engineering from the University of Mines and Technology (Ghana) in 2015. His Main research focuses on Network and Information Security.

Partitioned Group Password-based Authenticated Key Exchange with Privacy Protection

Hongfeng Zhu, Yuanle Zhang, Xueying Wang, and Liwei Wang
(Corresponding author: Hongfeng Zhu)

Software College, Shenyang Normal University
No. 253, HuangHe Bei Street, HuangGu District, Shenyang, P. C. 110034 - China
(Email: zhuhongfeng1978@163.com)
(Received June 20, 2019; Revised and Accepted Dec. 6, 2019; First Online Apr. 6, 2020)

Abstract

When a group Password-Based key exchange protocol is executed, the session key is typically extracted from two types of secrets: Shared keys (password) for authentication and freshly generated (nonces or timestamps) values. However, if one user (even subgroup users) runs the protocol with a non-matching password, all the others abort and no key is established. In this paper, we explore a more flexible, yet secure and privacy protection, GPAKE and put forward the notion of partitioned and privacy protection GPAKE, called PPP-GPAKE. PPP-GPAKE tolerates users that run the protocol on different passwords. Through a protocol run, any subgroup of users that indeed share a password, establish a temporary session key, and all the communication processes are user anonymity for outsiders by a temporary database helping. At the same time any two keys, each established by a different subgroup of users, are pair-wise independent if the corresponding subgroups hold different passwords. Compared with the related literatures recently, our proposed scheme can not only own high efficiency (only two communication rounds) and unique functionality, but is also robust to various attacks. Finally, we give the security proof and the comparison with the related works.

Keywords: Authentication; Group Key Agreement; Password; Privacy Protection

1 Introduction

With the popularization of network application, how to establish a secure channel between two nodes is a special problem worth considering. There is an increasing need for group PAKE [2] protocols to protect communications for a group of users. Although two-party password-authenticated key exchange (PAKE) protocols have been carefully studied for the past few years, group PAKE protocols have received much attention owing to it's a general settings. PAKE protocol is favored by cryptographers because of its short, low-entropy and easy-to-remember passwords for authentication. Low-entropy and human-memorable passwords are widely used for user authentication and secure communications in real applications, *e.g.* internet banking and remote user access, due to their user friendliness and low deployment cost. The problem of strong authentication and key exchange between two parties sharing a password, referred to as the two-party password-authenticated key exchange (2PAKE) problem, has been well studied and many solutions have been proposed in the literature.

With proliferation of group-oriented applications, *e.g.* teleconferencing, collaborative workspaces, there is an increasing need for group PAKE protocols to protect communications for a group of users. However, due to the low entropy of passwords, PAKE protocol is vulnerable to dictionary attacks. In dictionary attacks, an adversary tries to break the security of a protocol by exhaustive search. Dictionary attacks can be classified into three types: On-line (can be resisted by limiting number of attempts easily), off-line and undetectable on-line dictionary attacks, the two latter are not easy to resist. And group PAKE (GPAKE) is the natural extension to PAKE that empowers groups of more than two users to establish a session key, given that they share a common password. GPAKE focuses on a simpler, more realistic scenario where users only hold passwords, not credentials, and do not revoke them.

Consider the situation: Before participating in the GPAKE protocol, users must identify group members who claim to hold passwords. Then, the GPAKE protocol allows us to prove our understanding of passwords (and establish session keys). However, if only one user participates in the execution of the protocol with a different password, the user will be regarded as an active opponent and cause the user to terminate (even if all other users share the same password). The same principle is

applied in (non-cryptographic) group key exchange protocol: Whenever authentication fails, the user usually terminates the protocol execution and does not establish a joint key between those who successfully authenticate each other. In this paper, we design group key exchange more flexibly. That is, a packet PAKE protocol based on partition and privacy protection, PPP-GPAKE protocol. That is to say, if a user runs the protocol with a mismatched password, other users do not have to wait to establish the key again.

And in the paper, on the premise of GPAKE, we add the concepts of partition and privacy protection. For the concept of partition, we consider that it more convenient and flexible for users to perform some operations. Partitioned GPAKE defines natural applications in specific scenarios. For example, in the Internet of Things (IoT) cluster or a smart home which including many smart devices, and these devices belonging to the same user may need to establish a shared key (assuming that all devices of a given user have been initialized with the same password). In addition, in multi-user scenarios, different IoT or a smart home clusters belonging to different users will coexist, and key establishment in one group should not affect other groups. If a user (or even a subgroup) runs a protocol with a mismatched password, the shared password must be updated, which can be a very expensive process. For the other concept of security attribute, the privacy protection, which can ensure all the messages transmitting on the public channel are not plaintext. So, we call the new protocol PPP-GPAKE (partitioned and privacy protection GPAKE) which tolerates users that run the protocol on different passwords and owns the privacy protection. It is easy to see that PPP-GPAKE setting avoids the above problems and reduce the waiting time of users. We introduce here the new notion of PPP-GPAKE, aiming at designs suited for scenarios where the specific group of users sharing a password. That is, if there is a user password error, other users do not need to wait, and immediately form a new shared password.

Although the PAKE protocols have been studied to deal with multiple participants in a single domain for many years [5,7,13], it has many details are worth studying. Subsequently, with the increasing popularity of various types of group communication applications [9], including partitioned and privacy protection, a new research direction for PAKE protocols has moved gradually. In the next section, we discuss related work on PAKE protocols. Then we present our PPP-PAKE protocol, followed by the security proof. We analyze the performance of the proposed protocol and draw our concluding remarks at the end.

2 Security Model and Security Goals

Assuming that a public password dictionary $D \subseteq \{01\}^*$ to be efficiently identifiable and of constant or polynomial size. Especially, we assume that D can be enumerated by a polynomial bounded opponent.The set $S = \{U_1, \ldots, U_N\}$ of users is partitioned in $l \geq 2$ disjoint subsets, such that $S = U_1 \cup U_2 \ldots \cup U_l$. All users in U_δ, for $\delta = 1, \ldots, l$, share a public password $pw^\delta \in D$, with $pw^\delta \neq pw^\gamma$ given $\delta \neq_\gamma \in \{1, \ldots, l\}$. For simplicity's sake, we assume that all passwords are randomly selected from D, and are represented by a bit string of the same size (denoted by K).

2.1 Communication Model and Adversarial Capabilities

Protocol instances. Users are modeled as probabilistic polynomial time (ppt) Turing machines. Every user $U \in S$ parallelly and we use $\prod_i^j$ to consult the jth instance of user i, which can be regarded as a process executed by U_i. Every instance we distribute seven variables which are shown in Table 1. For more details on the variable usage, we refer to the work of Bellare *et al.* In [2].

Communication network. Assume that any point-to-point connections between users are available. The network is, nevertheless, non-private and completely asynchronous. More specifically, it is controlled by the opponent, who may delay, insert and delete messages at will.

Adversarial capabilities. We limit to probabilistic polynomial time (ppt) adversaries. The capabilities of an opponent A are made explicit through a number of oracles allowing A to communicate with protocol instances run by the users:

$Send(U_i, j, M)$. This oracle sends message M to the instance $\prod_i^j$ of U_i and returns the reply generated by this example. If A queries this oracle with an unused example $\prod_i^j$ and M being the set of users $\{U_{i_1}, \ldots, U_{i_\mu}\} \subseteq S$, going in for the protocol (including U_i), then the flag $used_i^j$ is set, and the first protocol message of $\prod_i^j$ for initializing a protocol run involving $\{U_{i_1}, \ldots, U_{i_\mu}\}$ is returned.

$Execute\left(\{\prod_{i_1}^{j_1}, \ldots, \prod_{i_\mu}^{j_\mu}\}\right)$. This oracle executes a complete protocol that run between specified unused instances of the respective users. The opponent gets a transcript of all messages sent over the network. A query to the Execute oracle should reflect passive eavesdropping. Especially, this Oracle can't guess passwords online.

$Reveal(U_i, j)$. Hand over the session key sk_i^j.

$Test(U_i, j)$. Active opponent A is only allowed to use one query of this form. Provided that sk_i^j is defined ($i.e. acc_i^j$ = true and $sk_i^j \neq$null), A can issue this query at any time when being activated. Then

Table 1: Variables

Variables	Definition
$used_i^j$	indicates whether this instance is being or has been used for a protocol run
$state_i^j$	keeps the state information needed during the protocol execution
$term_i^j$	indicates if the execution has terminated
sk_i^j	stores the session key once it is accepted by $\prod_i^j$. Before acceptance, it stores a distinguished $NULL$ value
sid_i^j	denotes a (possibly public) session identifier that can serve as an identifier for the session key sk_i^j
pid_i^j	stores the set of identities of those users that $\prod_i^j$ establishes a key with—including U_i himself [3]
P	Let P be a correct partitioned group password-authenticated key establishment protocol
acc_i^j	indicates if the protocol instance was successful, i.e. the user accepted the session key

with possibility 1/2 the session key sk_i^j and with possibility 1/2, a evenly chosen random session key is returned.

Corrupt (U_i). Returns the password *Corrupt* (U_i) held by U_i.

2.2 Correctness and Key Secrecy

2.2.1 Correctness

Our definition of correctness expands the standard one in GPAKE. Namely, without active countermeasure jamming, it should be the case that users holding matching passwords eventually set up a public session key as expected and assigning it the same name (sid). In addition, messages from users with mismatched password should not interrupt session key computations.

Definition 1. *(Correctness). Let D be a dictionary and S be a group of users as described earlier. After that, a partitioned group password-based key establishment protocol P is correct if there is a passive adversary A,*i.e. *A only uses the Execute oracle—a single execution of the protocol among* $U_{i_1}, \ldots, U_{i_\mu}$ *involves* μ *instances* $\prod_{i_1}^{j_1}, \ldots, \prod_{i_\mu}^{j_\mu}$ *and assures that with overwhelming possibility all examples:*

- *Accept,* i.e.$acc_{i_1}^{j_1} = \cdots = acc_{i_\mu}^{j_\mu} = true;$
- *Users belonging to the same subset* U_τ *the password-induced partition on S have accepted the same session key associated with the common session and partner identifier, that is* $\forall s,\ r \in \{1, \ldots, \mu\}$ *whenever* $U_{i_s}, U_{i_r} \in U_\tau$, *it holds* $sk_{i_s}^{j_s} = sk_{i_r}^{j_r} \neq NULL$, $sid_{i_s}^{j_s} = sid_{i_r}^{j_r}$ *and*

$$pid_{i_s}^{j_s} = pid_{i_r}^{j_r} \neq NULL.$$

(Note that if U_{i_s} *is the only user in* U_τ, *then she will end up with unique* $pid_{i_s}^{j_s}$, $sid_{i_s}^{j_s}$ *and* $sk_{i_s}^{j_s}$.*)*

2.2.2 Key Secrecy

Here we define the main security concepts of partitioned GPAKE protocols. In order to do so, we introduce the concepts of cooperation and novelty to indicate which instances are associated in a common protocol session, and how to exclude trivial attacks, separately.

Partnering. We adopt the concept of cooperation from [11] where instances $\prod_i^j$, $\prod_t^m$ are partnered if $sid_i^j = sid_t^m$,$pid_i^j = pid_t^m$ and $acc_i^j = acc_t^m$= true. Nevertheless, in [1], pid lists user instances engaging in a public protocol execution. In our scene, pid explicits instances that go in for a common protocol execution and share a password. In other words, in [3] and in other GPAKE suggests, a user defines pid at the beginning of the protocol, while in our settings, a user finds pid at the end of the protocol.

Note that the above concept of cooperation defines an equivalence relation on the set of possible instances (namely, it is reflexive, symmetric and transitive). In addition, to avoid trivial situations we assume that an instance $\prod_i^j$ always accepts the session key constructed at the end of the corresponding protocol operation, if no deviation from the protocol specification occurs. In addition, Non-confrontational interference, all users in the same protocol session belonging to the same subset U_k, *i.e.* with the same password, should come up with the same session key, store it under the same session identifier and know whom they share it with.

Freshness. This notion helps specifying under which conditions a Test-query can be executed by the opponent in the security experiment. An instance is called fresh if the opponent never made one of the following queries: $\prod_i^j$:

Corrupt(U_t) to any U_t holding the same password as U_t(*i.e.* so that U_i and U_t are both in U_τ for some $\tau \in \{1, \ldots, l\}$);

Reveal(U_t, m) with $\prod_i^j$ and $\prod_t^m$ being partnered.

The concept of novelty allows us to rule out trivial attacks. Especially, displaying a session key from an instance $\prod_i^j$ evidently yields the session key of all

instances partnered with $\prod_i^j$ and, hence, this kind of 'attack' is not take the security definition into account. In addition, note that this freshness definition means that corrupting users with different password from the one held by the uses specified in the Test query should be of no help to their opponents.

Key secrecy. Now that we have introduced cooperation and new concepts, we are ready to fully determine key confidentiality. As classic in password-based protocols, we observe that since the dictionary D has polynomial size we cannot prevent an adversary from correctly guessing a password $pw \in D$ used by any user. Hence, our goal is to limit the opponent A to verify password guesses online.

In the above setting, a protocol P is established for a fixed group key, let $Succ(\ell)$ be the possibility that an opponent A queries Test on a new instance $\prod_i^j$ and guesses correctly the bit b used by the Test oracle in a moment when $\prod_i^j$ is still fresh. Now we identify the advantages of A as the function

$$Adv_A(\ell) := |2Succ(\ell) - 1|.$$

We now introduce a function ε to capture the weaknesses that may due to the employed authentication technique; namely, as the opponent may guess passwords online, ε will explicit a bound on A's probability of guessing a shared password.

Definition 2. *(Key-secrecy). Let P be a correct partitioned group password-authenticated key establishment protocol, with D and S as mentioned above. Let A be a probabilistic polynomial time opponent with access to the Execute, Send, Reveal and Corrupt oracles. We say that P provides key secrecy, if for each such A, running in the experiment described in Section 2.1 and querying the Send oracle to at most q instances, the following inequality apply to some negligible function negl and some function ε which is at most linear in its second variable q:*

$$Adv_A(\ell) \leq \varepsilon(\ell, q) + \text{negl}(\ell).$$

Note that assuming passwords are chosen randomly and uniformly, and in each online attack, the opponent can only check a constant number of passwords, it holds $\varepsilon(\ell, q) = O(\frac{q}{|D|})$.

Remark 1. *Typically, in GAKE, the Corrupt oracle is used to model different flavors of forward security,* i.e. *to establish to what extent the leakage of authentication keys compromises the security of previously agreed session keys. In our scenario, however, corrupted users are to be understood as adversaries who might actually be legitimate members of a different password-defined subset U_δ. Thus, our model implicitly states that everyone who is not in the same password defined subset is understood as under adversarial control.*

2.3 Password Privacy and Privacy-Preserving

Unofficially, password-privacy ensures that an active opponent should not get any information about the use of passwords by legitimate users, so he should not even be able to tell if a given set of users really share the same password or not, unless he has guessed the involved password(s). Basically, if we consider the partition on the users set caused by the password allocation, then the opponents should not know about these partitions just by guessing wildly.

Interestingly, this concept is not relevant in many GPAKE proposals since, according to design, messages constructed from a non-matching password are typically recognized as maliciously generated and cause an abort (see for instance [6]). In fact, in this case, an active opponent may learn if two users U_i and U_t share the same password by starting a new session involving U_t and replaying messages generated by U_t in different executions. Now, the adversary just observes whether this rouge session is aborted or not. In contrast, in partitioned GPAKE protocols, executions always succeed and at their end, each participant eventually gets a valid key. However, only participants sharing the same password will share the same session key.

Our concept of password-privacy is rather inspired to that of affiliation hiding [10, 12] considered in authenticated key exchange. Association hiding means that an active opponent should not be able to obtain any information about group membership through a protocol execution (without considering trivial attacks where the opponent shares the affiliation of the victims). Especially, an opponent should not tell whether two users share the same affiliation or not. In our scenario, this means ensuring that no active opponent has access to information about the user's shared password, assuming he has not guessed the password used by any/some of them.

We use an indistinguishable game to simulate password privacy where the opponent A interacts with a challenger. First, he chooses the victim subgroup $U \subseteq S$ and two partitions p_0 and p_1 of it. Then the challenger randomly chooses one of the two partitions and assigns passwords (Random uniform selection) consistently with the corresponding subgroups. A wins if it can tell which of the two partitions has actually been chosen by the challenger, under the restriction that A cannot query the Reveal or Damage oracles on any of the users in U. We emphasize that in our game we do not assume passwords of all the remaining users in $S \backslash U$; These passwords can be even chosen by the opponent (*i.e.* the opponent can simulate any of these users himself).

Definition 3. *(Password-privacy). Let P be accurate partitioned GPAKE protocol. Consider a public dictionary D and (potential) set of users $S = \{U_1, \ldots, U_N\}$, where N is polynomial in the security parameter ℓ. Let A be a probabilistic polynomial time adversary interacting with a challenger Ch in the following game:*

1) *A selects a set of users $U \subseteq S$, and two partitions p_0 and p_1 of U.*

2) *Ch chooses a bit $b \in \{0,1\}$ uniformly at random and assigns a password, also chosen uniformly from the dictionary at random, for each subgroup of the partition p_b. In addition, he follows the specification of p.*

3) *A, equipped with Send and Execute, must output a guess.*

We say that P achieves password-privacy if every p.p.t. A wins the above password-privacy game with (at most) negligible probability over a random guess, provided he did not guess any password from a user in U. More precisely, for every p.p.t., let $Succ(\ell)$ be the probability that an adversary A guesses correctly the bit b selected by Ch. Now we define A's advantage as the function

$$Adv_A^{pwpri}(\ell) := |2.Succ(\ell) - 1|.$$

Let q denote the number of instances to which A has made a Send query. Then a protocol P has password-privacy if the following holds for some negligible function negl and some function ϵ which is at most linear in q,

$$Adv_A^{pwpri}(\ell) \leq \varepsilon(\ell, q)+\text{negl}(\ell),$$

our protocol has the privacy-preserving property which is realized by initiating two main ideas: firstly, the two partitions p_0 and p_1 can exchange the identity and nonces with an encrypted message using the shared password. And secondly, they can record the data in the temporary database as Table.3 does.

Definition 4. *(Privacy-preserving). Let P be a correct partitioned GPAKE protocol. Consider a public identity dictionary $\widetilde{ID}$ and (potential) set of users $S = \{U_1, \ldots, U_N\}$, where N is polynomial in the safety parameter ℓ. Let A be a probabilistic polynomial time adversary interacting with a challenger Ch in the following game:*

1) *A selects a set of users $U \subseteq S$, and two partitions p_0 and p_1 of U.*

2) *Ch chooses a bit $b \in \{0,1\}$ uniformly at random and assigns an identity, also be randomly selected from the identity dictionary $\widetilde{ID}$, for every subgroup of the partition p_b. Further, he follows the specification of p.*

3) *A, equipped with Send and Execute, must output a guess.*

We say that P achieves Privacy-preserving if every p.p.t. A wins the above Privacy-preserving game with (at most) negligible possibility over a random guess, the premise is that he did not guess any identity from a user in U. More precisely, for every p.p.t., let $Succ(\ell)$ be opponent A who correctly guesses the probability of bit B chosen by ch. Now we define A's advantage as the function $Adv_A^{idpri}(\ell) := |2Succ(\ell) - 1|$.

Let q denote the number of instances to which A has made a Send query. Then a protocol P has password-privacy if the following holds for some negligible function negl and some function ϵ which is at most linear in q, $Adv_A^{idpri}(\ell) \leq \varepsilon(\ell, q)+\text{negl}(\ell)$.

3 The Proposed PPP-GPAKE Protocol

3.1 The Settings and Notations

Now we are ready to show our concrete construction, as shown in Figure 1. And the Notations are described in Table 2. First of all, we introduce the main building blocks of our scheme:

1) A hash function H, which will be modeled as a random oracle; we assume it to range on $\{0,1\}^d$, for d polynomial in the security parameter ℓ,

2) A private key encryption scheme $\prod$= (KEYGEN, ENC, DEC), assumed to be secure in the unforgivable sense of existence and achieving chosen ciphertext security (see [8] and Section 3.1 above). For each choice of the security parameter, we will denote by ρ and C the corresponding polynomial sized plaintext and ciphertext spaces, and assume ρ to be an additive group. Furthermore, we will assume that KEYGEN selects keys uniformly at random from the range of the random oracle H.

3) An ideal cipher $\varepsilon : D \times G \mapsto \hat{G}$, $\varepsilon : \widetilde{ID} \times G \mapsto \hat{G}$, where D is the password dictionary and $\widetilde{ID}$ is the identity dictionary, G is a cyclic group of order q (polynomial in) and $\hat{G}$ is a finite set of q elements.

3.2 The Construction

Figure 1 illus trates the process of authenticated key agreement phase.

Round 1. When N participants want to create a group session key, each U_i chooses uniformly a random value $x_i \in \{1, \ldots, q-1\}$ and broadcasts $Y_i = \varepsilon_{pw_i}(U_i||g^{x_i})$. Each U_i will receive the messages (Y_t). If $\varepsilon_{pw_i}^{-1}(Y_t) = U_t||X_t \neq \perp$, then U_i sets $sid_{i,t} = U_i||Y_i||U_t||Y_t$ and computes $sk_{i,t} = H(U_i||U_t||X_i||X_t||X_t^{x_i})$. Otherwise U_i selects $sk_{i,t}$ equably at random in the range of H. Finally, for every U_t who holds a same two-party key as U_i, and user U_i defines the two-party key $sk_{i,t} = H(U_i||U_t||g^{x_i}||g^{x_t}||g^{x_i x_t})$, and a matching session identifier. Eventually, the user U_i stores $sid_{i,t}$ and the two-party key into a local temporary database, and the format are shown in the Table 3.

Table 2: Notations

Symbol	Definition
SK	the session key
Sid	session identifier
PW_A	Password of Alice
acc	the user accepted the session key
Adv_A	A's advantage as the function
p_0 , p_1	two partitions
P	Let P be a correct partitioned group password-authenticated key establishment protocol
$\|\|$	concatenation operation
$S = \{U_1,\ldots,U_N\}$	S is the collection of users
$Succ(\ell)$	$Succ(\ell)$ is the probability that an adversary A guesses correctly the bit b

Round 2. In the Round 2, each user U_i selects uniformly at random a value $r_i \in \{1,\ldots,q-1\}$ and broadcasts $M_{it} = (sid'_{i,t}, a_{it} = ENC_{sk_{i,t}}(r_i))$, where $sid'_{i,t} = Y_i||Y_t$. For each $t \neq i$, receiving the message M_{it}, U_t will compare $sid'_{i,t}$ with the database's records for getting the identity information $U_i||U_t$. Then, user U_t compute $c_{it} = DEC_{sk_{i,t}}(a_{ti})$ using $sk_{i,t}$ and sets $pid = \{i\} \cup \{t : c_{it} \neq \{r_i, \perp\}\}$ for every received messages $(sid'_{t,i}, a_{ti})$. Then select the database to get the identity information. Further, for each $t \in pid$, $t \neq i$, it sets $r^*_t = c_{it}$ and also $r^*_t = r_i$. Next is the knowledge of session key and session identifier definitions. User U_i sets $acc_i = true$, derives the (sub-group) key as the addition $sk_i = \sum_{l \in pid} r^*_l$, and also the session $identifier^b$ $sid_i = \{sid_{i,t}||a_{i,t}\}_{t \in pid_i}||pid_i$.

If any authenticated process fails, the protocol will be terminated immediately.

4 Security Analysis

4.1 Tools

4.1.1 Bellare, Pointcheval and Rogaway PAKE

Our major building block is the EKE2 PAKE proposed by Bellare *et al.* in [2] which is secure in the so-called ideal cryptographic model (see [4]). In this model, it is assumed that there exists a publicly accessible random block cipher with a k-bit key and a n-bit input/output, that is random selection of all block ciphers in this form. Besides, it is necessary to assume the existence of ideal random functions, that is to say, we will model the hash function H used in the key derivation process as a random oracle [14]. It has been proved that the two models are equivalent, as evidenced in [8].

4.1.2 Unforgeable Encryption

For the choice of the second building block, a symmetric encryption scheme $\prod$, we will choose structure that fully reflects the strong concept of unforgeability; Namely, we should not even allow our opponents to generate any new valid ciphertext without the private key. Such property is defined in [14] as existential unforgeability; We rewrite Definition 5 from that paper here:

Definition 5. *Let $\prod$= (KEYGEN,ENC, DEC) be a private-key encryption scheme. Let ℓ be the security parameter and A be any pptm algorithm. Define*

$\mathrm{Adv}^{exist}_{A,\prod}(\ell)$ == $\Pr[sk \leftarrow KEYGEN(1^\ell); y \leftarrow A : \mathrm{DEC}_{sk}(y) \neq \perp]$. *At this, y is produced by the adversary A which may use an encryption oracle ε_{sk}, yet y must not have been directly returned by ε_{sk}. We say that $\prod$ is $(t, p, b; \delta)$-secure in the sense of existential unforgeability if for any adversary A which runs in time at most t and asks at most p queries to the encryption oracle, these totaling at most b bits, we have $\mathrm{Adv}^{exist}_{A,\prod}(\ell) \leq \delta(\ell)$. Assuming t, p, and b, are polynomial in ℓ, if δ is negligible in ℓ we will simply say that $\prod$ is an unforgeable encryption scheme.*

Furthermore, in Theorem 1 of [14], it is proven that unforgeability along with chosen plaintext security means adaptive chosen ciphertext security. For our generic construction, we will make use of a symmetric key encryption scheme $\prod$ secure in this sense, therefore, we may assume that the adversary will cannot produce any valid ciphertext, nor to gain any information on the plaintexts underlying encrypted values. As evidenced in [14], such encryption scheme $\prod$ may simply be derived by instantiating appropriate block ciphers with unforgettable encryption patterns.

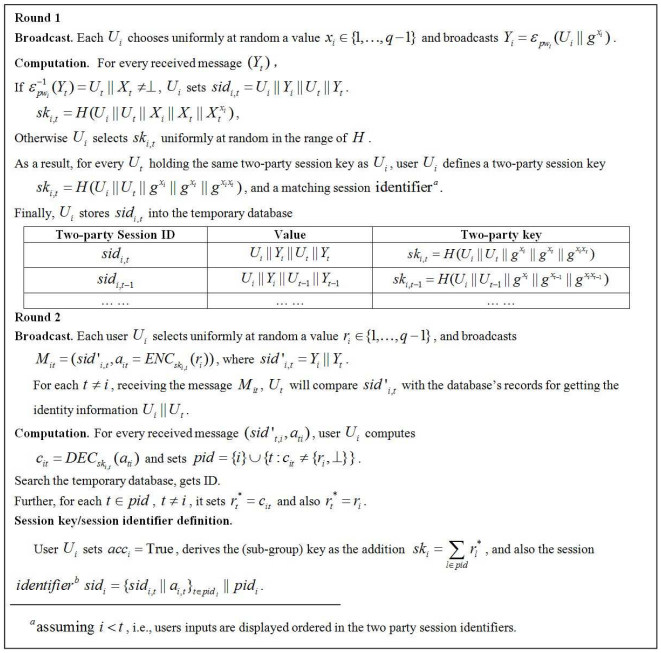
4.2 Security Proof

Theorem 1. *Let $\prod$= (KEYGEN, ENC, DEC) be a symmetric encryption scheme which is both unforgeable and chosen plaintext semantically-secure. Then, the protocol from Figure 1 is a correct partitioned password based group key agreement achieving key secrecy as defined in Definition 2 and password-privacy as defined in Definition 3 under the computational Diffie–Hellman assumption in group G in the random oracle/ideal cipher model.*

Correctness. In an true implementation of the protocol, it is easy to verify that all participants in the protocol

Table 3: The temporary database in the PPP-GPAKE protocol

Two-party Session ID	Value	Two-party key
$sid_{i,t}$	$U_i \| Y_i \| U_t \| Y_t$	$sk_{i,t} = H(U_i \| U_t \| g^{x_i} \| g^{x_t} \| g^{x_i x_t})$
$sid_{i,t-1}$	$U_i \| Y_i \| U_{t-1} \| Y_{t-1}$	$sk_{i,t-1} = H(U_i \| U_{t-1} \| g^{x_i} \| g^{x_{t-1}} \| g^{x_i x_{t-1}})$
… …	… …	… …



Round 1

Broadcast. Each U_i chooses uniformly at random a value $x_i \in \{1,\ldots,q-1\}$ and broadcasts $Y_i = \varepsilon_{pw_i}(U_i \| g^{x_i})$.

Computation. For every received message (Y_t),

If $\varepsilon^{-1}_{pw_i}(Y_t) = U_t \| X_t \neq \perp$, U_i sets $sid_{i,t} = U_i \| Y_i \| U_t \| Y_t$.

$sk_{i,t} = H(U_i \| U_t \| X_i \| X_t \| X_t^{x_i})$,

Otherwise U_i selects $sk_{i,t}$ uniformly at random in the range of H.

As a result, for every U_t holding the same two-party session key as U_i, user U_i defines a two-party session key

$sk_{i,t} = H(U_i \| U_t \| g^{x_i} \| g^{x_t} \| g^{x_i x_t})$, and a matching session identifier[a].

Finally, U_i stores $sid_{i,t}$ into the temporary database

Two-party Session ID	Value	Two-party key
$sid_{i,t}$	$U_i \| Y_i \| U_t \| Y_t$	$sk_{i,t} = H(U_i \| U_t \| g^{x_i} \| g^{x_t} \| g^{x_i x_t})$
$sid_{i,t-1}$	$U_i \| Y_i \| U_{t-1} \| Y_{t-1}$	$sk_{i,t-1} = H(U_i \| U_{t-1} \| g^{x_i} \| g^{x_{t-1}} \| g^{x_i x_{t-1}})$
… …	… …	… …

Round 2

Broadcast. Each user U_i selects uniformly at random a value $r_i \in \{1,\ldots,q-1\}$, and broadcasts

$M_{it} = (sid'_{i,t}, a_{it} = ENC_{sk_{i,t}}(r_i))$, where $sid'_{i,t} = Y_i \| Y_t$.

For each $t \neq i$, receiving the message M_{it}, U_t will compare $sid'_{t,t}$ with the database's records for getting the identity information $U_i \| U_t$.

Computation. For every received message $(sid'_{t,i}, a_{it})$, user U_i computes

$c_{it} = DEC_{sk_{i,t}}(a_{it})$ and sets $pid = \{i\} \cup \{t : c_{it} \neq \{r_i, \perp\}\}$.

Search the temporary database, gets ID.

Further, for each $t \in pid$, $t \neq i$, it sets $r_t^* = c_{it}$ and also $r_t^* = r_i$.

Session key/session identifier definition.

User U_i sets acc_i = True, derives the (sub-group) key as the addition $sk_i = \sum_{i \in pid} r_i^*$, and also the session identifier[b] $sid_i = \{sid_{i,t} \| a_{i,t}\}_{t \in pid_i} \| pid_i$.

[a] assuming $i < t$, i.e., users inputs are displayed ordered in the two party session identifiers.

Figure 1: An efficient partitioned GPAKE with privacy protection (PPP-GPAKE)

will terminate through accepting and computing the same session identifier and session key as participants with the same password.

Key secrecy. Evidence from several games, where a challenger interacts with the opponent confronting him with a counterfeit Test-challenge in the spirit of Definition 2. From game to game, the Challenger behaves differently from the previous one, with the corresponding effect on A's success probability. Following standard notation, we denote by $Adv(A, G_i)$ the opponent's advantage when confronted with Game i. The security parameter is denoted by ℓ.

In the sequel, we denote by q_{exe} the number of Execute calls made by the adversary. Also q will indicate the number of instances to which the opponent has launched a Send query, therefore, it is the number of instances that have suffered on-line attacks. In like wise,q_{ro} will express the number of queries A makes to the hash function H.

Game 0. This first game corresponds to a real attack, in which all the parameters are selected according to the actual scheme. By definition,

$$Adv(A, G_i) = Adv(A).$$

Game 1. We assume that the hash function H is simulated as a Random Oracle. Namely, each time a new query α is requested, the simulator selects u.a.r a value h_a from the range of H and stores the pair α, h_a in a table (from now on, the H-list). Should the value α be queried again, the simulator will look in the H-list and forward h_a as answer.

In addition, we explicit the ideal cipher simulation here. For a given password pw, the simulator will maintain an IC_{pw}-list in which for every query (pw,g) he stores a different value $\hat{g}$ which is selected uniformly at random in $\hat{G}$. Similarly, he also maintains a list capturing the decryption calls done to the Ideal Cipher (Called IC^{-1}_{pw}-list). Thus, a bijection $\sigma_{pw} : G \mapsto \hat{G}$ and list inverse are actually explicited by the two lists IC_{pw}-list, IC^{-1}_{pw}-list. The Random Oracle and the Ideal Cipher assumptions are made explicit by assuming

$$Adv(A, G_1) = Adv(A, G_0).$$

Game 2. In this game, we exclude certain conflicts of values chosen uniformly at random in different conversations. Namely, this game aborts in case the same exponent in Round 1 or the same random contribution in Round 2 is selected in different conversations by two (non-necessarily distinct) honest users. Similarly, we exclude the event that an Hcollision occurs at the time of extracting different two-party keys or session identifiers at the end of Round 1 in different protocol executions.

It is not hard to see that the difference between the two games

$$|Adv(A, G_2) - Adv(A, G_1)|,$$

the probability of 'partial collisions' on independent transcripts is bounded, which is in turn bounded by

$$\frac{q_{ro}^2}{2^d} + N^2 \left[\frac{1}{|G|} + \frac{1}{|\mathrm{P}|}\right],$$

where P is the plaintext space for $\prod$, from where the nonces are selected in Round 1.

Game 3. Consider the event that A queries the random oracle on the 5-tuple

$$(U_i \parallel U_t \parallel X_i \parallel X_t \parallel Z),$$

such that both the values X_i and X_t were generated by the simulator during the game and $Z{=}X_t^{x_i}$(essentially, if A queries the oracle on a valid CDH tuple). If such event (that we call Bad) happens, the simulation is aborted. Clearly,

$$|Adv(A, G_3) - Adv(A, G_2)| \leq P(Bad).$$

It is easy to see that for any adversary A that cause the Bad event to happen it is possible to construct another adversary B against the CDH assumption. The reduction is rather straightforward B, for inputting g^x, g^y, chooses a random index $q^* \leftarrow \{1, \ldots, q_{exe}\}$ and two user indices i, $t \leftarrow \{1, \ldots, N\}$ also at random. Then, in the q^*th protocol execution requested by the adversary B sets $X_i = g^x$ and $X_t = g^y$ for the users i and t, respectively. Finally, in the end of the game, it selects one random entry from H-list such that among the ones with $X_i = g^x$ and $X_t = g^y$, and returns the last value Z of the tuple. Clearly, if the event Bad occurs, and B guessed correctly the indices i, t, and q^*, then B found a solution for the CDH problem. Otherwise, if any of the guess was wrong, B aborts. It is not hard to see that

$$p(Bad) \times \frac{1}{q_{exe}} \frac{1}{N^2} \frac{1}{q_{ro}} \leq Adv_{G,g}^{CDH}(\ell),$$

where $Adv_{G,g}^{CDH}(\ell)$ is the probability that B has of winning a computational Diffie–Hellman challenge over G with generator g.

Game 4. Consider the event that A queries the random oracle on the 5-tuple

$$(U_i \parallel U_t \parallel X_i \parallel X_t \parallel Z),$$

such that the value X_t was generated by the simulator during the game, pw^* is the (random) password held by U_t whereas X_i is such that A made a query to the ideal cipher on input (pw^*, X_i) to get Y_i, and a Send query with the input (Y_i), because our scheme has privacy protection and for any adversary A that they just input the Y_i without the Identity of any user. If such event (that we call Bad^*) happens, the simulation is aborted. Clearly, $|Adv(A, G_4) - Adv(A, G_3)| \leq P(Bad^*)$. Now, the probability of the event Bad^* is bounded by the probability of a password guess, which is $O(q/|D|)$. We remark that from this point on in the simulation all H queries of the form $(U_i \parallel U_t \parallel X_i \parallel X_t \parallel X_i^{x_t})$, where users U_i and U_t sharing a password pw^* are either fully generated by the adversary or fully generated by the challenger. This means that for any two users sharing a password pw^* which has not been guessed by the adversary the corresponding two-party keys will be indistinguishable from random.

Game 5. This game deals with adversaries that only modify messages in Round 2, for the tested instance $\prod_i^j$. Precisely, consider any pair of users (U_i, U_t) for which the adversary had not made a random oracle query as the ones 'excluded' in the previous two games. Then if in the second part of the protocol execution the adversary A sends a valid message M_{it}^2 that decrypts correctly and is not a replay, then the game aborts.

With a simple reduction to the unforgeability of the encryption scheme M_{it}^2, it is possible to show that

$$|Adv(A, G_5) - Adv(A, G_4)| \leq Adv_{A\prod}^{exist}(\ell).$$

Where $Adv_{A\prod}^{exist}(\ell) \leq \delta(\ell)$, for some negligible function δ.

Game 6. Now, we modify the Execute and Send simulation in that we construct messages a_{it} as encryptions of 0, *i.e.* $a_{it} := ENC_{sk_{it}}(0)$. Precisely, this change is for all pairs of users (U_i, U_t) for which the adversary had not made a random oracle query as the ones excluded in the previous games. By relying on the CCA-security of $\prod$, one can argue that

$$|Adv(A, G_6) - Adv(A, G_5)| \leq Adv_{A\prod}^{CCA}(\ell).$$

After making this last change, the session key of a fresh session is completely random and independent from the simulated protocol transcript. Therefore, $Succ(\ell) = 1/2$, and the proof follows by putting together the bounds between the games.

Password privacy. The security proof for password privacy proceeds very similar to the one of key secrecy given above. The main idea is that after applying similar game changes as for key secrecy, the protocol messages become independent of the users passwords.

The games are defined as follows.

Game 0. This first game corresponds to a real attack, in which all the parameters are chosen as in the actual scheme. By definition, $Adv(A, G_0) = Adv(A)$.

Game 1. This is the same as Game 1 in the proof of Theorem 1. It simply makes explicit the simulation of the random oracle and the ideal cipher.

$$Adv(A, G_1) = Adv(A, G_0).$$

Game 2. This is the same as Game 2 in the proof of Theorem 1, and thus

$$|Adv(A, G_2) - Adv(A, G_1)| \leq \frac{q_{ro}^2}{2^d} + N^2 \left[\frac{1}{|G|} + \frac{1}{|P|}\right]$$

where P is the plaintext space for $\prod$, from where the nonces are selected in Round 1.

Game 3. This is the same as Game 3 in the proof of Theorem 1, and thus

$$\begin{aligned} & |Adv(A, G_3) - Adv(A, G_2)| \\ \leq \; & q_{exe} \cdot N^2 \cdot q_{ro} \cdot Adv_{G,g}^{CDH}(\ell). \end{aligned}$$

Game 4. This proceeds similarly to Game 4 in the proof of Theorem 1. Let us consider the event that A queries the random oracle on the 5-tuple $(U_i \parallel U_t \parallel X_i \parallel X_t \parallel Z)$,such that the value X_t was generated by the simulator during the game, pw_t^* is the (random) password held by U_t, whereas X_i is such that A made a query to the ideal cipher on input (pw_t^*, X_i) to get Y_i, and a Send query with the input (U_i, Y_i). If such event (that we call Bad^*) happens, the simulation is aborted. The difference between this and the previous game lies in the occurrence of event Bad^* whose probability is bounded by that of a password guess. Therefore,

$$\begin{aligned} |Adv(A, G_4) - Adv(A, G_3)| &\leq P(Bad^*) \\ &= O\left[\frac{q}{|D|}\right]. \end{aligned}$$

Game 5. This is the same as Game 5 in the proof of Theorem 3.2, and thus

$$|Adv(A, G_5) - Adv(A, G_4)| \leq Adv_{G,g}^{CDH}(\ell),$$

where $Adv_{G,g}^{CDH}(\ell) \leq \delta(\ell)$ for some negligible function δ.

Game 6. Finally, in this game, the challenger modifies the Execute and Send simulation by constructing messages a_{it} as encryptions of randomly selected values R_{it}, *i.e.*$a_{it} := ENC_{sk_{it}}(R_{it})$, while the session key is still computed using the randomly sampled values r_i. Based on the CCA-security of $\prod$ one can argue that

$$|Adv(A, G_6) - Adv(A, G_5)| \leq Adv_{A,\prod}^{CCA}(\ell).$$

In addition, after making this last change, the protocol messages in the simulation are independent of the password selection, and, in particular, are distributed identically in both the cases when the users in U share the same password pw^* or have each a different password. So, the probability that the adversary succeeds in correctly guessing the bit b in this game is $1/2 - Succ(\ell) = 1/2$. Therefore, by putting together the various bounds of the game differences, we have that the chances of A to win the password-privacy game are only negligibly above $1/2 + O[q/|D|]$.

Privacy-preserving. The process of proof is the same as the process of Password privacy. So, we can get the opportunity of A to win the Privacy-preserving game are only negligibly above $1/2 + O\left[q/|\widetilde{ID}|\right]$.

5 Conclusion

This work presents a PPP-GPAKE protocol which firstly combines group Password-Based key exchange protocol with the security attributes of privacy and partitioned which can tolerates the user entered the wrong password. The first key idea is using a temporary database to make the privacy of our scheme possible, and the other key idea is using subgroup to compute the middle two-party session keys for tolerating the entered wrong passwords of some users. Additionally, the proposed scheme is no need pre-shared secret key which can make the proposed protocol become more practical. Moreover, the proposed protocol has been shown secure under the random oracle model. In the future, we will study the PPP-GPAKE under the standard model instead of random oracle model, and give the PPP-GPAKE more secure properties with high efficiency.

Acknowledgements

This work was supported by the Liaoning Provincial Natural Science Foundation of China (Grant No. 2019-MS-286), and Shenyang Science & Technology Innovation Talents Program for Young and Middle-aged Scientists (2019).

References

[1] M. Abdalla, J. M. Bohli, M. I. G. Vasco, R. Steinwandt, "(Password) Authenticated key establishment: From 2-party to group," in *Lecture Notes in Computer Science (TCC'07)*, pp. 499–514, 2007.

[2] S. M. Bellovin, M. Merritt, "Encrypted key exchange: Password-based protocols secure against dictionary attacks," in *Proceedings IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 489-890, 1992.

[3] J. Black, P. Rogaway, "Ciphers with arbitrary finite domains," in *Ciphers with Arbitrary Finite Domains*, pp. 114–130, 2002.

[4] P. Chaidos, J. Groth, "Making sigma-protocols non-interactive without random oracles," in *Part of the Lecture Notes in Computer Science Book Series*, pp. 650-670, 2015.

[5] M. Chuangui, W. Fushan, G. Fengxiu, "Efficient client-to-client password authenticated key exchange based on RSA," in *Proceedings of the 5th IEEE International Conference on Intelligent Networking and Collaborative Systems*, pp. 233–238, 2013.

[6] R. Gelles, R. Ostrovsky, and K. Winoto, "Multiparty proximity testing with dishonest majority from equality testing," in *International Colloquium on Automata, Languages, and Programming*, pp. 537–548, 2012.

[7] X. Hu, Z. Zhang, "Cryptanalysis and enhancement of a chaotic maps-based three-party password authenticated key exchange protocol," *Nonlinear Dynamics*, vol. 78, no. 2, pp. 1293-1300, 2014.

[8] J. Katz, M. Yung, "Unforgeable encryption and chosen ciphertext secure modes of operation," in *Fast Software Encryption (FSE'00)*, *Lecture Notes in Computer Science*, , pp. 284–299, 2000.

[9] L. J. Liao, Z. I. Zhang, L. H. Zhu, "Computationally sound symbolic security reduction analysis of the group key exchange protocols using bilinear pairings," *Information Sciences*, vol. 20, no. 9, pp. 93–112, 2012.

[10] M. Manulis, B. Poettering and G. Tsudik, "AffiliationHiding key exchange with untrusted group authorities," in *Lecture Notes in Computer Science*, pp. 402–419, 2010.

[11] V. S. Naresh, S. Reddi, N. V. E. S. Murthy, "A provably secure cluster-based hybrid hierarchical group key agreement for large wireless ad hoc networks," *Human-centric Computing and Information Sciences,*, vol. 9, no. 1, pp. 1-32, 2019.

[12] A. Rivero-García, I. Santos-González, J. Munilla, M. Burmester, P. Caballero-Gil, "Secure lightweight password authenticated key exchange for heterogeneous wireless sensor networks," *Information Systems*, vol. 88, no. 101423, 2019. (`https://doi.org/10.1016/j.is.2019.101423`)

[13] B. Xiang, C. M. Chen, K. H. Wang, K. H. Yeh, T. Y. Wu, "Attacks and solutions on a three-party password-based authenticated key exchange protocol for wireless communications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 8, pp. 3133-3142, 2019.

[14] X. Yang, X. P. Sheng, M. Zhang, "A certificateless signature scheme with strong unforgeability in the random oracle model," *Journal of Computational Methods in Sciences and Engineering*, vol. 18, no. 3, pp. 715-724, 2018.

Biography

Hongfeng Zhu, obtained his Ph.D. degree in Information Science and Engineering from Northeastern University. Hongfeng Zhu is a full professor of the Kexin software college at Shenyang Normal University. He is also a master's supervisor. He has research interests in wireless networks, social networks, network security and quantum cryptography. Dr. Zhu had published more than 60 international journal and international conference papers on the above research fields.

Yuanle Zhang, a postgraduate studying at Shenyang Normal University. She has researched interests in network security and quantum cryptography. Under the guidance of the teacher, she has published one article in EI journals.

Xueying Wang, obtained her Ph.D. degree in Management Science and Engineering from Wuhan University. Xueying Wang is a Dean of the Kexin software college at Shenyang Normal University. She is also a full professor and a master's supervisor. She has research interests in cloud computing, social networks, network security and E-commerce. Dr. Wang had published more than 40 international journal papers on the above research fields.

Liwei Wang, a postgraduate studying at Shenyang Normal University. She has researched interests in network security and quantum cryptography. Under the guidance of the teacher, she has published one article in EI journals.

A Differentially Private K-means Clustering Scheme for Smart Grid

Shuai Guo[1], Mi Wen[1], and Xiaohui Liang[2]
(Corresponding author: Shuai Guo)
College of Computer Science and Technology, Shanghai University of Electric Power[1]
2103 PingliangRoad, 200090, Shanghai, China
Department of Computer Science University of Massachusetts[2]
100 Morrissey Boulevard, Boston, MA 02125, USA
(Email: g.shuai@mail.shiep.edu.cn)
(Received Sept. 7, 2019; Revised and Accepted Jan. 28, 2020; First Online Feb. 5, 2020)

Abstract

Cluster analysis via data mining is of great significance to smart grid for enabling power load analysis. However, the privacy-sensitive electricity consumption data may be leaked in the process of data mining. To address this problem, privacy-preserving data mining has been widely studied. This paper proposes an improved differentially private K-means clustering scheme while considering the unique characteristics of smart grid data. Using dimensionality reduction, the proposed scheme improves the effectiveness of data mining while preserving the data privacy. Performance evaluations are further conducted to illustrate that the proposed scheme outperforms the existing differential privacy preserving k-means clustering schemes.

Keywords: Differential Privacy; Dimensionality Reduction; K-means Clustering; Smart Grid

1 Introduction

With the development of smart grid and the progress of big data technology, smart grid data mining has entered a new stage. The smart meter plays a vital role in information collection. However, accurate real-time power usage data contain a wealth of sensitive personal information. For example, electric power consumers may be assumed to be sleeping or leaving home when their electricity consumption is very low. The privacy preservation for smart grid is of profound significance and has been widely studied.

The privacy information of smart grid customers may be stolen directly, or may be leaked indirectly in the data mining process, and this paper focuses on solving the latter issue. There are many ways to preserve the privacy of individuals, such as data perturbation, encryption, anonymity and other privacy-preserving techniques [8, 12, 18, 26]. However, if cryptography is used for encryption in the process of data mining, the data will lose the usability of analysis. On the other hand, recent studies have shown that the anonymized models such as k-anonymity and its extended model [20], l-diversity [13] and t-closeness [10] have some drawbacks. Firstly, these early models cannot analyze their privacy-preserving level quantitatively. Secondly, these models need to be continually improved to resist new types of attacks. These shortcomings undermine the reliability of these privacy-preserving techniques. Differential privacy [5] is a definition of privacy proposed by Dwork in 2006 to address the issue of privacy leakage in statistical database. In this definition, the computational processing of a data set is insensitive to specific changes of any one record, i.e. the impact on the computational results is minimal whether the single record is in this data set or not. It can resist a variety of attacks even if the attacker has the background knowledge. Based on the comparison above, this paper uses differential privacy techniques.

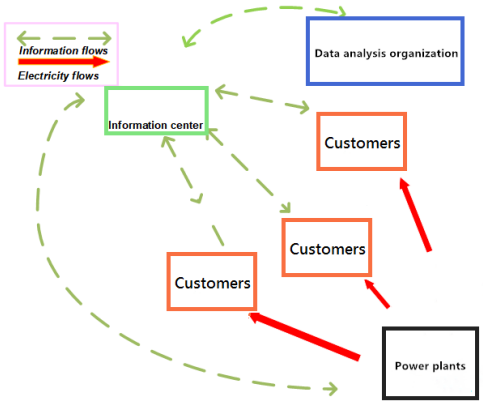


Figure 1: The architecture of the smart grid information system

In terms of information security and privacy preservation of smart grid, many data aggregation schemes [1, 19, 21] have been proposed to preserve the privacy of individual users. However, the current research on the privacy preservation of smart grid data mining is relatively rare. To compensate for the blank of privacy preservation in data mining in the smart grid, This paper introduces differential privacy into data analysis of smart grid.

Data mining has broad application prospects in smart grid. The distribution of energy and power load is unbalanced in power system and the unsupervised classification of power load is of great significance. Clustering analysis is an unsupervised classification method in data mining which can help formulate and adjust electricity price, predict the power load, and provide customers with personalized electric power services. The architecture of smart grid data analysis system is shown in Figure 1. Compared with traditional power grid, smart grid information systems are more intelligent and informative. The high-speed, two-way, real-time, integrated communications system makes the smart grid a large, dynamic, real-time information and power exchange interaction infrastructure, which is also a prerequisite for smart grid data mining. As a typical dynamic clustering algorithm, the K-means method is very effective and popular, and it is no exception in the data mining of smart grid. However, many proposed K-means clustering algorithms, calculating the distance between each sample point and the nearest central point, do not protect the data privacy [11]. For privacy preservation of clustering, there are some researches. Blum *et al.* [2] introduce a K-means algorithm with differential privacy. Dwork [6] improves the work [2] from the perspective of budget allocation of privacy preserving. Li *et al.* [9] propose a framework based on MapReduce calculation. Yu *et al.* [25] propose the Outlier-eliminated K-means clustering algorithm (OEDP), which considers the negative influence of outliers on the K-means algorithm and introduces a method to detect and eliminate outliers. Li *et al.* [11] propose an IDP K-means algorithm based on differential privacy preservation, which considers the influence of the selection of initial clustering centers, but its scheme for the selection of initial centers is simply to segment the data. Wang *et al.* [22] use local and global clustering methods to improve the effectiveness of mass data analysis under differential privacy preservation. These researches could still be improved to strike a better balance among data usability, privacy and efficiency while considering the unique characteristics of smart grid data.

To address this problem, we propose a K-means clustering method with differential privacy preservation for electricity consumption analysis. Specifically, the cleaning of the original data and the dimensionality reduction with Principal Components Analysis (PCA) can make data more suitable for clustering algorithm and the statistical regularity of the original data was maintained at the same time. The reduction of dimensions and the optimization of initial centers reduce the noise needed to be added, so that the usability of the clustering results is improved. Compared with similar algorithms, the proposed algorithm achieves a good balance among privacy preservation, the usability of clustering results and the scalability of cluster analysis.

The contributions of this paper are four folds:

- First, an improved K-means scheme is proposed for the clustering of electricity information while preserving the privacy of power grid customers.
- Second, the dimensionality reduction scheme using PCA and Singular Value Decomposition (SVD) are developed to optimize the process of clustering. It can significantly reduce the noise addition in the iteration and improve data usability.
- Third, the treatment of outliers is considered to make the clustering results more practical.
- Fourth, the proposed scheme is evaluated based on real-world electricity consumption data. Based on the evaluation results, it outperform the existing works in terms of accuracy, availability, and stability.

The rest of this article is organized as follows: after the introduction in Section 1, we introduce the relevant knowledge in Section 2. In the Section 3, we propose our scheme model. The Section 4 gives theoretical analysis and performance evaluations. Finally, the paper is summarized.

2 Preliminary Knowledge

This section introduces the relevant knowledge of differential privacy, clustering algorithm and dimensionality reduction.

2.1 Differential Privacy

Differential privacy is a popular technology for data security with strict mathematical proof, which ensure that whether a certain record is in the data set or not does not affect the statistical regularity, so that the data can be further used under the premise of privacy preserving.

2.1.1 The Defination of Differential Privacy

Differential privacy is proposed by Dwork [4] and is defined as follows:

$$P(M(D_1) \in E) \leq e^{\varepsilon} \cdot P(M(D_2) \in E),$$

where D_1 and D_2 are adjacent data sets with only one record difference, and M represents all possible output, P is the probability of something happening. Specifically, the differential privacy preservation guarantees that when the same query accesses to these two adjacent data sets,

the probability of the result is very close, i.e. there is little impact on the query results which are final released. Privacy budget ε is used to control the probability of that algorithm M gets the same output on two adjacent data sets. The smaller the ε, the higher the privacy preservation level. The value of ε should be determined to achieve a balance between the security and usability of output results [23].

2.1.2 The Sensitivity

Assume that D_1 and D_2 are adjacent data sets and there is the function $f : D \to R^d$, where d is the dimension of the output real-number vector, and the sensitivity is defined as

$$\Delta f = \max_{D_1, D_2} \left\| f(D_1) - f(D_2) \right\|_1,$$

where $\left\| f(D_1) - f(D_2) \right\|_1$ represents the 1 norm distance between $f(D_1)$ and $f(D_2)$.

Sensitivity is determined by the query function, regardless of the size of the data set. The higher the sensitivity, the more noise is needed to ensure that privacy is well protected, which will reduce the usability of data.

2.1.3 Laplace Mechanism

The Laplace mechanism is a widely used method for adding the noise required for differential privacy protection [7]. For data set D, there is a function $f : D \to R^d$, the sensitivity of the function is Δf and the value of random noise obeys the distribution $Y \sim Lap(b)$, where the scale parameter is $b = \Delta f/\varepsilon$. The probability density function of random noise is expressed as

$$p_r(x, b) = \frac{1}{2b} e^{(-\frac{|x|}{b})}.$$

And we say that the algorithm provides ε-differential privacy preservation.

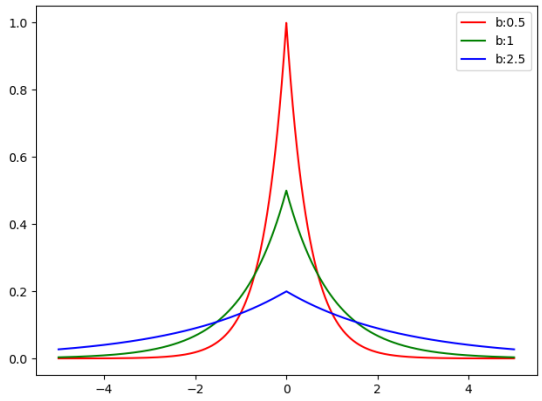


Figure 2: Laplace distribution

As shown in Figure 2, it can be seen that if ε is smaller, b is larger, then more noise is introduced, so the level of privacy preservation would be higher.

2.2 K-means Clustering

K-means clustering is a well-known partition clustering algorithm [17], which is widely used for its simplicity and efficiency. The steps of K-means are briefly described as follows: firstly, determine the initial central points, and the distance from each object point to each cluster center is calculated, and each point is assigned to the nearest cluster center. Secondly, recalculate the center of each cluster by the points that already exist in the cluster. Repeat this process until the specified requirements is met or

- No points are reallocated to different clusters;
- The clustering centers would not change;
- The sum of error squares is the least.

The objective function(the sum of error squares) is expressed as

$$v = \sum_{i=1}^{k} \sum_{x_j \in s_i} (x_j - u_i)^2,$$

where u is the clustering center, x means the sample point.

2.3 Dimensionality Reduction

This paper uses the idea of dimensionality reduction. The commonly used dimensionality reduction algorithms include PCA(Principal Components Analysis), Laplacian eigenmaps, Self-organizing mapping, Locally linear embedding and so on. Among them, PCA is an important multi-dimensional vector statistical analysis method in data compression and feature extraction, which is often used to reduce the dimension of high-dimensional data [14]. The reference of [27] shows that the computing time (including dimensionality reduction time and clustering time) of PCA is the shortest and the clustering effect of the reduced dimension data set is better in its scheme. SVD(Singular Value Decomposition) can be used for data compression and de-noising in the process of PCA dimension reduction. PCA needs to find the largest eigenvectors of the covariance matrix of the sample, and then use the matrix composed of the largest eigenvectors to do the low-dimensional projection. This calculation is inefficient when the number of samples or features is large. SVD can solve the right singular matrix without calculating the covariance matrix to simplify the computation. Therefore, this paper uses PCA and SVD to reduce the dimensions of the data. This method is more effective when the sample size is very large.

3 Proposed Differentially Private Clustering Scheme

To preserve the privacy of electric power consumers, an improved differential privacy clustering scheme is proposed for smart grid in this paper. Compared with existing differential privacy preservation algorithms, our

method improves the usability of clustering results while preserving users' privacy information. Specifically, after the information center collects electricity information, the data is cleaned and then sent to the analysis center. We divide the differentially private data mining for smart grid into two parts:

1) The fully trusted grid information center cleans the collected original information data, then reduces the dimension and establishes differential privacy protection;

2) Data analysis institutions carry out differentially private k-means data clustering on this basis.

According to the actual operation in data mining for the smart grid, differential privacy preservation is added to the process of K-means clustering in our scheme, and the clustering is improved by dimensionality reduction and outlier processing. As a result, the number of iterations and the complexity of clustering are reduced, making the higher usability of clustering results.

In the smart grid, because the collected data are very complex and original, the usability of original data can be improved by pre-processing or preliminary classification, but for clustering, the efficiency of high-dimensional data processing is very low. The reference of [3] summarizes it as the sparsity of high-dimensional data, the phenomenon of spatial emptiness and the dimensionality effect. Thus, in this paper, PCA and SVD are used to reduce the dimension of massive data, then the K-means clustering algorithm is used to clustering, and the differential privacy preservation is provided in the above process. Proposed scheme is mainly divided into dimensionality reduction and data clustering.

3.1 Dimension Reduction of Data

The original data obtained by information center of the smart grid needs to be cleaned before it is available for data mining, *e.g.*, the anonymization of some attributes, the processing of missing values. For the power consumption data, dimension reduction can be realized by manual allocation and automatic data reduction according to actual needs. In this paper, SVD and PCA are used to reduce the dimension of the cleaned data. In the meanwhile, refering to [24], the dimension reduction data is protected by the output disturbing privacy preserving algorithm.

3.2 Clustering Process

After dimensionality reduction, the first clustering and outlier detection are carried out. Obvious outliers are identified and then eliminated or classified into other clusters according to the specific circumstance. After that, further K-means clustering is started. In the clustering process, Laplacian noise is added to meet the differential privacy requirements. Finally, the clustering results are obtained.

In the second stage, we refer to the method of [25]. The main steps of the K-means scheme with ε-differential privacy preservation are as follows: First of all, input n d-dimensional points and divide these points into k parts on average. The average of each part will produce the points as $u_1 \cdots u_k$, then add noise to these points to generate new points $u'_1 \cdots u'_k$ as the initial central points and return them to the d dimensional space. The program will update as follows: (1) assign each sample point x_j to the nearest central point u'_i and divide the sample set D into k sets recorded as $s_1, s_2 \cdots s_k$ according to the central point. (2) for $1 \leq i \leq k$, $sum = \sum x_j$ and $num = |s_i|$ are calculated. Then the sum' and num' are obtained by adding noise respectively on the sum and the num. Update $u''_i = sum'/num'$ as the new central point of s_i. The above processes continue to iterate until the division of the sets meets the clustering requirements. The functional expression of the added noise is $Lap(b)$, where $b = \Delta f/\varepsilon$.

In this paper, the main steps of the experimental method are shown in Algorithm 1.

Algorithm 1 Proposed scheme

Input: the original dataset D, clusters s_i, k initial center points u_i, the number of clusters k, the sensitivity of query function b=$sensitivity/\varepsilon$, ε value

Output: clustering results

```
c ← Data cleaning (D)
c ← differentially private dimension reduction (c)
while the Sum of Squared Error does not converge do
    for j = 0 → c.lenth do
        d_j=dist(x_j, initial[u])
        d'_j ← minimum(d_j)
        partition x_j into the nearest center point's cluster
    end for
    for i = 0 → k do
        set sum_i=∑ x_j of the s_i cluster , num_i = |s_i|
        sum' = sum + Lap(b)
        num' = num + Lap(b)
        set new centerpoint u'' = sum'/num'
    end for
end while
```

4 Performance Evaluation

In this section, we evaluate the performance of the proposed scheme in terms of the effectiveness of differential privacy and the usability of clustering.

4.1 Analysis of Privacy Preservation and of the Usability of Clustering

4.1.1 Privacy Preserving

In this paper, Laplacian noise is added to the important part of electricity data mining. Assuming $M(D_1)$ and $M(D_2)$ correspond to the query results of the clustering of D_1 and D_2, According to the defination of differential privacy and the Laplace mechanism, we can see that $P(M(D_1) \in E)/P(M(D_2) \in E) \leq e^{\varepsilon}$ [16] which proves that our algorithm satisfies ε-differential privacy.

4.1.2 The Usability of Clustering Data

1) As mentioned above, the collected electricity consumption data are high-dimensional and very large, which may lead to the phenomenon of spatial emptiness and the dimensional effect. Therefore, in this paper, the dimension reduction method is used before the K-means algorithm for data clustering, which improves the usability from the data themselves.

2) The reduction of dimension makes clustering algorithm more effective, and the program runs faster. The processing of outliers after dimensionality reduction makes the central points more accurate.

3) Assume that D_1 and D_2 represent two data sets that differ from each other by only one record. When add or remove a point in a space $[0,1]^d$, the sensitivity is 1 for the sum of all dimensions. Therefore, the sensitivity of the entire query sequence is $d+1$. The description of noise addition in k-means algorithm is further given by Dwork [6]. Given that the number of iterations is N, the added noise follows the Laplace distribution

$$Lap((d+1)N/\varepsilon),$$

where d is the data dimension and ε is the level of privacy preservation. As shown in Figure 2, when the dimension d decreases obviously in this paper, the added noise decreases significantly, thus the overall usability of the data is improved.

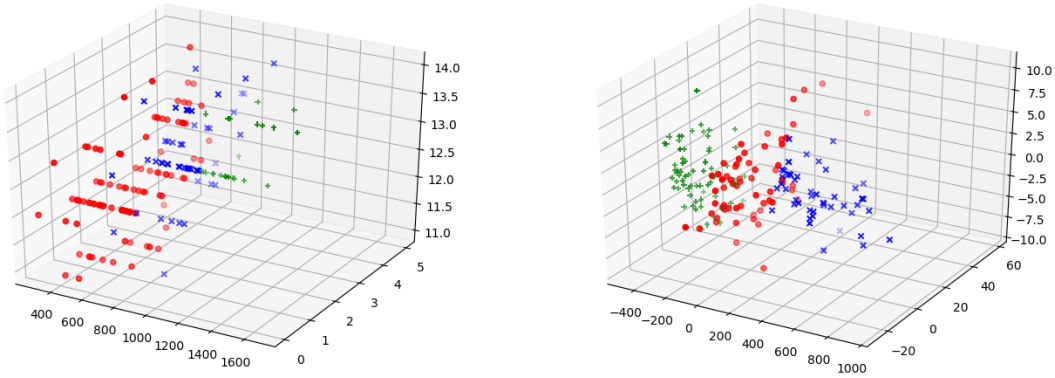
4.2 Experimental Analysis

In this paper, we use Python language to carry out the system simulation experiment. The source of the algorithm in this paper is the open-source algorithm in the computer field. The programming environment is JetBrains PyCharm2018. The experimental environment is Windows 10 AMD RYGEN 2200G 3.5GHz, 12.00GB, GTX1060 with CUDA core. And the data sets involved in our algorithm come from the University of CaliforniaIrvine (UCI) open-source data sets and partial open data sets of electricity.

Table 1: Data sets

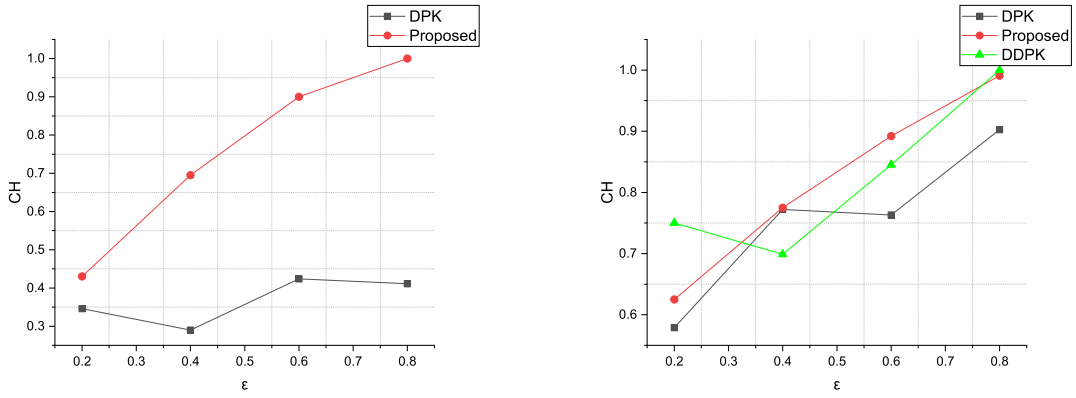
Data Set	Sample Size	Dimensions Size
Iris	150	4
Wine	178	13
Electricity data	400	5

We use the dimension reduction method based on PCA and SVD. In order to verify the effect of dimension reduction, we compare K-means clustering with or without dimension reduction on the Wine data set without adding noise. The experimental results are shown in Figure 3. Figure 3(a) represent the projection of the results of direct clustering of data sets on three attributes. Figure 3(b) shows the results of clustering after dimension reduction. Since the label of the wine data set is real, the k of two labs are set to 3. And the outlier detection is not used in these data sets. By comparing the two images, we can observe that the clustering results are more compact and easy to distinguish after dimensionality reduction. Since the data results are presented as projection, this intuitive comparison may be inaccurate. For quantitative analysis, at first, we use one of the internal evaluation indexes



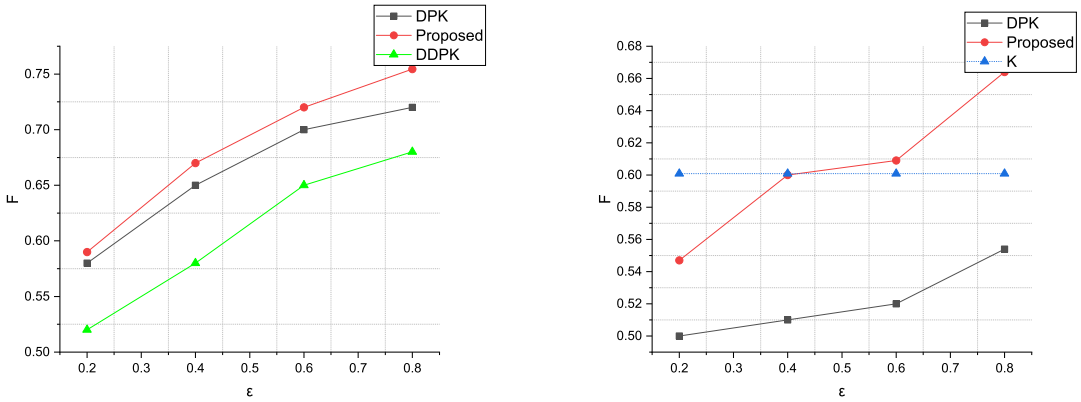
(a) (b)

Figure 3: The comparison between the results of the dimensionality reduction clustering and the results of the non-dimension reduction clustering



(a) (b)

Figure 4: Comparison of CH scores of running results on Wine and Iris data sets



(a) (b)

Figure 5: Comparison of F scores of running results on Iris and wine datasets

(Calinski-Harabasz score) to evaluate the density of clusters.

Unlike supervised classification or regression, unsupervised clustering usually has no sample output, so there is hardly any intuitive evaluation method for it. We can evaluate the clustering effect from the density of cluster and the degree of dispersion between clusters. Calinski-Harabasz Index is one of the popular internal evaluation methods [15]. The higher the value of Calinski-Harabasz(CH), the better the clustering effect. The mathematical expression of Calinski-Harabasz value is

$$s(k) = \frac{tr(B_k)}{tr(W_k)} \frac{m-k}{k-1},$$

where k is the number of categories, m is the number of samples, B_k is the inter-class covariance matrix, and W_k is the intra-class covariance matrix, and tr is the trace of the matrix. If the covariance of the data in the categories is smaller or the covariance between the categories is larger, the calinski-harabasz score will be higher. In this paper, to improve accuracy, the program for each ε value runs 10 times to get the average of CH. The experimental data and evaluation results are normalized.

On the Wine data set and the Iris data set, we compare the proposed scheme with the DPK [11] scheme. The DPK-means method differs from our proposed method in that it performs simple averaging processing on the data and then combines differential privacy techniques with clustering. The comparison results of CH values are shown in Figure 4(a)-(b). Through the comparison, it can be seen that our method has higher CH values, which shows that the proposed scheme is better than the DPK clustering on the internal index of clustering.

It is worth noting that we try a special method on the Iris data set. In order to simulate manual data dimensionality reduction, two-dimensional dimensionality reduction attributes (called DDPK here) are randomly selected to replace PCA and SVD, and the experimental results show high CH values. In fact, this is not an optimal solution because the randomly selected properties do not represent the original data set very well, as shown in Figure 5(a)(described later). Thus, to make the comparison of experiments more comprehensive, we use a combination of internal and external standards to evaluate our scheme.

F-measure is an external evaluation method for clus-

tering [25] which can compare the results with the real labels to evaluate the availability of clustering algorithms. Assume that n represents the size of the data set, i represents the correct class label of the data set, j represents the cluster result label, the precision(P) is $P(i,j) = |P_i \bigcap C_j|/|C_j|$ and the recall (R) is $R(i,j) = |P_i \bigcap C_j|/|P_i|$. F-measure is defined as follows:

$$Fmeasure(i,j) = \frac{(\beta^2+1)\cdot P(i,j)\cdot R(i,j)}{(\beta^2)\cdot P(i,j)+R(i,j)};$$
$$F = \sum_i \frac{n_i}{n} max_j\{Fmeasure(i,j)\}.$$

According to Figure 5(a) and Figure 5(b), we can observe that the F value of our scheme is higher than that of DPK-means clustering algorithm, which shows that the clustering results of our algorithm are closer to the reality and shows the better usability of cluster. In some cases, it is even better than the direct k-means clustering without adding noise(The blue line named K in Figure 5, there is actually no value of ε). At the same time, we can see that the clustering results of the DDPK method mentioned above are less accurate. More detailed data is given in the appendix as shown in Table 2 and Table 3. All these prove the higher clustering availability of our scheme.

Table 2: Comparison of F score on Wine dataset

Scheme	**ε=0.2**	**ε=0.4**	**ε=0.6**	**ε=0.8**
DPK-means	0.501	0.510	0.522	0.554
K-means	0.601			
Proposed	0.547	0.600	0.609	0.664

Table 3: Comparison of F score on Iris dataset

Scheme	**ε=0.2**	**ε=0.4**	**ε=0.6**	**ε=0.8**
DPK-means	0.580	0.649	0.701	0.725
Proposed	0.591	0.669	0.720	0.754
DDPK-means	0.520	0.577	0.651	0.678

Finally we make an experimental comparison on the real consumers' electricity consumption data. The data set is from UMassTraceRepository. We evaluate the property as five dimensions:

1) Power consumption ratio during peak hours, electricity consumption during peak hours/total electricity consumption.
2) Load rate, average load/maximum load of household users.
3) Valley electricity coefficient, electricity consumption in trough period/total electricity consumption.
4) Electricity consumption percentage in off-peak time.
5) The period of time when electricity consumption is at its highest.

Since there is no established label in the real data sets, we use CH values for evaluation as shown in Figure 6. We divide energy consumer into 5 categories and set the principal component contribution rate to 90%. And we mark the records that with all zero values as outliers. Compared with the DPK-means method, we can see that our clustering effect is much better. We randomly select some samples in each cluster in the clustering results and get average values of them, and the results are shown in Figure 7, which shows the usage habits and characteristics of different consumers.

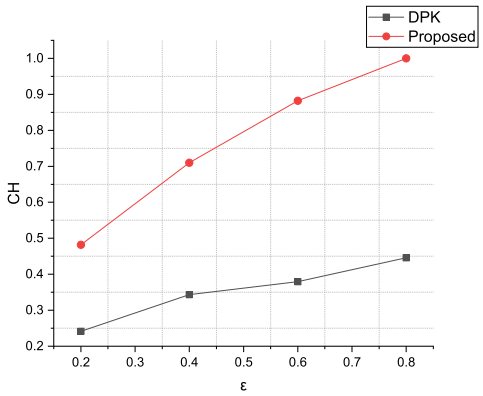


Figure 6: Comparison of CH scores of running results on electricity data sets

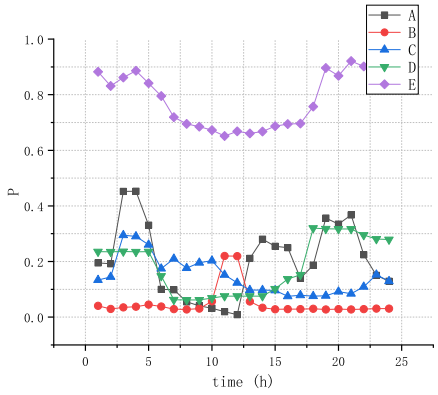


Figure 7: Typical curve

According to our research and experimental comparison, the proposed scheme considers the availability of data while preserving the privacy of power users, and achieves good results in actual data sets. In practical work, our scheme will better support the privacy preservation of the smart grid data mining process.

5 Conclusion

In the process of smart grid data mining, it is particularly important to preserve the privacy information of power consumers. To meet the requirement of maintaining the usability of clustering while preserving privacy, this paper proposes a mining scheme for smart grid based

on K-means clustering with differential privacy preservation. The algorithm of data clustering is improved by dimensionality reduction combined with outlier elimination. Comparing with other schemes, performance evaluations show that the proposed method improves the accuracy of clustering and the confidentiality of data.

For our future work, since there are many other methods for data mining, we intend to explore the privacy preservation for other methods in data mining. Furthermore, we intend to improve our scheme from the optimization of K-means algorithm, and explore the wider application of the scheme proposed in this paper.

Acknowledgments

This study is supported by the National Natural Science Foundation of China under Grant No.61872230 and No.61572311. We are very grateful to the reviewers for their valuable comments.

References

[1] M. Badra and S. Zeadally, "An improved privacy solution for the smart grid," *International Journal of Network Security*, vol. 18, no. 3, pp. 529–537, 2016.

[2] A. Blum, C. Dwork, F. Mcsherry, and K. Nissim, "Practical privacy: The SuLQ framework," in *Twenty-fourth Acm Sigmod-sigact-sigart Symposium on Principles of Database Systems*, 2005. (`http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.126.209&rep=rep1&type=pdf`)

[3] J. Chen, *K-Harmonic Means Clustering Method and Its Application on High-Dimensional Data*, PhD thesis, 2012.

[4] C. Dwork, "Differential privacy," in *International Colloquium on Automata, Languages, and Programming*, vol. 4052, pp. 1-12, 2006.

[5] C. Dwork, "Differential privacy: A survey of results," in *International Conference on Theory and Applications of Models of Computation*, pp. 1-19, 2008.

[6] C. Dwork, "A firm foundation for private data analysis," *Communications of the Acm*, vol. 54, no. 1, pp. 86–95, 2011.

[7] C. Dwork, F. McSherry, K. Nissim, A. Smith, "Calibrating noise to sensitivity in private data analysis," *Theory of Cryptography*, vol. 3876, no. 8, pp. 265–284, 2006.

[8] M. Hwang, T. Sun, and C. Lee, "Achieving dynamic data guarantee and data confidentiality of public auditing in cloud storage service," *Journal of Circuits Systems and Computers*, vol. 26, no. 5, pp. 1750072, 2016.

[9] H. Li, X. Wu, and Y. Chen, "k-means clustering method preserving differential privacy in mapreduce framework," *Journal on Communications*, vol. 37, no. 2, pp. 124–130, 2016.

[10] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *IEEE International Conference on Data Engineering*, 2007. DOI: 10.1109/ICDE.2007.367856.

[11] Y. Li, Z. Hao, W. Wen, and G. Xie, "Research on differential privacy preserving k-means clustering," *Computer Science*, vol. 40, no. 03, pp. 287–290, 2013.

[12] L. Liu, W. Kong, Z. Cao, and J. Wang, "Analysis of one certificateless encryption for secure data sharing in public clouds," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 110–115, 2017.

[13] A. Machanavajjhala, D. Kifer, and J. Gehrke, "L -diversity: Privacy beyond k -anonymity," *Acm Transactions on Knowledge Discovery from Data*, vol. 1, no. 1, pp. 3, 2007.

[14] Y. N. Rao and J. C. Principe, "A fast, on-line algorithm for PCA and its convergence characteristics," in *Neural Networks for Signal Processing X, IEEE Signal Processing Society Workshop*, 2000. DOI: 10.1109/NNSP.2000.889421.

[15] J. Ren, J. Xiong, Z. Yao, R. Ma, and M. Lin, "DPLK-means: A novel differential privacy k-means mechanism," in *IEEE Second International Conference on Data Science in Cyberspace (DSC'17)*, pp. 133–139, 2017.

[16] J. Ren, J. Xiong, Z. Yao, M. Rong, and M. Lin, "DPLK-means: A novel differential privacy k-means mechanism," in *IEEE Second International Conference on Data Science in Cyberspace*, 2017. DOI: 10.1109/DSC.2017.64.

[17] Y. Salim, M. Latief, N. Kandowangko, and R. Yusuf, "Comparison analysis of the artificial neural network algorithm and k-means clustering in gorontalo herbal plant image identification system," in *The 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT'18)*, pp. 50–55, 2018.

[18] N. Sang, X. Mengbo, and Q. Quan, "Clustering based k-anonymity algorithm for privacy preservation," *International Journal of Network Security*, vol. 19, no. 6, pp. 1062 – 1071, 2017.

[19] H. Shen, M. Zhang, and J. Shen, "Efficient privacy-preserving cube-data aggregation scheme for smart grids," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1369–1381, 2017.

[20] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.

[21] X. Tian, Q. Song, and F. Tian, "Multidimensional data aggregation scheme for smart grid with differential privacy," *International Journal of Network Security*, vol. 20, no. 6, pp. 1137 – 1148, 2018.

[22] B. Wang, H. Hu, and S. Zhang, "Differential privacy protection based clustering analysis of electricity consumption data for massive consumers," *Automation of Electric Power Systems*, vol. 42, no. 2, pp. 121–127, 2018.

[23] P. Xiong, T. Zhu, and X. Wang, "Differential privacy protection and its application," *Chinese Journal of Computers*, vol. 37, no. 1, pp. 101–122, 2014.
[24] Y. Xu, G. Yang, Y. Bai, and W. Wang, "Differential privacy data publish algorithm for principal component analysis," *Information Security and Technology*, vol. 9, no. 10, pp. 74–82, 2018.
[25] Q. Yu, Y. Luo, C. Chen, and X. Ding, "Outlier-eliminated k-means clustering algorithm based on differential privacy preservation," *Applied Intelligence*, vol. 45, no. 4, pp. 1179–1191, 2016.
[26] H. Zhu and R. Wang, "A survey to design privacy preserving protocol using chaos cryptography," *International Journal of Network Security*, vol. 20, no. 2, pp. 313–322, 2018.
[27] Y. Zhou, C. Zheng, X. Jian, W. Xiu, and G. Xu, "Ensemble clustering algorithm combined with dimension reduction techniques for power load profiles," *Proceedings of the Csee*, vol. 35, no. 15, pp. 3741–3749, 2015.

Biography

Shuai Guo received the B.S. degree in Electrical Engineering and Automation from Linyi University in 2015. He is currently pursuing the M.S. degree in information technology of electric power at Shanghai University of Electric Power. His current Acknowledgments research interests include data mining, privacy preserving and machine learning.

Mi Wen received the M.S. degree in Computer Science from University of Electronic Science and Technology of China in 2005 and the Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China in 2008. She is currently a Professor of the College of Computer Science and Technology, Shanghai University of Electric Power. She was a visiting scholar at University of Waterloo, Canada from May 2012 to May 2013. She keeps acting as the TPC member of some conferences such as IEEE INFOCOM, IEEE ICC, IEEE GLOEBECOM, etc. from 2012. Her research interests include privacy preserving in wireless sensor network, smart grid, etc.

Xiaohui Liang is an Assistant Professor with the Department of Computer Science at University of Massachusetts, Boston (UMB) where he leads the Mobile Security and Privacy (MobSP) Lab. He received the PhD degree in Electrical and Computer Engineering, University of Waterloo, Canada, in 2013. He received the BSc and MSc degree in Computer Science from Shanghai Jiao Tong University, China, in 2006 and 2009, respectively. His research interests are Security and Privacy for Communication and Networking Systems, Mobile Healthcare, Internet of Things, and Wearable Computing. He has published over 100 refereed journal and conference papers.

Additively Homomorphic IBE with Auxiliary Input for Big Data Security

Zhiwei Wang[1], Congcong Zhu[1], Nianhua Yang[2], and Zhanlin Wang[3]
(Corresponding author: Zhiwei Wang)
School of Computer Science, Nanjing University of Posts and Telecommunications[1]
Nanjing 210023, China
School of Statistics and Information,Shanghai University of International Business and Economics[2]
Shanghai 201620, China
Yangzhou Shuren School, Yangzhou, China[3]
(Email: zhwwang@njupt.edu.cn)
(Received July 6, 2019; Revised and Accepted Dec. 11, 2019; First Online Feb. 3, 2020)

Abstract

Additively homomorphic encryption is a relaxed notion of homomorphic encryption, which enables us to compute linear functions over the encrypted data. Additively homomorphic identity-based encryption (IBE) is an efficient resolution tool for the problem of security with privacy in the big data applications. In this paper, we design a leakage resilient additive homomorphic IBE scheme with auxiliary input to resist side-channel attacks for the end users. We prove that our scheme is auxiliary input chosen-plaintext attack (AI-CPA) secure, and test our scheme over the resource-constrained Intel Edison Platform. Both theoretical analysis and experimental result show that our scheme is very suitable for aggregating data submitted from the end users, who may be at the risk of leaking their secret keys.

Keywords: Additively Homomorphic IBE; Auxiliary Input; Big Data; CPA Secure; Security with Privacy

1 Introduction

Many novel applications, such as cloud systems, smart mobile phones, social networks, and Internet of Things (IoT), are leading to process and share huge amounts of data, which is called *big data* [5]. There are three characteristics for the definition of big data.

1) *Volume* - data sizes are very huge, and rang from terabytes to zettabytes.

2) *Variety* - the structures of data have many different formats, like image, sounds, and videos which are difficult to be analyzed.

3) *Velocity* - in many applications, data continuously arrive at high frequencies, and result in high speed data streams. We want to extract useful information from big data, such as patterns and predict trends. Big data are making some tasks possibly, which were difficult before, like preventing crime, identifying new opportunities in business, personalizing healthcare and supporting precision agriculture. The utilization of big data for many confidential and privacy sensitive tasks make data security with privacy to be an important issue. Pervasive data aggregating from multiple sources, such as smart phones, smart electronic meters, further exacerbates the problem of data privacy [27, 29, 35].

Data privacy becomes more critical than over in almost all applications. Although data confidential is important to achieve data privacy, data privacy still has some additional requirements. For example, managing consents of user's personal data, and complying with privacy related regulations [2]. Designing privacy-enhancing techniques becomes very active in recent years. As a result, many such techniques have been proposed, such as homomorphic encryption that supports computation on encrypted data [30], and differential privacy technique that transforms the data to make difficult to link special data records to the special individuals [7]. Other researches focus on data privacy in different application domains, such as smart grid [17], social networks [8]. Although such large number of research efforts have been made, data privacy is still a challenge problem in the era of big data. There are many critical research directions in data privacy, like efficiency of privacy-enhancing techniques [16], security with privacy [31], and data sharing.

Security with privacy may be a special issue in data privacy. Some researches focus on data security, such as Wang *et al.*'s attribute-based encryption scheme for big data security [25], Wang *et al.*'s blind batch encryption-based protocol for smart health [24].

However, security and privacy are usually conflicting requirements. If we want to achieve security, then we should harm privacy; while we want to keep up privacy, we may give up security. However, recently advances in applied cryptography are making possible to be security with privacy.

Homomorphic encryption is an important one among these cryptographic techniques. Gentry *et al.* constructed a *fully homomorphic encryption* scheme supporting arbitrary functions f over encrypted data [13]. More recently, further fully homomorphic schemes [4, 15, 18, 34] were presented following Gentry's framework. A critical aspect of Gentry's fully homomorphic encryption scheme and all the subsequent schemes is the ciphertext refreshing, which is called *Recrypt* operation. Although large number of research efforts have been made to improve this operation, fully homomorphic encryption schemes are still very costly for the practical applications [26].

Since fully homomorphic encryption will incur a huge computational overhead with current state of the art, we relax the requirements of homomorphic encryption in some specific applications so that we can implement it efficiently.

Additively homomorphic encryption is such a relaxed notion, which can be used to aggregate the data submitted from users, without sacrificing their privacy [14]. For example, a main concern of smart grid is that the fine-grained metering data may leak customers' privacy information. If additively homomorphic encryption is used to this scenario, then the electronic power provider (ESP) can only get the total power consumption data to monitor the power supply, but cannot analyze it with fine granularity [12]. In contrast to what we usually require from a fully homomorphic cryptosystem, decryption of additively homomorphic encryption scheme returns the correct result only if it is numerically small enough. It is suitable for calculating small values such as temperature measurements, pow consumption data or prices, which is sufficient for many big data applications. There many public-key encryption (PKE) systems can be modified to additively homomorphic encryption scheme by trivial adjustments. These include: Pallier cryptosystem [22], Regev cryptosystem [23], and Okamoto-Uchiyama cryptosystem [21] etc. In practical, many end users in big data applications utilize public-key certificates for identity identifications and cryptographic session establishments, but it requires too much time and processing to periodically update cryptographic keys. Thus, the Cloud Security Alliance (CSA) recommended identity-based encryption (IBE) for big data applications [9]. Felix *et al.* realized an efficient additively homomorphic IBE scheme [12] by slightly modifying the Boneh *et al.*'s IBE scheme [6].

Another important issue for the application of additively homomorphic IBE scheme is how to resist the side channel attacks, by which attackers can learn partial information about the secret key through observing physical properties of a cryptographic scheme execution such as power assumption, radiation, and temperature etc. As we know, many end devices in big applications are exposed to the open air, such as wireless sensors and smart meters. The notion of *leakage resilient cryptography* has been proposed, and a large number of efforts have been made in this topic. In general, there are three leakage models have been proposed.

1) *Bounded retrieval model* [11, 20], the total number of bits leaked over the lifetime of system is bounded, and hope the attack is detected and stopped before the whole secret is leaked;

2) *Continual leakage model* [3], it is assumed the leakage between consecutive updates is bounded in term of a fraction of the secret key size, and the secret key should be refreshed continually.

3) *Auxiliary input model* [10, 28, 32], it allows any uninvertible leakage function f that no probabilistic polynomial-time (PPT) attacker can compute the actual pre-image with non-negligible probability. That is to say, even such a function information-theoretically reveals the entire secret key SK, it still computationally infeasible to recover SK from $f(SK)$.

This paper aims to propose an efficient additively homomorphic IBE scheme in auxiliary input model. The key point for the designing of cryptographic schemes in auxiliary input model is how to split the secret key into m pieces, which is the "hardcore" of modified Goldreich-Levin theorem [10]. The modified Goldreich-Levin theorem states that if the pieces of secret key belong to a field $GF(q)$ (q is a λ-bit prime), then the running time of inverter is closed to $poly(2\lambda)$[1], which cannot be born by the inverter.

The contributions of this paper can be listed as follows.

1) We design an additively homomorphic IBE scheme with auxiliary input from Felix *et al.*'s scheme [14], which not only achieves leakage resiliency, but also keeps up the property of additively homomorphic.

2) From the property of strong extractor used in our construction, we prove that our scheme is auxiliary input chosen-plaintext attack (AI-CPA) secure.

3) To evaluate the appropriacy of our scheme for the resource constrained devices, we implement our scheme over the Intel Edison Platform which is a development system for Internet of Things devices. The experimental result shows that our scheme is efficient enough for aggregation data submitted from the

[1]We denote the polynomial function of λ as $poly(\lambda)$.

constrained-resource end users at the risk of leaking their secret keys.

Organization. Security model of IBE with auxiliary input is defined in Section II. Section III provides a definition of strong extractor with auxiliary input. We design an additive homomorphic IBE scheme with auxiliary input in Section IV. Section V discusses the performance of our scheme on the platform of MacBook Pro and Edison. Finally, we conclude our paper in Section VI.

2 Security Model of IBE with Auxiliary Input

We denote the negligible function of λ as notation $negl(\lambda)$. Let $\mathcal{M}$ denote the message space and $\mathcal{C}$ denote the ciphertext space. An identity-based encryption scheme Π consists of four PPT algorithms:

Setup(1^λ): Generates the master public/secret keys mpk and msk.

Extract(ID, mpk, msk): Outputs a private key sk_{ID} on an identity $ID \in \{0,1\}^*$.

Enc(M, ID, mpk): Encrypts a message $M \in \mathcal{M}$ to a ciphertext $C \in \mathcal{C}$.

Dec(C, sk_{ID}): Decrypts a ciphertext $C \in \mathcal{C}$ to a message $M \in \mathcal{M}$.

If for all $ID \in \{0,1\}^*$, $M \in \mathcal{M}$, we have $Dec(mpk, Extract(mpk, msk, ID), Enc(mpk, ID, M)) = M$, then we call the IBE scheme Π is correct.

Additively Homomorphic IBE: If for all $ID \in \{0,1\}^*$, $M, M' \in \mathcal{M}$, we have $Dec(mpk, Extract(mpk, msk, ID), Enc(mpk, ID, M) \cdot Enc(mpk, ID, M')) = M + M'$, then we call the IBE scheme Π is additively homomorphic.

Next, we introduce the security model of IBE with auxiliary input, which is similar to the classic IND-ID-CPA (indistinguishable identity chosen-plaintexts attack) model and the auxiliary input model. Let $\mathcal{F}$ denote a polynomial-time computable leakage function family. Let $\Gamma = (Setup, Extract, Enc, Dec)$ be an IBE scheme, and we define the security model as follows:

Setup: The challenger runs $(mpk, msk) \leftarrow Setup(1^\lambda)$, and sends mpk to the attacker $\mathcal{A}$. The challenger also maintains an empty list $\mathcal{L}_{ID}$.

Query 1: The following queries can be issued by $\mathcal{A}$.

Extract Query: When $\mathcal{A}$ makes an extract query on an $ID \in \{0,1\}^*$ and an index i, the challenger firstly checks $\mathcal{L}_{ID}$ for the tuple (sk_{ID}, ID, j). If there is no such tuple in $\mathcal{L}_{ID}$, then the challenger sets j to 1, and runs $sk_{ID} \leftarrow Extract(ID, msk, mpk)$ and puts (sk_{ID}, ID, j) to $\mathcal{L}_{ID}$. Otherwise, the sk_{ID} from the tuple (sk_{ID}, ID, j) is returned.

Leakage query: When $\mathcal{A}$ chooses $f \in \mathcal{F}$ for the leakage query on secret keys, the challenger returns $f(msk, mpk, ID, \mathcal{L}_{ID})$.

Challenge: $\mathcal{A}$ sends two messages M_0 and M_1 with the same length and an identity ID^* to the challenger. The challenger chooses a random bit b, and returns $C^* \leftarrow Enc(mpk, ID^*, M_b)$ to $\mathcal{A}$.

Query 2: $\mathcal{A}$ is allowed to make extract queries adaptively.

Output: $\mathcal{A}$ outputs a guess bit b' of b.

If $b' = b$ and there is no extract query on ID^*, then $\mathcal{A}$ wins the above game. If the advantage of $\mathcal{A}$ $Pr[\mathcal{A}wins] - 1/2$ is negligible, then the IBE scheme Γ is IND-ID-CPA secure with auxiliary input.

Definition 1. *An IBE scheme is AI-CPA (auxiliary input CPA) secure if it is IND-ID-CPA secure with auxiliary input.*

3 Strong Extractor with Auxiliary Input

Definition 2. ***(One-way hash function family)*** *[33] Let $\mathcal{H}_{ow}(\epsilon)$ be the class of all polynomial-time computable functions $h : \{0,1\}^{|x|} \to \{0,1\}^*$. If it satisfies that given $h(x)$, where x is randomly generated, no PPT algorithm can recover x with probability greater than ϵ, then $\mathcal{H}_{ow}(\epsilon)$ is called a one-way hash function family. Here, the function $h(x)$ can be a composition of q functions: $h(x) = \{h_1(x), \cdots, h_q(x)\}$, and $\{h_1(x), \cdots, h_q(x)\} \in \mathcal{H}_{ow}(\epsilon)$.*

Then, we introduce the definition of strong extractor based on one-way hash function family [33].

Definition 3. ***((ϵ, δ)-Strong extractor with auxiliary input)*** *Let $SE : Z_p^m \times Z_p^m \to Z_p$, where m is polynomial in λ. SE is called a (ϵ, δ)-strong extractor with auxiliary input, if for any PPT attacker $\mathcal{A}$, given all $f(\boldsymbol{x})$ such that $\boldsymbol{x} \in Z_p^m$ and $f \in \mathcal{H}_{ow}(\epsilon)$, we have $|Pr[\mathcal{A}(\boldsymbol{s}, f(\boldsymbol{x}), SE(\boldsymbol{s}, \boldsymbol{x}) = 1)] - Pr[\mathcal{A}(\boldsymbol{s}, f(\boldsymbol{x}), \gamma = 1)]| < \delta$, where $\boldsymbol{s} \in Z_p^m$, $\gamma \in Z_p$ are randomly chosen.*

Let $< \mathbf{s}, \mathbf{x} >= \sum_{i=1}^{m} s_i x_i$ denote the inner product of vector $\mathbf{s} = (s_1, \cdots, s_m)$ and $\mathbf{x} = (x_1, \cdots, x_m)$. From the modified Goldreich-Leivin theorem, we can construct a (ϵ, δ)-strong extractor with auxiliary input. Let's review the modified Goldreich-Leivin theorem [10] as follows.

Theorem 1. ***(Modified goldreich-leivin theorem)*** *Let q be a big prime, and let H be any subset of $GF(q)$. Let f map from $H^{\bar{m}}$ to $\{0,1\}^*$ be any polynomial-time computable function. Then a vector $\boldsymbol{x}$ is uniformly random chosen from $H^{\bar{m}}$, and we have $y = f(\boldsymbol{x})$. Then,*

randomly selects a vector $\boldsymbol{s}$ *from* $GF(q)^{\bar{m}}$*, and* γ *is randomly chosen from* $GF(q)$*. If a PPT distinguisher* $\mathcal{A}$ *runs in time* t*, and there exists a probability* ϵ *such that*

$$|Pr[\mathcal{A}(y, \boldsymbol{s}, <\boldsymbol{x}, \boldsymbol{s}>) = 1] - Pr[\mathcal{A}(y, \boldsymbol{s}, \gamma) = 1]| = \epsilon,$$

then there exists an inverter $\mathcal{B}$ *who can compute* $\boldsymbol{x}$ *from* y *in time* $t' = t \cdot poly(\bar{m}, |H|, 1/\epsilon)$ *with the probability*

$$Pr[\boldsymbol{x} \leftarrow H^{\bar{m}}, y \leftarrow f(\boldsymbol{x}) : \mathcal{B}(y) = \boldsymbol{x}] \geq \frac{\epsilon^3}{512 \cdot m \cdot q^2}.$$

We show that a (ϵ, ϵ')-strong extractor with auxiliary input can be constructed from inner product by using the modified Goldreich-Leivin theorem.

Theorem 2. *Let* $\boldsymbol{x}$ *be randomly chosen from* $Z_p^{m(\lambda)}$ *where* $m(\lambda) = poly(\lambda)$ *and* λ *is the security parameter. Similarly, we randomly choose* $\boldsymbol{s}$ *from* $Z_p^{m(\lambda)}$ *and* γ *random from* Z_p*. Then, given* $f \in \mathcal{H}_{ow}(\epsilon)$*, no PPT attacker can distinguish* $(\boldsymbol{s}, f(\boldsymbol{x}), <\boldsymbol{s}, \boldsymbol{x}>)$ *from* $(\boldsymbol{s}, f(\boldsymbol{x}), \gamma)$ *with probability* $\epsilon' \geq (512m(\lambda)p^2\epsilon)^{1/3}$

Proof. Let $H = Z_p$ and $\bar{m} = m(\lambda)$. We assume that there exists an algorithm that can distinguish $(\mathbf{s}, f(\mathbf{x}), <\mathbf{s}, \mathbf{x}>)$ from $(\mathbf{s}, f(\mathbf{x}), \gamma)$ with the probability ϵ'. According to the modified Goldreich-Leivin theorem, there exists an inverter $\mathcal{B}$ that runs in time $t' = t \cdot poly(m(\lambda), p, 1/\epsilon)$ such that $Pr[\mathcal{B}(f(\mathbf{x})) = \mathbf{x}] \geq \frac{\epsilon'^3}{512 \cdot m(\lambda) \cdot p^2} \geq \epsilon$ if $\epsilon' \geq (512m(\lambda)p^2\epsilon)^{1/3}$. It contradicts the one-way property of $f \in \mathcal{H}_{ow}(\epsilon)$, and thus we construct a (ϵ, ϵ')-strong extractor with auxiliary input from inner product. □

4 Additively Homomorphic IBE with Auxiliary Input

We firstly review the definition of bilinear pairing map. Assuming that G and G_T are two cyclic groups with the prime order p, we define $e : G \times G \rightarrow G_T$ be the bilinear map as it has the following properties:

1) Bilinear: $\forall g_1, g_2 \in G, a_1, a_2 \in Z_p$, $e(g_1^{a_1}, g_2^{a_2}) = e(g_1, g_2)^{a_1 a_2}$.
2) Non-degenerate: $\exists g \in G$, $e(g, g) \neq 1$.
3) Efficient computability: There exists an efficient algorithm to compute $e(g_1, g_2)$ for all $g_1, g_2 \in G$.

4.1 Review of an Additively Homomorphic IBE Scheme

In this section, we review Felix *et al.*'s additively homomorphic IBE scheme [14], which consists of four PPT algorithms.

Setup(1^λ)**:** Takes a security parameter λ as input, and generates the bilinear group parameters $(G, G_T, g, p, e : G \times G \rightarrow G_T)$, where g is a generator of G, and G and G_T are all the prime order groups with order p. Let $g_t = e(g, g)$. Randomly chooses $x \in Z_p$ and sets $y = g^x$. Fixes a cryptographic hash function $H : \{0,1\}^* \rightarrow G$. The message place is $\mathcal{M} = Z_M \subset Z_p$ with $M = q(\lambda) < p$ for some polynomial q. Then, the master public key is $mpk = (G, G_T, g, g_t, p, e, y, H)$, while the master secret key is $msk = x$.

Extract(mpk, msk, ID)**:** Generates the identity based secret key as $sk_{ID} = H(ID)^x$.

Enc(mpk, ID, M)**:** Randomly chooses $r \in Z_p$ and outputs the ciphertext as $C = (g^r, g_t^M \cdot e(H(ID), y)^r)$.

Dec(mpk, sk_{ID}, c)**:** Computes $M_t = \frac{g_t^M \cdot e(H(ID), y)^r}{e(sk_{ID}, g^r)}$ and $M = \log_{g_t} M_t$ as the discrete log of M_t on the base of g_t[2].

The additively homomorphic property of this scheme can be described as: $C \cdot C' = (g^r \cdot g^{r'}, g_t^M \cdot e(H(ID), y)^r \cdot g_t^{M'} \cdot e(H(ID), y)^{r'}) = (g^{r+r'}, g_t^{M+M'} \cdot e(H(ID), y)^{r+r'}) = Enc(mpk, ID, M + M')$.

4.2 Construction of Additively Homomorphic IBE with Auxiliary Input

Our leakage resilient additively homomorphic IBE scheme with auxiliary input can be described as follows:

Setup(1^λ)**:** Generates the bilinear group parameters $(G, G_T, g, g_t, p, e : G \times G \rightarrow G_T)$ as Felix *et al.*'s scheme. Randomly chooses $x_1, \cdots, x_m \in Z_p$ and sets $y_1 = g^{x_1}, \cdots, y_m = g^{x_m}$. Fixes a cryptographic hash function $H : \{0,1\}^* \rightarrow G$. The master public key is $mpk = (G, G_T, g, g_t, p, e, y_1, \cdots, y_m, H)$, while the master secret key is $msk = (x_1, \cdots, x_m)$.

Extract(mpk, msk, ID)**:** Generates the identity based secret key as $sk_{ID} = (H(ID)^{x_1}, \cdots, H(ID)^{x_m})$.

Enc(mpk, ID, M)**:** Randomly chooses $s_1, \cdots, s_m \in Z_p$ and outputs the ciphertext as $C = (g^{s_1}, \cdots, g^{s_m}, g_t^M \cdot \prod_{i=1}^m e(H(ID), y_i)^{s_i})$.

Dec(mpk, sk_{ID}, c)**:** Computes $M_t = \frac{g_t^M \cdot \prod_{i=1}^m e(H(ID), y_i)^{s_i}}{\prod_{i=1}^m e(H(ID)^{x_i}, g^{s_i})}$ and $M = \log_{g_t} M_t$ as the discrete log of M_t on the base of g_t.

The correctness of decryption can be depicted as follows:

$$\begin{aligned} & \frac{g_t^M \cdot \prod_{i=1}^m e(H(ID), y_i)^{s_i}}{\prod_{i=1}^m e(H(ID)^{x_i}, g^{s_i})} \\ = & \frac{g_t^M \cdot \prod_{i=1}^m e(H(ID), y_i)^{s_i}}{\prod_{i=1}^m e(H(ID), g^{x_i})^{s_i}} \\ = & \ g_t^M. \end{aligned}$$

[2]Here M should be only polynomial size.

The additively homomorphic property can be depicted as follows:

$$\begin{aligned} & C \cdot C' \\ = \; & (g^{s_1} \cdot g^{s'_1}, \cdots, g^{s_m} \cdot g^{s'_m}, g_t^M \cdot \prod_{i=1}^{m} e(H(ID), y_i)^{s_i} \\ & \cdot g_t^{M'} \cdot \prod_{i=1}^{m} e(H(ID), y_i)^{s'_i}) \\ = \; & (g^{s_1+s'_1}, \cdots, g^{s_m+s'_m}, g_t^{M+M'} \cdot \prod_{i=1}^{m} e(H(ID), y_i)^{s_i+s'_i}) \\ = \; & Enc(mpk, ID, M+M') \end{aligned}$$

4.3 Security Proof

Felix *et al.* have proved that their additive homomorphic IBE scheme is CPA secure under Decisional Bilinear Diffie-Hellman (DBDH) assumption [14]. Let Π' denote Felix *et al.*'s scheme and Π denote our scheme. We prove that the security of our scheme relies on Felix *et al.*'s scheme without the random oracles as follows.

Theorem 3. *If SE is a $(\epsilon, neg(\lambda))$-strong extractor with auxiliary input, then Π based on Π' is AI-CPA secure with respect to the family $\mathcal{H}_{ow}(\epsilon_x)$.*

Proof. Let s denote $gcd(s_1, \cdots, s_m)$, $\mathbf{s}$ denote the vector $(s_1/s, \cdots, s_m/s)$ and $\mathbf{x}$ denote the vector $x_1, \cdots, x_m)$. $SE : Z_p^m \times Z_p^m \rightarrow Z_p^m$ is a $(\epsilon, neg(\lambda))$-strong extractor with auxiliary input. In Π' scheme, the ciphertext is $g_t^M \cdot e(H(ID), y)^r$, which implies $g_t^M \cdot e(H(ID), g^x)^r$. In our scheme Π, the ciphertext is $g_t^M \cdot \prod_{i=1}^{m} e(H(ID), y_i)^{s_i}$, which can be denoted as $g_t^M \cdot e(H(ID), g^{SE(\mathbf{s},\mathbf{x})})^s$. That is to say, in Π scheme, the secret key x is substituted by the strong extractor $SE(\mathbf{s}, \mathbf{x})$ with auxiliary input.

Let $Game_0$ be the AI-CPA secure game with the scheme Π. $Game_1$ is the same as $Game_0$ except that when encrypting the challenge ciphertext, we substitute a random number $\gamma \in Z_p$ for $SE(\mathbf{s}, \mathbf{x})$. The leakage oracle outputs $f_i(\mathbf{x})$ for the both games.

Let $Adv_{\mathcal{A}}^{Game_i}(\Pi)$ denote the advantage of an attacker $\mathcal{A}$ winning in $Game_i$ with the scheme Π. We should prove that for any PPT attacker $\mathcal{A}$, $|Adv_{\mathcal{A}}^{Game_0}(\Pi) - Adv_{\mathcal{A}}^{Game_1}(\Pi)| \leq negl(\lambda)$. Now, we assume that $|Adv_{\mathcal{A}}^{Game_0}(\Pi) - Adv_{\mathcal{A}}^{Game_1}(\Pi)| \geq \epsilon$ which is non-negligible.

The challenger $\mathcal{C}$ is given $(\mathbf{s}, f_1(\mathbf{x}), \cdots, f_q(\mathbf{x}), T)$ where T is either $T_0 =< \mathbf{s}, \mathbf{x} >$ or $T_1 = \gamma$ which is a random number in Z_p. From the definition of $\mathcal{H}_{ow}(\epsilon_x)$, no PPT attacker can recover $\mathbf{x}$ with the probability greater than ϵ_x, given $f_1(\mathbf{x}), \cdots, f_q(\mathbf{x})$. Then, the challenger $\mathcal{C}$ runs $(mpk, msk) \leftarrow Setup(1^\lambda)$ and $sk_{ID} \leftarrow Extract(mpk, msk, ID)$, and gives mpk to the attacker $\mathcal{A}$. $\mathcal{C}$ can answer all the leakage queries as it has (mpk, msk, sk_{ID}). Finally, $\mathcal{A}$ sends two messages M_0 and M_1 with the same length to $\mathcal{C}$ where $\mathcal{C}$ randomly chooses a bit b. Then, $\mathcal{C}$ encrypts M_b to get the challenge ciphertext c^* by using T, and returns c^* to $\mathcal{A}$. Then, $\mathcal{A}$ outputs its guess bit b' to $\mathcal{C}$. If $b' = b$, then $\mathcal{A}$ wins the game; otherwise, it loses.

Since we assume that $|Adv_{\mathcal{A}}^{Game_0}(\Pi) - Adv_{\mathcal{A}}^{Game_1}(\Pi)| \geq \epsilon$, we can get $|Pr[b' = b|T_1] - |Pr[b' = b|T_1]| \geq \epsilon$ easily, which is non-negligible. However, it contradicts the property of strong extractor $SE(\mathbf{s}, \mathbf{x})$. Thus, no PPT attacker can distinguish $Game_0$ and $Game_1$ with non-negligible probability.

Then, we can easily find that $Adv_{\mathcal{A}}^{Game_1}(\Pi) = negl(\lambda)$, since the challenge ciphertext in $Game_1$ involves a random number γ not $SE(\mathbf{s}, \mathbf{x})$. Thus, the answers of leakage queries $f_i(\mathbf{x})$ in $Game_1$ are useless, and they will not disclose any information related to the challenge ciphertext. Then $Game_1$ is the same as the CPA game with Π'. Since Π' has been proved CPA secure, we have that $Adv_{\mathcal{A}}^{Game_1}(\Pi)$ is negligible. Thus, Π scheme is AI-CPA secure with respect to the one way hash family $\mathcal{H}_{ow}(\epsilon_x)$. □

5 Performance Analysis

We implement our additively homomorphic IBE scheme with auxiliary input over a resource-limited platform, which is the Intel Edison development platform with a dual-core, dual-threaded Intel Atom CPU at 500 MHz and 1GB RAM, running Yocto Linux v1.6. As we all know, many end users in big data applications are resource-constrained, like wireless sensors and smart meters. The Intel Edison development platform is considered as a good choice to rapidly prototype the Internet of Things (IoT) devices. And thus, Intel Edison development platform can simulate the end devices in big data applications perfectly. We implement our scheme in C by using the pairing based cryptography (PBC) library [19], which has been implemented the basic arithmetic and pairing operations. There are seven types of curves in PBC, and we choose the fastest Type-A curves for the implementation, where the group order is 160bits long, and the order of the base field is 512bits long.

Paillier *et al.*'s additive homomorphic encryption scheme [22] also can be modified to a leakage resilient scheme with auxiliary input using the ϵ, δ)-Strong Extractor. We also implement Paillier *et al.*'s additive homomorphic encryption scheme with auxiliary input for comparing it with our scheme. To achieve the security level recommended by National Institute of Standards and Technology (NIST), we choose the length of modulus $|N| = 1024bits$.

Fig 2. shows the time costs of encryption algorithm in our scheme and Paillier's scheme. The cost of our scheme is a little better than Paillier's scheme. In the experiment, m doest not require to be set very large. For example $m = 10$, according to the Theorem 2, the distinguish probability is $\epsilon' \geq (512m(\lambda)p^2\epsilon)^{1/3}$, we have that $p = 512$, $\epsilon \leq \frac{1}{160^{10}}$ and $\epsilon' \geq (\frac{512^3 \cdot 10}{160^{10}})^{1/3} \approx \frac{1}{80^{10}}$. Such probability is very negligible, both our scheme and paillier's scheme can achieve leakage resilient to auxiliary input. Fig 3. shows the time costs of decryption algorithm in our scheme and

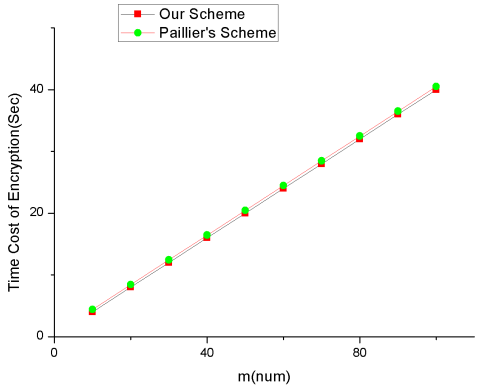


Figure 1: Time cost of encryption

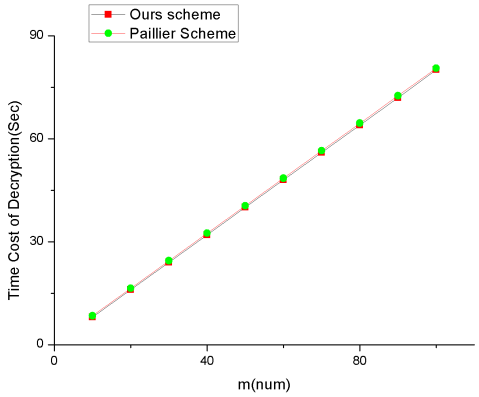


Figure 2: Time cost of decryption

Paillier's scheme, which is a bit heavy for the Intel Edison Platform. The cost of our scheme is also a little lighter than Paillier's scheme. In big data applications, most of decryption works are carried out by the cloud severs. From the experiment result, the proposed scheme may be a good choice for the resource-constrained end users in big data applications.

6 Conclusion

Additively homomorphic IBE scheme can be used to perform data aggregation on the data submitted by the end users, without sacrificing their privacy. In this work, we propose a leakage resilient additive homomorphic IBE scheme with auxiliary input, for solving the problem that the secret keys stored in end devices may leaked by side channel attacks. In the theory of auxiliary input model, no matter how many bits of secret keys can be acquired by the attacker, it still cannot recover the secret keys. We prove our scheme is AI-CPA secure under the strong extractor with auxiliary input. The implementation and perform analysis show that the efficiency of our scheme is suitable for the resource-constrained end users.

Acknowledgment

This research is partially supported by the National Natural Science Foundation of China under Grant No.61672016, the Jiangsu Qing Lan Project, the Six talent peaks project in Jiangsu Province under grant No.RJFW-010, and the Humanities and Social Science Research Planning Fund of the Education Ministry of China under grant No.15YJCZH201.

References

[1] A. Akavia, S. Goldwasser and V. Vaikuntanathan, "Simultaneous hardcore bits and cryptography against memory attacks," in *Theory of Cryptography Conference (TCC'09)*, vol. 5444, pp. 474-495, 2009.

[2] A. Anton, E. Bertino, N. Li, T. Yu, "A roadmap for comprehensive online privacy management," *Communications of ACM*, vol. 50, no. 7, pp. 109-116, July 2007.

[3] M. Bellare, A. O'Neill, I. Stepanovs, "Forward-security under continual leakage," in *International Conference on Cryptology and Network Security*, vol. 11261, pp. 3-26 2018.

[4] A. Berkoff, F. H. Liu, "Leakage resilient fully homomorphic encryption," in *Theory of Cryptography Conference*, vol. 8349, pp. 515-539, 2014.

[5] E. Bertino, "Big data - Opportunities and challenges panel position paper," in *IEEE 37th Annual Computer Software and Applications Conference*, 2013. DOI: 10.1109/COMPSAC.2013.143.

[6] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Annual International Cryptology Conference*, vol. 2139, pp. 213-229, 2001.

[7] J. W. Byun, A. Kamra, E. Bertino, N. Li, "Efficiently k-anonymization using clustering techniques," in *International Conference on Database Systems for Advanced Applications*, pp. 188-200, 2007.

[8] B. Carminati, E. Ferrari, M. Viviani, "Security and trust in online social networks," *Security and Trust in Online Social Networks*, 2014. ISBN:1627052658 9781627052658.

[9] Cloud Security Alliance, *Expand Top ten Big Data Security and Privacy Challenges*, 2013. (`https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf`)

[10] Y. Dodis, S. Goldwasser, Y. T. Kalai, C. Peikert, V. Vaikuntanathan, "Public key encryption schemes with auxiliary inputs," in *Theory of Cryptography Conference*, vol. 5978, pp. 361-381, 2010.

[11] K. Durnoga, S. Dziembowski, T. Kazana, M. Zajac, M. Zdanowicz, "Bounded-retrieval model with keys derived from private data," in *International Conference on Information Security and Cryptology*, vol. 10143, pp. 273-290, 2017.

[12] C. I. Fan, S. Y. Huang, Y. L. Lai, "Privacy-enhanced data aggregation scheme against internal attackers in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 666-675, 2014.

[13] C. Gentry, "Fully homomorphic encryption using ideal lattices," *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, pp. 169-178, 2009. ISBN: 978-1-60558-506-2.

[14] F. Gunther, M. Manulis, A. Peter, "Privacy-enhanced participatory sensing with collusion resistance and data aggregation," in *International Conference on Cryptology and Network Security*, vol. 8813, pp. 321-336, 2014.

[15] R. Huang, Z. Li, J. Zhao, "A verifiable fully homomorphic encryption scheme," in *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, vol. 11611, pp. 412-426, 2019.

[16] B. Kreuter, A. Shelat, B. Mood, K. Butler, "PCF: A portable circuit format for scalable two-party secure computation," in *Proceedings of the 22nd USENIX conference on Security*, 2013. (`https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/kreuter`)

[17] R. Lu, X. Liang, X. Li, X. Lin, X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621-1631, 2012.

[18] F. Luo, K. Wang, C. Lin, "Leveled hierarchical identity-based fully homomorphic encryption from learning with rounding," in *International Conference on Information Security Practice and Experience*, vol. 11125, pp. 101-105, 2018.

[19] B. Lynn, *The Pairing-based Cryptography (PBC) Library.*(`https://crypto.stanford.edu/pbc/thesis.html`)

[20] R. Nishimaki, T. Yamakawa, "Leakage-resilient identity-based encryption in bounded retrieval model with nearly optimal leakage-ratio," in *IACR International Workshop on Public Key Cryptography*, vol. 11442, pp. 466-495, 2019.

[21] T. Okamoto and S. Uchiyama, "A new public-key cryptosystem as secure as factoring," in *International Conference on the Theory and Applications of Cryptographic Techniques*, vol. 1403, pp. 308-318, 1998.

[22] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International Conference on the Theory and Applications of Cryptographic Techniques*, vol. 1592, pp. 223-238, 1999.

[23] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*, pp. 84-93, 2005.

[24] Z. Wang, "Blind batch encryption-based protocol for secure and privacy-preserving medical services in smart connected health," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9555-9562, 2019.

[25] Z. Wang, C. Cao, N. Yang, V. Chang, "ABE with improved auxiliary input for big data security," *Journal of Computer and System Sciences*, vol. 89, pp. 41-50, 2017.

[26] L. Wang, L. Ge, Y. Hu, Z. He, Z. Zhao, H. Wei, "Research on full homomorphic encryption algorithm for integer in cloud environment," *International Conference on Intelligent Computing*, vol. 11645, pp. 109-117, 2019.

[27] Z. Wang, F. Xiao, N. Ye, R. Wang, P. Yang, "A see-through-wall system for device-free human motion sensing based on battery-free RFID," *ACM Transactions on Embedded Computing Systems*, vol. 17, no. 1, pp. 1-21, 2017.

[28] Z. Wang, S. M. Yiu, "Attribute-based encryption relient to auxiliary input," in *International Conference on Provable Security*, vol. 9451, pp. 371-390, 2015.

[29] F. Xiao, Z. Wang, N. Ye, R. Wang, X. Y. Li, "One more tag enables fine-grained RFID localization and tracking," *IEEE/ACM Transactions on Networking*, pp. 1-14, 2017. DOI:10.1109/TNET.2017.2766526.

[30] X. Yi, R. Paulet, E. Bertino, "Homomorphic encryption and applications," *Springer Briefs in Computer Science*, 2014. ISBN:3319122282 9783319122281.

[31] X. Yi, F. Rao, E. Bertino, A. Bouguettaya, "Privacy-preserving association rule mining in cloud computing," in *The 10th ACM Symposium*, 2015. DOI: 10.1145/2714576.2714603.

[32] T. H. Yuen, S. S. M. Chow, Y. Zhang, S. M. Yiu, "Identity-based encryption resilient to continual auxiliary leakage," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, vol. 7237, pp. 117-134, 2012.

[33] T. H. Yuen, Y. Zhang, S. Yiu, J. K. Liu, "Identity-based encryption with post-challenge auxiliary inputs for secure cloud applications and sensor networks," in *European Symposium on Research in Computer Security*, vol. 8712, pp. 130-147, 2014.

[34] Y. Zhang, R. Liu, D. Lin, "Improved key generation algorithm for Gentry's fully homomorphic encryption scheme," in *International Conference on Information Security and Cryptology*, vol. 10779, pp. 93-111, 2017.

[35] H. Zhu, F. Xiao, L. Sun, R. Wang, P. Yang, "R-TTWD: Robust device-free through-the-wall detection of moving human with WiFi," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 5, pp. 1090-1103, 2017.

Biography

Zhiwei Wang biography. He is a professor in the school of somputer, Nanjing University of Posts and Telecommunications, Nanjing, China. He was a Research Associate at the University of Hong Kong from March 2014 to March 2015. He has published more than 80 journal articles and referred conference papers. His research interests include applied cryptography, security and privacy in mobile and wireless systems, clouding computing, and

fog/edge computing.

Congcong Zhu biography. She is a master student of Nanjing University of Posts and Telecommunications.

Nianhua Yang biography. is an associate professor of Shanghai University of International Business and Economics. His research interests include security and privacy in mobile and wireless systems, software security.

Zhanlin Wang biography. He is a student of Yangzhou Shuren Middle School.

An Access Control Scheme Based on Access Tree Structure Pruning for Cloud Computing

Ze Wang, Minghua Gao, Lu Chen, and Shimin Sun
(Corresponding author: Ze Wang)

School of Computer Science and Technology, Tianjin Polytechnic University
399 Binshui W Rd, Xiqing, Tianjin, China
(Email: wangze@tjpu.edu.cn)
(Received July 8, 2019; Revised and Accepted Dec. 6, 2019; First Online Apr. 19, 2020)

Abstract

In the era of rapid development of information, people are spreading and sharing information all the time. These resources bring us a lot of privacy challenges while bringing us convenience. Therefore, We propose an attribute based encryption access control scheme based on access tree structure pruning (ATSP-ABE). The scheme mainly prune the branch of the ID attribute of the right subtree user managed by the Data Owner (DO) and design the permission access attribute as the leaf node to replace the branch. For the left subtree of the access tree managed by the Attribute Authorization Center (AAC) the decision tree is generated by the data of the user feature attribute and the subtree with the best pruning performance is selected as the pruning result. Finally, pruning the reduced feature attributes in the decision tree in the access left subtree. The experimental results show that the ATSP-ABE scheme can improve the computational efficiency of attribute-based access control encryption, decryption and user attribute revocation in cloud computing. More than that makes the access tree structure more concise and strengthen the DO control attribute ability. Reducing Calculation overhead in the process of encryption and decryption of DO and AAC.

Keywords: Access Control; Attribute Based Encryption; Cloud Computing; Decision Tree

1 Introduction

In this new digital era filled with vast amounts of data or information, everyone enjoys the convenience of instant information sharing and dissemination. More and more user data is uploaded to third-party cloud servers for storage, management or exchange [8, 10]. In order to reduce the efficiency of user data transmission, an access control scheme is introduced in the face of privacy protection and access threats. Access control scheme [6, 11, 19] be used to protect personal data on public platforms from unauthorized access or disclosure. In addition, data encryption algorithms [27] are often used to prevent platform operators and other attackers who are curious during data communication from snooping. Therefore, an efficient access control scheme must be designed according to the requirements of the user to make the stored data value of the shared user available to the authorized user. Once the user's data is outsourced to the cloud, the user will loses Control ability of their data. Since access control schemes are becoming more and more important. In order to solve the data protection problem in cloud storage, attribute-based encryption(ABE) [13] is considered one of the most promising technologies, which is from identity-based passwords. Learning from the development of [23], the ABE scheme performs fine-grained access control on the data stored in the cloud server by setting attributes. The ABE scheme mainly consists of the following two types, such as Ciphertext-Policy Attribute-Based Encryption(CP-ABE) [7, 31, 32] and Key-Policy Attribute-Based Encryption(KP-ABE) [9, 18, 21]. Considering the frequent update of ciphertext and a large number of users of the mobile Internet, CP-ABE is more suitable for fine-grained data access control in cloud storage scenarios.

The access structure that CP-ABE can adopt is a linear access structure or a tree access structure. Waters *et al.* [26] implements a CP-ABE access control scheme based on linear access structure to support attribute revocation. Linear access structures are better able to solve completely independent properties, but less efficient for incompletely independent properties that appear in real-world situations. Xiong and Simoes and Touatil *et al.* [24, 25, 29] use the tree access structure to implement the CP-ABE access control scheme to support attribute revocation, which solves the problem of the user's incomplete independence attribute in the actual situation. Huang *et al.* [22] proposes a multi-authority revocable attribute-based encryption (MA-ABE) scheme, which the classifification manages user attributes, to relieve the management burden of single organization effectively. In addition, the tree access policy and the secret

sharing scheme are adopted to implement fine-grained access control of shared information and support system attribute revocation. In the attribute-based encryption-based access control scheme in the cloud computing environment [1, 15, 28], leaf nodes in the access tree represent user attributes, and non-leaf nodes represent access policies.

The AAC determines whether the user satisfies the access tree structure through user attributes, thereby being able to manage and control the users who want to access the data resources. However, all user attribute data is managed and controlled by a third party, so DO loses the authority to manage its shared data. Yang *et al.*proposed a scheme [16] to divide the user attribute into two parts, which are managed and controlled by AAC and DO respectively, DO also has the right to manage its attributes. However, as the number of users and attributes increases, the workload of AAC and DO increases, resulting in reduced efficiency. Therefore, based on the literature [16], this paper optimizes the structure of the access subtree managed by AAC and DO respectively, and improve the efficiency of user attribute management and control. By simplifying the access tree, the computational overhead of AAC and DO is reduced. Through the experimental results, it can be verified that the pruning of the left subtree is constructed, the decision tree [12, 20, 30] is constructed to process the user data, and the subtree with the maximum pruning performance can be significantly improved. Then, the ATSP-ABE scheme proposed in this paper can also implement the function of user attribute revocation [2, 3, 17]. Compared with the two ABE schemes using linear access structure [26] and tree access structure [16], the proposed scheme greatly improves the performance of private key generation, password text size, encryption and decryption, and user attribute revocation in cloud computing.

2 Our Contribution

1) An access control scheme based on access tree structure pruning in cloud computing environment is proposed. It performs different pruning on the access right subtree and access left subtree which is managed by DO and AAC respectively. Accessing the right subtree to prun the branch where the user ID attribute node is located, and design the permission access attribute to replace the branch with the leaf node. This scheme allows DO to retain the key attributes of its shared data, fully control its shared data and reduce the computational overhead of DO in the access policy.

2) Accessing the left subtree in the cloud computing environment first generates a decision tree based on the data of the user feature attribute, which selects the subtree with the best pruning performance as the pruning result. Finally, accessing the left subtree will reduce the feature attributes in the decision tree. After pruning, the access tree is simplified. The solution reduces the computational overhead of the AAC in the access policy and improves the management and control efficiency of the AAC.

3) An efficient cloud computing access control scheme based on CP-ABE structure is proposed. Users can decrypt ciphertext and attributes with a small amount of calculation. In our scheme, it can be achieved by pruning, which only a small amount of computational overhead is required. The effectiveness of the scheme is demonstrated by comparison with other schemes in terms of computational complexity and communication overhead.

2.1 System Model

In the architecture of ATSP-ABE scheme, there are four entities (see Figure 1): Data Owner (DO), Data User (DU), Platform Server (PS), and Attribute Authentication Center (AAC). The DO uploads the algorithm encrypted file to the PS, and the security of the file is guaranteed by the access control and decryption process. PS and AAC always stay online, assuming it has infinite storage and computing power to ensure that DU download and decrypt these files from PS. AAC is responsible for the distribution and revocation of attributes, then the attributes of the user are jointly controlled by AAC and DO. AAC is responsible for managing the user's feature attributes, which is a set of attributes describe the DU. We assume that DO not only stores data files, but also creates a set of attribute-defined access policies for its data files.

The complexity of the ATSP-ABE algorithm in the cloud environment is proportional to the complexity of the structure of its corresponding access tree. Therefore, the algorithm delivers a lot of mixed content instead of the core algorithm to the PS in the implementation process. Most of the attributes of the DU are managed and controlled by AAC. The DO still retains its key attributes and shared data calculations, maintains its original security, the security level and the locally calculated security level in the original CP-ABE scheme remain unchanged. During the encryption and decryption operations, the PS has access to most of the keys in the tree structure but not all keys. In the process of decrypting the calculation, the bilinear pair in the ciphertext and key generation spend a lot of calculations in the system, so we safely pass this part of the operation to the PS. The last step of the decryption operation is performed by the data user DU itself, and the data sharing resources will not leak to the PS.

3 Detailed Description

The traditional CP-ABE access control scheme mainly uses the access tree as the access policy. The complexity of the access tree determines the efficiency of DO and

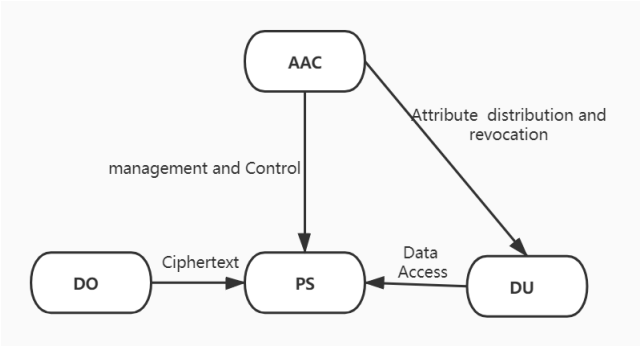


Figure 1: The proposed system model

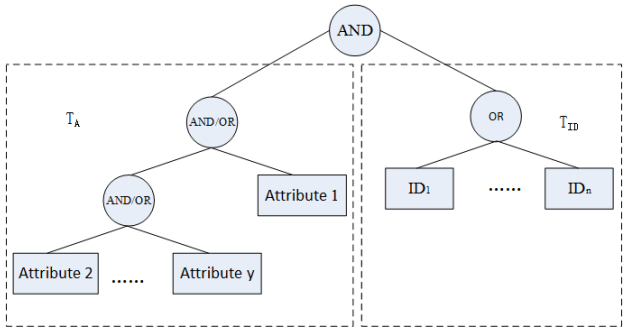


Figure 2: The access tree structure of the CP-ABE

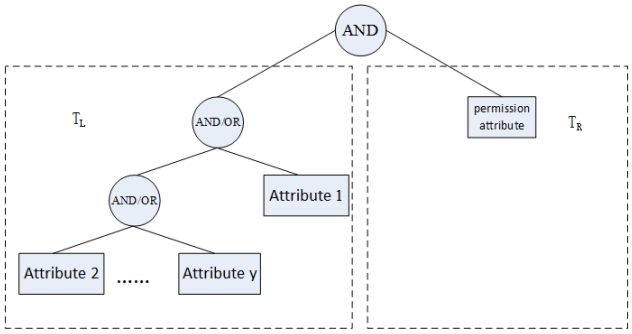


Figure 3: The access tree structure of the ASTP-ABE scheme

AAC access control for user attributes. Therefore, the access control scheme is designed for pruning the access tree structure in this paper, which simplifies the access tree and reduces the complexity. The access tree structure is divided into accessing the left subtree T_A and accessing the right subtree T_{ID}, which contain different attributes. The former contains the feature attributes of the DU, and the latter contains the ID attributes of the DU. Therefore, our proposed ATSP-ABE scheme prunes the two subtrees of these schemes separately.

3.1 The Pruning of the Access Right Subtree

The Figure 2 depicts the access tree structure of the CP-ABE scheme in literature [16], and $\{A_1, A_2, ..., A_y\}$ representing a user's feature attribute set. $\{ID_1, ID_2, ..., ID_n\}$ representing the user's ID attribute collection. The access tree T is a binary tree with access to the left subtree T_A and access to the right subtree T_{ID}. The feature attribute in the access left subtree is managed by AAC, and the user ID attribute in the access right subtree is controlled by DO. The root node of the access tree is an "AND" node, which indicates that the user attribute must satisfy both the access left subtree and the right subtreeto satisfy the access policy. Accessing the right subtree contains an "OR" node whose leaf nodes are related to the user ID attribute. In this access tree structure, although most user attributes are managed and controlled by AAC.

The ID attribute of many users managed by DO still affects the efficiency of user attributes and key control. Therefore, in order to make the data access more convenient and faster, this paper designs the structure of accessing the right subtree to reduce the computational cost of access control during encryption and decryption. Experiments show that the pruning result of accessing the right subtree is shown in Figure 3. The structure is simplified and the computational overhead is reduced, and attribute revocation can be implemented more efficiently. The branch accessing the right subtree in the CP-ABE scheme is an "OR" node and n ID attribute nodes. Each attribute node will be assigned a separate user, which will cause a burden on the key calculation. When the algorithm needs to determine the access tree structure, the "OR" node is used as the root node in the right subtree to prun the branch, including its n ID attribute nodes and is designed to access the license access attribute of the right subtree to replace the branch. The changed access to the right subtree allows the security of encryption and decryption to be guaranteed, since the last step of the decryption operation is performed by the data user DU itmself. Permission access properties are constantly updated to ensure the security of shared data. At the same time, the pruning of the access tree also reduces the computational cost of encryption and decryption. It enables users to access the data they need more effectively and to share data easily.

3.2 The Pruning of the Access Left Subtree

The AAC manages and controls many feature attributes of DU. Because of the overlapping feature attributes among DUs, AAC performs many tasks to repeatedly determine feature attributes which increases the workload of AAC. Therefore, we use the decision tree [14] to classify user data, we can divide user data into different categories. Depending on the category of the DU, users can be granted different permissions. In this way, AAC no longer needs to perform access control defined by one DU after another. Instead, it firstly determines the classification of DU data and then performs access control defined by the attributes of the data classification which effectively reduces the efficiency and computational overhead of AAC management and controls the attributes.

We have adopted the idea of reducing the error pruning method (REP) [4,20]. It uses a separate data set to make up for the ERP of the pruning process, which not only considers the accuracy of the classification but also considers the performance of both the classification balance and the complexity. In the case of ensuring the accuracy of the algorithm, the decision tree is simplified and the computational complexity of the access tree structure is reduced. In Table 1, we list the symbols used in ATSP-ABE:

1) Accuracy of classification. It mainly reflects the classification accuracy of decision trees, defined as:

$$m(T') = \frac{1}{Q'} \sum_{i \in Y} b(i)'.$$

We use it to calculate the classification accuracy of the decision tree, which is given by the ratio of the sum of the correct number of users per node to the sum of the number of users in the pruning set. If the classification accuracy of the decision tree is greater, the accuracy of the decision tree will higher.

2) The balance of classification. It mainly reflects the classification balance of the decision tree, defined as:

$$r(T') = \frac{1}{Q'} \sum_{i \in \omega} q(i)' r(i).$$

Where r(i) is the classification accuracy of the node and can be calculated as:

$$r(i) = \begin{cases} \frac{m(i)'}{m(i)} & m(i)' < m(i) \\ \frac{m(i)}{m(i)'} & m(i)' > m(i) \end{cases}$$

$m(i)$ and $m(i)'$ in the above formula are mainly calculated by the pruning set and the training set, and can be defined as:

$$m(i)' = \frac{b(i)'}{q(i)'}$$

$$m(i) = \frac{b(i)}{q(i)}$$

Therefore, the larger the classification balance value of the decision tree, the higher the classification stability of the entire decision tree.

3) Complexity. If the decision tree is too complex, the number of users arriving at certain nodes will be reduced, making the decision tree unable to process its user set. In order to ensure the accuracy of classification and the performance of classification, the complexity of the decision tree should be reduced as much as possible. The combination of leaf nodes and depths of the decision tree can be represented by t. Among $t = \omega + \upsilon$ its complexity can be defined as follows:

$$f(t) = \begin{cases} 0 & t < 4 \ or \ t > 35 \\ \frac{t+10}{20} & 4 \le t \le 10 \\ \frac{44-t}{40} & 20 \ge t > 10 \\ \frac{50-t}{30} & 35 \ge t > 20 \end{cases}$$

In summary, the classification between the number of leaf nodes and the depth of the tree in the decision tree is best. When the range of t is $t < 4 \ or \ t > 35$, it is a very unfavorable situation. This paper proposes to use the pruning performance to evaluate the performance of the decision tree, as can be defined as follows:

$$P(T') = x_1 m(T') + x_2 r(T') + x_3 f(T').$$

In the above formula x_1, x_2, x_3 represents the classification accuracy, classification balance, and complexity ratio of the decision tree, at the same time, satisfies $x_1 + x_2 + x_3 = 1$. In short, we allocate the ratio of the three performances evenly, and can also be based on different actualities. In the case of the proportion of each performance is assigned. During the pruning process, the pruning performance of each candidate subtree is compared, the pruning tree with the highest pruning performance is selected to ensure the optimal pruning performance of the decision tree.

3.3 The Detailed Trimming Process

1) From the bottom up, each subtree in the decision tree is a candidate subtree of the pruning, the subtree is replaced by the leaf node, and the node is identified by the category represented at most instances, reaching the leaf node in the training set. It generates a set of pruned subtrees $\{T'_0, T'_1, ..., T'_i\}$ representing the decision trees that T'_0 have not been pruned.

2) Based on the categorical data of the trained set and the data of the pruned set of the original decision tree, we calculated the pruning performance $P(T'_i)$ of each pruned subtree T'_i.

3) In the candidate subtree set $\{T'_0, T'_1, ..., T'_i\}$, the algorithm compares the pruning performance $P(T'_i)$ of each candidate subtree and selects the tree with the highest pruning performance as the final decision tree.

4) The pruning of the decision tree subtree corresponds to the pruning of the feature attributes, and the reduction of each subtree corresponds to the reduction of the determined feature attributes. Finally, the algorithm prunes the reduced characteristic attributes of the decision tree on the access tree structure.

5) By separately pruning the left and right subtrees of the access tree, the access tree structure is simplified, the computational overhead of DO and AAC

Table 1: Notations for ATSP-ABE

$m(T')$	the taxonomy veracity of the decision tree T'.
$r(T')$	the taxonomy balance of the decision tree T'.
$f(T')$	the complexity of the decision tree T'.
$r(i)$	the taxonomy balance of the node i.
$m(i)'$	the taxonomy veracity of the node i in the pruned set.
$m(i)$	the taxonomy veracity of the node i in the trained set.
Q'	the users number in the pruned set.
Q	the users number in the trained set.
$q(i)'$	the users number of the node i in the pruned set.
$q(i)$	the users number of the node i in the trained set.
$b(i)'$	the users number belongs to the node i in the pruned set.
$b(i)$	the users number belongs to the node i in the trained set.
ω	the number of the leaf node in the decision tree.
υ	the depth of the decision tree T'.
i	the i-th node of the decision tree.

management and control attributes is realized. Improve the efficiency of its property management and control.

4 The ATSP-ABE Algorithm

The mathematical basis of the ATSP-ABE algorithm is bilinear mapping. Let q be a large prime number, G_1 and G_2 be two multiplicative cyclic groups of order q, p is the generator of G_1, and $e : G_1 * G_1 \to G_2$ is a bilinear map. It has the following properties:

- The Bilinear. For any $P, Q, R \in G_1$ and $a, b \in Z_q$, there are:

$$\begin{aligned} e(P \cdot Q, R) &= e(P, R)e(Q, R) \\ e(P^a, Q^b) &= e(abP, Q) = e(P, abQ) = e(P, Q)^{ab} \end{aligned}$$

- The Non Degeneracy. There is $P, Q \in G_1$ that makes $e(P, Q) \neq 1$, among them, 1 is the generator of the multiplicative cycle group G_2.

- The Computability. For all $P, Q \in G_1$, there is a valid algorithm for the calculation of $e(P, Q)$.

The ATSP-ABE algorithm consists of four parts. They are system settings, encryption algorithms, user private key generation and decryption algorithms, described as follows:

System setting. The algorithm selects a bilinear multiplicative cyclic group G_1 with a prime order q and a generator p. Let $e : G_1 * G_1 \to G_2$ represents a bilinear map. The AAC selects two random parameters $a_1, b_1 \in Z_q$, and generates the first master key as:

$$MK_1 = \{b_1, p^{a_1}\}.$$

The first public key is as:

$$PK_1 = \{G_1, p, \eta_1 = p^{b_1}, e(p, p)^{a_1}\}.$$

The DO selects two random parameters $a_2, b_2 \in Z_q$, and generates the second master key as:

$$MK_2 = \{b_2, p^{a_2}\}.$$

The second public key is as:

$$PK_2 = \{G_1, p, \eta_2 = p^{b_2}, e(p, p)^{a_2}\}.$$

The system setting also selects a random parameter $\varepsilon_0 \in Z_q$ for later use.

Encryption algorithm. In the case of access tree structure, ATSP-ABE algorithm encrypts information M. Select two random parameters $\mu_1, \mu_2 \in Z_q$ and select two polynomials $g_L(x), g_R(x)$ to represent access the left subtree and the right subtree respectively. Suppose that the leaf node set of accessing the left subtree is W, which A_λ is the permission access attribute node for accessing the right subtree. The $att(w)$ is a function of the attribute that w is a leaf node and is associated with a leaf node X in the access tree. The algorithm uses a hash function $H : \{0, 1\}^* \to G_1$, and describes any attribute on a bilinear map as a binary string of random elements. The access tree generates the ciphertext as:

$$\begin{aligned} CT = \{&T_L, \tilde{C} = Me(p, p)^{a_1,\mu_1} e(p, p)^{a_2,\mu_2}, \\ &C_1 = \eta_1^{\mu_1}, C_2 = \eta_2^{\mu_2}, \\ &\forall w \in W : C_w = p^{g_{w(0)}}, C'_w = H(att(w))^{g_{w(0)}}, \\ &\forall \lambda \in A_\lambda : C_\lambda = p^{\mu_2}, C'_\lambda = H(att(w))^{\mu_2}\}. \end{aligned}$$

User private key generation. Including the private key of the feature attribute and the private key of the license attribute, respectively calculated as follows: The AAC algorithm inputs the attribute set A_u of the user u, and generate a key for the attribute set. The algorithm selects a random number $\varepsilon \in Z_q$ and $\varepsilon_j \in Z_q$ and selects the random number $j \in A_u$ for

the feature attribute. The feature attribute private key is as follows:

$$SK_1 = \{D_1 = P^{(a_1+\varepsilon)/b_1}, \\ \forall j \in A_u : D_j = p^{\varepsilon} \times H(j)^{\varepsilon_j}, D'_j = p^{\varepsilon_j}\}.$$

The data owner DO's algorithm enters the user's permission access attribute and outputs the private key of the license access attribute. The algorithm selects a random number $\varepsilon_0 \in Z_q$ and $\varepsilon_\lambda \in Z_q$ for the user. The private key of the license access attribute is as follows:

$$SK_2 = \{D_2 = P^{(a_2+\varepsilon_0)/b_2}, \\ D_\lambda = p_0^{\varepsilon} \times H(att(\lambda))^{\varepsilon_\lambda}, D'_\lambda = p^{\varepsilon_\lambda}\}.$$

It then executes the above two-part algorithm, and generates the user private key as:

$$SK = (SK_1, SK_2).$$

Decryption algorithm. Including decryption access to the left subtree and the right subtree. The first part is the decryption process of accessing the left subtree, which is the same as the CP-ABE algorithm and represtents by A_1.

$$A_1 = DecryptNode(CT, SK_1, w) \\ = e(p,p)^{\varepsilon\mu_1}.$$

$$M_1 = Decrypt(CT, SK_1) \\ = \tilde{C}/(e(C_1, D_1)/A_1) \\ = \tilde{C}/e(p,p)^{a_1,\mu_1} \\ = Me(p,p)^{a_2,\mu_2}.$$

The second part is the decryption process of accessing the right subtree and represtents by A_2. Finally we can get the ciphertext shown as below:

$$A_2 = DecryptNode(CT, SK_2, \lambda) \\ = \frac{e(D_\lambda, C_\lambda)}{e(D'_\lambda, C'_\lambda)} \\ = \frac{e(p^{\varepsilon_0} \times H(att(\lambda))^{\varepsilon_\lambda}, p^{\mu_2})}{e(p^{\varepsilon_\lambda}, H(att(\lambda))^{\mu_2})} \\ = e(p,p)^{\varepsilon_0,\mu_2}.$$

$$M_2 = M_1/(e(C_1, D_2)/A_2) \\ = M_1/e(p,p)^{a_1,\mu_2} \\ = M.$$

5 Security Proof

The security analysis is mainly composed of the following four aspects: full control of shared data, prevention of user key leakage, untrusted third party organizations, and data confidentiality analysis.

Full control of shared data: With the help of the license access properties, the data owner DO can fully manage their data resources. The branch in the right subtree in the CP-ABE scheme is the OR node and its n ID attribute nodes, which are assigned to each user and easily burden the key calculation. When the algorithm needs to determine the access tree structure, branches with the "OR" node as the root node in the right subtree, including its n ID attribute nodes, are pruned, and the branch is designed for the right subtree design permission access attribute. This can not only meet the data owner DO control shared data requirements, but also reduce the computational overhead and improve the efficiency of the ATSP-ABE access control scheme.

Preventing user key abuse: This problem is solved by means of user private key separation, and the data owner DO can immediately suspend any user sharing data. The data owner DO still controls the final step of decrypting the ciphertext. The license access attribute is continuously updated to ensure the security of shared data. At the same time, access tree pruning also reduces the computational overhead of encryption and decryption, enabling users to access required data more efficiently and quickly, and easy to implement data sharing.

untrusted third party organizations: The data owner DO can entrust a semi-trusted organization to complete the revocation task. The data owner DO personal information is based on the proxy re-encryption method and is transparent to the organization's transmission. The user attribute undo operation may revoke one or more attributes owned by the user without affecting the current attributes of other users. The revocation will cause a large number of key update operations, and the user and ciphertext encrypted with the expired public key need to be updated. This paper uses the platform server PS or other service system to solve the problem. When the user attribute revocation occurs, the attribute authorization center AAC passes the information to the platform server PS to directly revoke the user attribute. When the user wants to access the encrypted data, the platform server PS firstly checks the attributes of the user. If the platform server PS determines that the user's attribute does not satisfy the access policy, the user will not be assigned an encrypted data key.

Data confidentiality: The data confidentiality is analyzed by the following scheme, which proves that the scheme satisfies the indiscernibility of the message under the assumption of DBDH. The mathematical basis of the security analysis is the Decision Bilinear key exchange algorithm DBDH [5](Decisional Bilinear Diffie-Hellman) hypothesis. It is assumed that $\alpha, \beta, \gamma, z \in Z_q$ is uniformly selected and G_1 is a group

whose prime order q and the generator element is p. The DBDH assumption means that an attacker cannot distinguish tuples $(p^\alpha, p^\beta, p^\gamma, e(p,p)^{\alpha\beta\gamma})$ and $(p^\alpha, p^\beta, p^\gamma, e(p,p)^z)$ in a polynomial time with a non-negligible advantage.

Theorem 1. *Under the security model of DBDH hypothesis, if an attacker can destroy the model of the algorithm with a non-negligible advantage, and then we can construct a simulator to solve the DBDH problem.*

Proof. Suppose that attacker I can attack the algorithm's model in a polynomial time with a non-negligible advantage ε. We set up a simulator E, which can perform the DBDH match with the advantage $\varepsilon/2$. The simulator E is set to:G_1, G_2 is a valid bilinear map e with generator p and DBDH instance $(p^\alpha, p^\beta, p^\gamma, e(p,p)^z)$, where $Z = \alpha\beta\gamma$ or random. The simulator operates as follows: □

1) Initialization: Attacker I selects a challenged access structure T^* and sends it to Simulator E.

2) Setting: Simulator E sets the parameter $Y = e(A,B) = e(p,p)^{\alpha\beta}$ to select the random parameter $\delta \in Z_q$ and sets the parameter $\eta = p^\delta, \varphi = p^{1/\delta}$. Send public parameters to attacker I.

3) Search 1: The private key that the attacker I requested from the simulator E to set the attribute.

$$w_i = \{\alpha_i | \alpha_i \in \Omega \cap \alpha_i \notin T^* \cup U_\lambda\}.$$

Simulator E selects a random function F_{s_k} for the attribute authorization center AAC, It sets the parameters $y_{k,u} = F_{s_k}(\lambda)$, Where λ is the user permission access attribute. Selecting parameter $r, s_k \in Z_q$, setting parameter $D = p^{(y_k + y_{k,u} + r)/\delta}$. If attribute $\alpha_i \in w_i$, it sets parameters $D_{\alpha_i} = p^r H(\alpha_i)^{r_{\alpha_i}}, D'_{\alpha_i} = p^{r_{\alpha_i}}$, and sends the private key to attacker I.

4) Challenge: Attacker I submits a challenge attribute and two challenge messages M_0, M_1 to Simulator E. We assume that attacker I never asks for the private key in the Search 1 setting. The simulator E randomly selects $\beta \in \{0,1\}$, and encrypts the information as:

$$M_\beta : CT = (T^*, \tilde{C} = M_\beta Z, C = \eta^\alpha, \forall i \in T^* : C_i = p^{\alpha_i}, C'_i = H(i)^{\alpha_i}).$$

According to the encryption algorithm in the ATSP scheme, we set the root node τ for the challenge access tree T^*. The simulator E sends ciphertext to the attacker I. If $Z = e(p,p)^{\alpha\beta\gamma}$, we implicitly set $\tau = c$, that is $Y^\tau = Z = e(p,p)^{\alpha\beta\gamma}$ and $C = \eta^c, C_i = p^{c_i}$. It shows that the ciphertext is a valid random encryption of the information M. Otherwise, if $Z = e(p,p)^z$ for a random z, $\tilde{C} = M_\beta e(p,p)^z$. From the perspective of the attacker I, CT is a random element of G_2, and the ciphertext does not contain information M_β.

5) Search 2. It performs the same operation as Search 1.

6) Conjecture. The attacker I submits β' of the guess β. If $\beta = \beta'$, the simulator E will output 0, indicating $Z = e(p,p)^{\alpha\beta\gamma}$, otherwise the simulator will output 1 to indicate that the attacker I has not obtained any information of the encrypted M_β.

- If $\beta' \neq \beta$, then there is

$$P_r[\beta' \neq \beta | Z = (p,p)^z] = 1/2.$$

- If $\beta' = \beta$, we define the advantage of the attacker I as ε, and there is

$$P_r[\beta' = \beta | Z = (p,p)^{\alpha\beta\gamma}] = 1/2.$$

- Therefore, the advantage of the simulator E in the DBDH match is

$$\begin{aligned} Adv &= P_r[\beta' = \beta] - 1/2 \\ &= 1/2 \cdot (P_r[\beta' = \beta | Z = (p,p)^{\alpha\beta\gamma}] \\ &+ P_r[\beta' = \beta | Z = (p,p)^z]) - 1/2 \\ &= \varepsilon/2. \end{aligned}$$

Only when the attribute settings satisfy the access policy, the user can decrypt and get the encrypted information of the scheme. The ATSP-ABE model is proved to be safe by DBDH hypothesis theory.

6 Results and Discussion

6.1 Analysis of the Pruning Results of the Access Tree

The ATSP-ABE scheme by using the pairing-based cryptography PBC (Pairing-Based Cryptography) library version 0.4.18. The experiment in this paper was carried out by using a PC with a dual-core 3.1GHz, Intel Core i7-6500U CPU, 16GB RAM, and 64-bit Win10 operating system. The experimental data set of this paper is the blood transfusion service center data set in the UCI machine learning database. The data set is moderately sized, and the access tree is not overly complex, facilitating pruning and is suitable for simple and intuitive descriptions. The blood service center has 748 user data, including 5 attributes. The category attribute is category, and the remaining attributes are represented by A_1, A_2, A_3, A_4 respectively. Their meanings are as follows:Category indicates whether blood was donated in March 2007. A_1 indicates the number of months since the last donation. A_2 indicates the total amount of donations. A_3 indicates the total number of months of blood donation. A_4 indicates the total amount of blood donation (c.c.).
In this paper, the independent pruning dataset is used to randomly extract the user data, and 60.70% of the

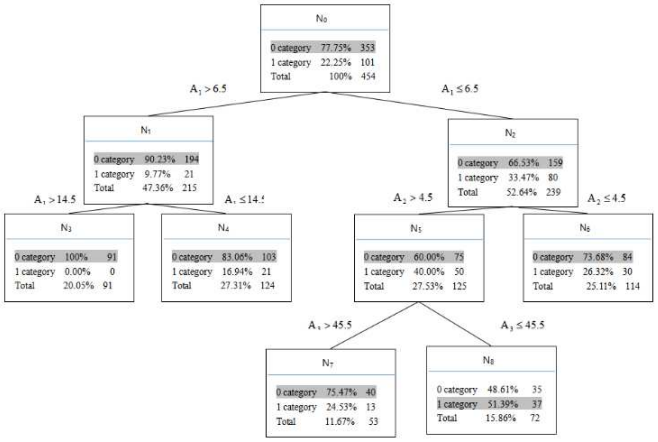


Figure 4: Training data set classification

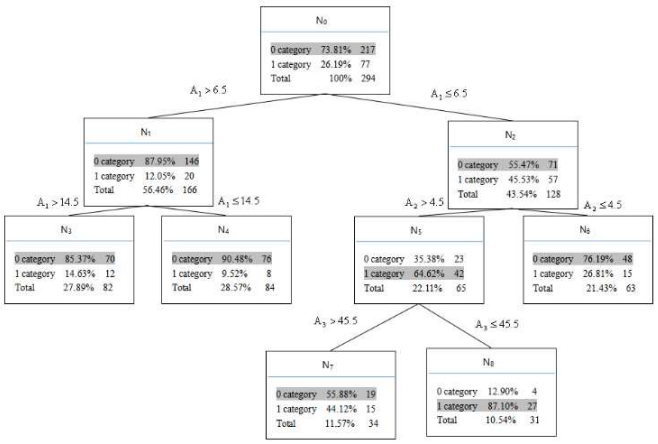


Figure 5: Pruning data set classification

users are selected as the training dataset, and the remaining 39.30% of the users are used as the pruning dataset. The decision tree generated by the user's feature attribute data is shown in Figure 4 and Figure 5. Figure 4 shows the classification of the training set, and Figure 5 shows the classification of the pruning set. Since the decision tree selected in this paper is not complicated, the sum of the leaf nodes and the depth of the tree is less than 10, which can reduce the proportion of the complexity of the decision tree when calculating the pruning performance. This paper adjusts the weight distribution to 45% 45% and 10%. The pruning performance is calculated as follows:

$$P(T') = 0.45m(T') + 0.45r(T') + 0.1f(T').$$

The nodes in the decision tree are represented as $N_t(t = 0, 1, 2, ..., n)$. The pruning performance of the subtree formed after removing the node N_i from the decision tree is expressed as $P(T'_{N_i})$. The classification accuracy of the nodes i on the pruning set and the training set can be obtained and as shown in Table I, and Table II shows the leaf nodes, classification accuracy $m(T')$, classification balance $r(T')$, tree complexity $f(T')$ and corresponding pruning performance $P(T')$ of candidate subtrees.

The algorithm uses these seven subtrees as candidate pruning subtrees and compares their pruning performance in bottom-up order. The candidate subtree has the best pruning performance, and the subtree is used as the final decision tree. The algorithm first prunes the branch from the original decision tree with node N5 and replaces it with a leaf node.The pruning branch N1 of the node is then replaced with a leaf node. The decision tree obtained using the REP pruning method is shown in Figure 6. The pruning performance method used in the paper obtains the decision tree after pruning, as shown in Figure 7. Compared to Figures 6 and 7, the decision tree generated by the pruning performance method used herein reduces the two leaf nodes compared to the REP pruning method. Reduce the size and complexity of the tree, making the structure of the access tree more concise and understandable.As shown in Table 4, the pruning performance method was 11.21% higher than the REP pruning method in the classification accuracy rate of category 1. While improving the classification accuracy, the goal of the access tree structure is more concise and the computational complexity is reduced.

The access left subtree T_A is composed of user feature attributes and is managed and controlled by the attribute authorization center AAC. The access right subtree T_ID consists of the attributes of the user data, and the last step of decryption is controlled by the data owner. In order to select the donors in March 2007 from the user data set and grant them special permissions, the access tree structure constructed using the CP-ABE algorithm is shown in Figure 8. The access tree structure expression is as follows: $("A_1 \leq 6.5" AND "A_2 > 4.5" AND "A_3 \leq 45.5" AND "A_4")AND("ID_1" OR "ID_2" OR ... "ID_{748}")$. Firstly, it is necessary to determine whether the feature attribute of the user satisfies the access to the left subtree. If the feature attribute of the user satisfies $("A_1 \leq 6.5" AND "A_2 > 4.5" AND "A_3 \leq 45.5" AND "A_4")$ the four attributes at the same time, the user feature attribute satisfies the left subtree. It is necessary to determine whether the user ID attribute is satisfied $("ID_1" OR "ID_2" OR ... "ID_{748}")$. If the user ID attribute satisfies any one of them, the user's ID attribute satisfies the right subtree. When the user's attributes satisfy the left and right subtrees successively, the user can be granted special permissions. If the user attribute attribute is not satisfied, it is not necessary to judge the ID attribute, determine that the user does not satisfy the access structure, cannot access the data resource, and does not assign special rights to the user. If the user already has the special right, the user is revoked special permission. If the user feature attribute is satisfied T_A but not satisfied T_ID, the user still cannot access the data resource and cannot assign the user special permission. Because the DO controls the final step of decryption, the data owner DO can control their data resources.

The access tree constructed using the ATSP-ABE algorithm is shown in Figure 9. In the access structure of the CP-ABE algorithm, T_A is improved to T_L, and T_ID

Table 2: The taxonomy veracity of the node i on the pruned and trained set

Node	N_0	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8
$m(i)$	73.81%	87.95%	55.47%	85.37%	90.48%	64.62%	76.19%	55.88%	87.10%
$m(i)'$	77.75%	90.23%	66.53%	100.00%	83.06%	60.00%	73.68%	75.47%	51.39%

Table 3: The Performance of the candidate subtree

Candidate Subtree	Leaf Node	$m(T')$	$r(T')$	$f(T')$	$P(T')$
T'_m	$N_3N_4N_6N_7N_8$	81.61%	85.51%	100.00%	85.20%
T'_{N_5}	$N_3N_4N_5N_6$	80.25%	91.26%	90.00%	86.18%
T'_{N_1}	$N_1N_6N_7N_8$	65.29%	90.52%	90.00%	79.11%
$T'_{N_5N_1}$	$N_1N_5N_6$	80.28%	96.31%	80.00%	87.47%
$T'_{N_5N_2}$	$N_2N_3N_4$	73.80%	86.31%	80.00%	80.05%
$T'_{N_5N_2N_1}$	N_1N_2	73.80%	91.32%	70.00%	81.30%
$T'_{N_5N_2N_1N_0}$	N_0	73.81%	94.93%	0.00%	75.93%

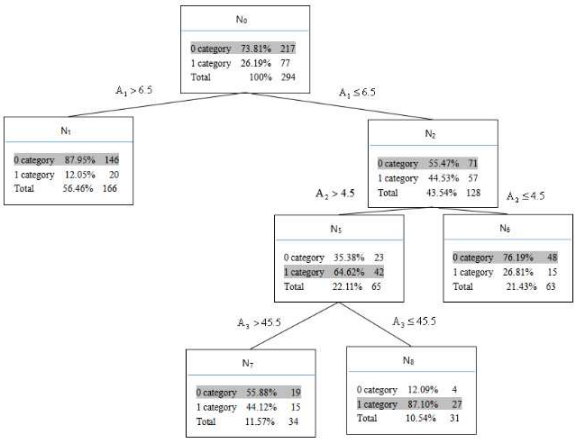


Figure 6: The REP pruned method

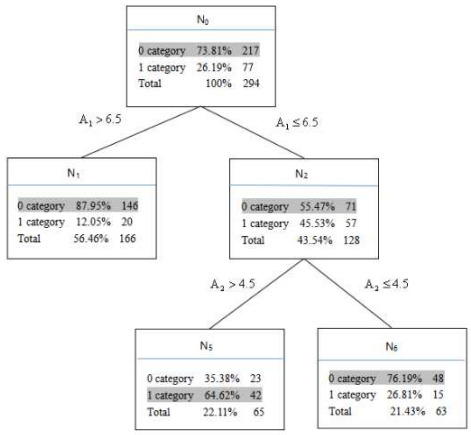


Figure 7: The pruned performance method

is improved to T_R. In the left subtree of the CP-ABE access structure. The decision tree is used to classify users, which improves the complexity of managing user attributes one by one. The pruning performance is proposed, and some feature attributes in the access tree are pruned to make the access tree The structure is more concise. Finally, the access tree structure prunes the two feature attributes $A_3 \leq 45.5$ and reducing the number of leaf nodes accessing the left subtree. Accessing the right subtree prune all of the user's 748 ID attribute nodes, replacing them with the permission access attribute node. The data owner controls the final step of decrypting the data, therefore, the access tree structure is made more concisely without affecting the performance of the algorithm, and reduced the computational complexity of the algorithm.

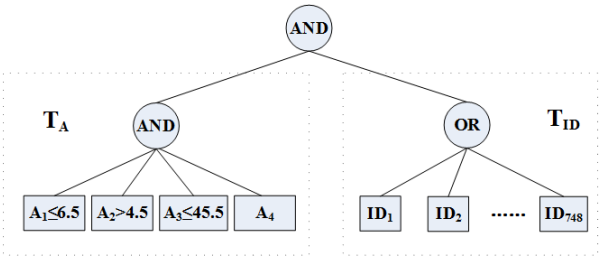


Figure 8: Transfusion user data set of CP-ABE access tree structure

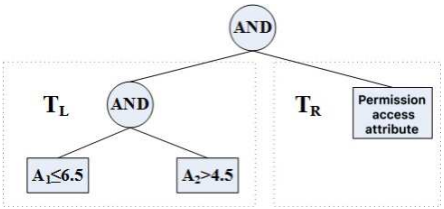


Figure 9: Transfusion user data set of ATSP-ABE access tree structure

Table 4: Classification accuracy of decision trees after pruning

		Correct quantity	Number of errors	Accuracy(%)
Pruning	Category 0	265	23	91.76
performance	Category 1	42	92	31.35
method	total	307	115	72.75
REP	Category 0	284	4	98.60
Pruning	Category 1	27	107	20.14
Method	total	311	111	73.69

6.2 Performance and Experimental Analysis

The performance of the ATSP-ABE scheme and the two typical ABE attribute schemes are compared in terms of system settings, private key generation, ciphertext size, attribute revocation, encryption and decryption, as shown in Table 5. Where n represents the number of system attributes, $L*$ represents the bit length of the element in $*$, A_u represents the number of attributes associated with the user, A_c represents the number of attributes associated with the ciphertext, A_{ID} represents the number of attributes associated with the user ID, and N_u represents the number of attributes. The number m is the size of the decryption key. The next step is to analyze the setup phase, user private key generation phase, ciphertext size, encryption and decryption algorithms phase.

Setup phase. DO defines the underlying bilinear map and generates the master key MK and the public key PK. The computational overhead of the ATSP-ABE system setup is less than the n-order multiplication of the bilinear group G_1, generating a master key MK requires a power operation. Generating a public key PK requires a power operation and a bilinear pair operation. The attribute authorization center AAC and the data owner DO each need to generate a pair of master key and public key, so the system setting phase requires a total of two power operations and two bilinear pair operations, wherein the bilinear pair is undoubtedly consuming the most time. The calculation overhead of the system setting of the ATSP-ABE scheme is the same as that proposed by Yang *et al.* [16].

Private key generation phase. The private key generation includes two parts: the feature attribute private key generation and the permission access attribute private key generation. The computational cost of this operation is the $2(A_u + 1)$-order multiplication of bilinear groups G_1. Generating a private key requires four power operations, one hash operation and one multiplication operation. The private key SK needs to be generated separately for the feature attribute and the permission access attribute, so the private key generation requires a total of eight power operations, two hash operations and two Submultiplication operation. The impact of the access tree structure of the ATSP-ABE scheme on the private key generation is to access the leaf node pruning part in the left subtree and the part that accesses the user permission attribute in the right subtree to generate the private key. Through the ATSP-ABE pruning method, the access to the left subtree prunes off some of the feature attribute nodes, so the attribute attribute managed by the attribute authorization center AAC is reduced so that the user private key generated by the attribute authorization center AAC is reduced. Accessing in the right subtree D_{id} becomes D_λ, and D'_{id} becomes D'_λ, so the calculation overhead of the user license attribute generating private key portion is reduced, thereby reducing the calculation overhead of the overall private key generation.

Ciphertext size. The ciphertext consists of a access tree, a header file, and a message body. The header file for each data consists of a collection of attributes consisting of $2(A_u+1)$ elements of G_1. Generating ciphertext requires two multiplication operations, two bilinear pair operations, two hash operations, and eight power operations. Due to the pruning process of the access tree structure, C_{id} in the information body becomes C_λ, and C'_{id} becomes C'_λ which reduces the computational overhead of the process of generating the information subject in the ciphertext, and is simplified after accessing the pruning process of the left subtree structure.Reducing the computational overhead of the entire ciphertext generation process.The summary analysis can be concluded that the computational overhead of generating the ciphertext size of the ATSP-ABE scheme is reduced by $(nA_c-2A_u-1)L_{G_1}+L_{G_2}$ compared to the computational overhead of Yang *et al.* [16], and the computational overhead is reduced by compared to Water *et al.* [26].

User attribute revocation phase. User attribute revocation includes re-generation and private key of all users, as well as ciphertext update operations. Among them, the user attribute revocation requires a thirteenth power operation, three bilinear pair op-

Table 5: Analysis and comparison of ATSP-ABE and two attribute encryption ABE schemes

Mechanism	Waters *et al.* [26]	Yang *et al.* [16]	ATSP-ABE
Structure	Linearity	Tree	Pruned tree
Complexity hypothesis	Group model	DBDH	DBDH
Revocation category	System attribute revocation, User revocation, User attribute revocation		
System settings	$3L_{G_1} + L_{G_2}$	nL_{G_1}	nL_{G_1}
Private key generation	$(1 + n + A_u)L_{G_1}$	$2(A_u + A_{ID})L_{G_1}$	$2(A_u + 1)L_{G_1}$
Ciphertext size	$(1 + nA_c)L_{G_1} + L_{G_2}$	$2(A_u + A_{ID})L_{G_1}$	$2(A_u + 1)L_{G_1}$
Attribute revocation	$(1 + 3nA_c)L_{G_1} + 2L_{G_2}$	$2N_u(A_u + A_{ID})L_{G_1} + nL_{G_2}$	$2N_u(A_u + 1)L_{G_1} + nL_{G_2}$
Encryption	$(1 + 3nA_c)L_{G_1} + 2L_{G_2}$	$(n + m + 1)L_{G_1} + 2L_{G_2}$	$(n + 1)L_{G_1} + 2L_{G_2}$
Decryption	$(1 + n + A_c)L_e + (3A_c - 1)L_{G_1} + 3L_{G_2}$	$2L_e + (m + 1)L_{G_1} + 2L_{G_2}$	$2L_e + 2L_{G_2}$
Advantage	The proxy re-encryption technology.	The fine-grained access control.	The DO can fully control the shared data, achieve the fine-grained access control, and owns high DO management attributes.
Disadvantage	No proof of the security under standard complexity assumptions, the third party and the AAC need to remain online.	The third party and the AAC need to remain online, the DO management attributes are not efficient.	The third party and the AAC need to remain online.

erations, three hash operations and three multiplication operations. Due to the ATSP-ABE pruning process on the access tree structure, the computational overhead of the system setup phase, the private key generation phase and the ciphertext size phase is reduced, so the computational overhead in the user property revocation process is also inevitable. The analysis shows that the computational overhead of the user attribute revocation of the ATSP-ABE scheme is reduced by $2N_uA_{ID}L_{G_1}$ compared to the computational overhead of Water *et al.* [26].

Encryption and decryption phase. When the information M needs to be encrypted under the condition of accessing the tree, the ciphertext CT is decrypted. The decryption operation includes two operations of accessing the left subtree and accessing the right subtree.The decryption algorithm for accessing the left subtree requires five bilinear pair operations, three multiplication operations, and two power operations. The decryption algorithm for accessing the right subtree requires two bilinear pair operations, five power operations, one multiplication operation, and two hash operations. Therefore, the total decryption algorithm requires a total of seven bilinear pair operations, four multiplication operations, seven power operations, and two hash operations. The ATSP-ABE scheme changes the access tree structure by pruning the access tree, reduces the complexity of the tree access structure, and reduces the computational overhead of accessing the right subtree encryption and decryption process. The ID-based key creation time is approximately 14-18ms. Accessing the right subtree during the encryption and decryption process eliminates the creation time of the user ID attribute, thereby reducing the computational overhead of encryption and decryption. Performing the comprehensive coefficient pruning method for accessing the left subtree reduces the subtree leaf node set W, reduces the size of the ciphertext generated during the encryption process, and reduces the computational overhead when decrypting the ciphertext.The computational overhead of the encryption operation of the ATSP-ABE scheme is reduced by $n(3A_c - 1)L_{G_1}$ compared to the scheme proposed by Waters *et al.* [16], and the scheme proposed by Yang *et al.* [26] is reduced by mL_{G_1}. Similarly, the computational overhead of the decryption operation of the ATSP-ABE scheme is reduced by $(n + A_c - 1)L_e + (3A_c - m - 2)L_{G_1} + L_{G_2}$ compared to the scheme proposed by Waters *et al.* [16] which reduces the compared to the scheme proposed by Yang *et al.* [26], compared to the two classic ABE schemes, ATSP-ABE scheme takes less time to execute, reducing the computational overhead of $2A_{ID}L_{G_1}$ size in

total, which is quite feasible for practical implementation.

This paper compares the three access structures of linear tree and pruning trees. Compare the ATSP-ABE algorithm with two typical ABE algorithms at the same security level and the same environment, and give quantitative conclusions. As shown in the experimental results in Table 6, when $n = 3$, our decryption algorithm execution time is one-fifth of Waters *et al.* [16], which is one-half of the text Yang *et al.* [26].The complexity of the access tree structure largely affects the computational overhead in the ABE algorithm. The encryption and decryption time of the algorithm depends to a large extent on the specific access structure and the set of attributes involved.

7 Conclusion

This paper proposes an access control scheme ASTP-ABE for cloud computing, which is based on CP-ABE to reduce access control policy access tree structure. Access the right subtree to prun the branch of the user ID attribute and design the permission access attribute to replace this branch with a leaf node. Accessing the left subtree generates a decision tree through the data of the user feature attribute. The algorithm selects the optimal pruning subtree as the result of pruning, and finally prunes the feature attributes in the left subtree, which are simplified in the decision tree. Simplify the pruned access tree structure and improve the efficiency of DO and AAC management and control attributes in the access policy.
In the environment of cloud computing, our solution can achieve complete control of shared data, with the help of permission access properties, DO can fully manage their data resources. Secondly, DO still controls the last step of decrypting ciphertext. In the cloud computing scenario, it can ensure that user key abuse is prevented.To solve this problem, DO can immediately terminate any user sharing data by means of user private key separation. Nextly, untrusted third-party DO can entrust semi-trusted organization to complete revocation task. DO's personal information is based on proxy re-encrypted method, which is transparent to the transferred organization. Finally, under the assumption of DBDH, our scheme satisfifies the indistinguishability of messages and ensures the confifidentiality of data in cloud computing environment.

Acknowledgments

This work was supported in part by the Key Project Foundation of Tianjin under Grant 15ZXHLGX003901, Tianjin Natural Science Foundation under Grant 19JCYBJC15800 and National Natural Science Foundation of China under Grant 61702366.

References

[1] Y. Baseri, A. S. Hafid, and S. Cherkaoui, "Privacy preserving fine-grained location-based access control for mobile cloud," *Computer and Security Journal*, vol. 73, pp. 249-265, 2018.

[2] Y. L. Chen and L. Y. Zhang, "CP-ABE based searchable encryption with attribute revocation," *Journal of Chongqing University of Posts and Telecommunication (Natural Science Edition)*, vol. 28, no. 4, pp. 545–554, 2016.

[3] X. F. Chen, Y. H. Zhang and J. Li, "Attribute-based data sharing with flexible and direct revocation in cloud computing," *KSII Transactions on Internet and Information Systems*, vol. 8, no. 11, pp. 4028–4049, 2014.

[4] T. Elomaa and M. Kaariainen, "An analysis of reduced error pruning,"*Journal of Artificial Intelligence Research*, vol. 15, pp. 163–187, 2001.

[5] J. J. A. Fournier, N. E. Mrabet and L. Goubin, "A survey of fault attacks in pairing based cryptography," *Cryptography and Communications-Discrete-Structures Boolean Functions and Sequences*, vol. 7, no. 1, pp. 185–205, 2015.

[6] J. Han, A. S. M. Kayes and A. Colman, "Ontcaac: An ontology-based approach to context-aware access control for software services," *Computer Journal*, vol. 58, no. 11, pp. 3000–3004, 2015.

[7] H. S. Hong and Z. X. Sun, "A key-insulated ciphertext policy attribute based signcryption for mobile networks," *Wireless Personal Communications*, vol. 95, no. 2, pp. 1215–1228, 2017.

[8] W. F. Hsien, C. C. Yang and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133-142, 2016.

[9] S. T. Hsu, C. C. Yang, and M. S. Hwang, "A study of public key encryption with keyword search", *International Journal of Network Security*, vol. 15, no. 2, pp. 71–79, Mar. 2013.

[10] M. S. Hwang, W. Y. Chao, C. Y. Tsai, "An improved key-management scheme for hierarchical access control," *International Journal of Network Security*, vol. 19, no. 4, pp. 639–643, 2017.

[11] G. Karatas and A. Akbulut, "Survey on access control mechanisms in cloud computing," *Journal of Cyber Security and Mobility*, vol. 7, pp. 1–36, 2018.

[12] S. S. Keerthi K. R. K. Murthy and M. N. Murty, "Rule prepending and post-pruning approach to incremental learning of decision lists," *Pattern Recognition*, vol. 34, no. 8, pp. 1697–1699, 2001.

[13] M. C. Li, Z. Z. Guo and W. F. Sun, "Attribute based encryption with attribute-sets and multi-authority," *Journal of Chinese Computer Systems*, vol. 32, no. 12, pp. 2419–2423, 2011.

[14] Y. F. Li, W. C. Zhang and P. Wang, "Research of post-pruning decision tree algorithm based on bayesian theory in discipline evaluation," *Computer*

Table 6: Comparison of operating time between ATSP-ABE and two ABE schemes when n=3

Scheme	Encryption time	Decryption time
Water *et al.*[15]	33ms	79ms
Yang *et al.*[16]	29ms	32ms
ATSP-ABE	16ms	16ms

Engineering and Design, vol. 34, no. 11, pp. 3873–3877, 2013.

[15] Z. Liu, Z. Jiang, X. Wang, S. Yiu, R. Zhang, and Y. Wu, "A temporal and spatial constrained attribute-based access control scheme for cloud storage," *TrustCom*, pp. 614–623, 2018.

[16] F. Liu, M. Yang and J. L. Han, "An efficient attribute based encryption scheme with revocation for outsourced data sharing control," in *Proceeding of the First International Conference on Instrumentation, Measurement, Computer, Communication and Control (IMCCC '11)*, pp. 20–23, 2011.

[17] M. Y. Luo and J. Ling, "A security cloud storage scheme based on cipertext policy attribute-based encryption," *Journal of Guangdong University of Technology*, vol. 31, no. 4, pp. 36–40, 2014.

[18] J. F. Ma, Q. Li and R. Li, "Large universe decentralized key-policy attribute-based encryption," *Securitys and Communication Networks*, vol. 8, no. 3, pp. 501–509, 2015.

[19] C. Mao, L. Liu, Z. Cao, "A note on one outsourcing scheme for big data access control in cloud," *International Journal of Electronics and Information Engineering*, vol. 9, no. 1, pp. 29–35, 2018.

[20] K. M. Osei-Bryson, "Post-pruning in decision tree induction using multiple performance measures," *Computers Operations Research*, vol. 34, no. 11, pp. 3331–3345, 2007.

[21] T. Peng, H. Ma and Z. H. Liu, "Directly revocable and verifiable key-policy attribute-based encryption for large universe," *International Journal of Network Security*, vol. 19, no. 2, pp. 272–284, 2017.

[22] B. D. Qin, *et al.*, X. F. Huang, Q. Tao, "Multi-authority attribute based encryption scheme with revocation," in *IEEE 24th International Conference on Computer Communication and Networks (ICCCN'15)*, 2015.

[23] S. Ryu, K. R. B. Butler and P. Traynor, "Leveraging identity-based cryptography for node ID assignment in structured P2P systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 12, pp. 1803–1815, 2009.

[24] D. S. Simoes and Z. S. Donizetti, "An access control mechanism to ensure privacy in named data networking using attribute-based encryption with immediate revocation of privileges," in *Proceedings of the 12th Annual IEEE Consumer Communications and Networking Conference (CCNC'15)*, 2015.

[25] L. Touati and Y. Challal, "Efficient CP-ABE attribute/key management for Iot applications," in *Proceedings of the IEEE International Conferences on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM)*, 2015.

[26] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," *Public Key Cryptography*, vol. 6571, pp. 53–70, 2011.

[27] T. Welzer, M. Holbl and B. Brumen, "An improved two-party identity-based authenticated key agreement protocol using pairings," *Journal of Computer and System Sciences*, vol. 78, no. 1, pp. 142–150, 2012.

[28] Y. Xie, H. Wen, B. Wu, Y. Jiang, and J. Meng, "A modified hierarchical attribute-based encryption access control method for mobile cloud computing," *IEEE Transactions on Cloud Computing*, vol. 7, no. 2, pp. 383–391, 2019.

[29] C. X. Xu, A. P. Xiong and Q. X. Gan, "A CP-ABE scheme with system attributes revocation in cloud storage," in *Proceedings of the 11th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP'14)*, 2014.

[30] W. C. Zhang, and Y. F. Li, "A post-pruning decision tree algorithm based on bayesian," in *Proceeding of the International Conference on Computational and Information Sciences (ICCIS'13)*, 2013.

[31] Y. Q. Zhang, Q. Q. Zhao and G. H. Zhang, "Ciphertext-policy attribute based encryption supporting any monotone access structures without escrow," *Chinese Journal of Electronicse*, vol. 26, no. 3, pp. 640–1815, 2017.

[32] Z. Y. Zhao and J. H. Wang, "Verifiable outsourced ciphertext-policy attribute-based encryption for mobile cloud computing," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 6, pp. 3254–3272, 2017.

Biography

Ze Wang received the BE degree and the ME degree both from Xi'an Jiaotong University, China, in 1998 and 2001 respectively, and the PhD degree from Northeastern University, China, in 2004. He has been an associate professor in the School of Computer Science and Technology Tianjin Polytechnic University in China since November

2006. His primary research interests include network security, mobile computing and distributed systems.

Minghua Gao is currently a master of software engineering from Tianjin Polytechnic University. he received the bachelor degree from Tianjin University of Technology in 2018. His research interests include network security and mobile computing.

Lu Cheng is currently a master candidate from Tianjin Polytechnic University. She received the bachelor degree from Tianjin University of Technology in 2015. Her research interests include network security and mobile computing.

Shimin Sun received the BE degree and the ME degree from Chongqing University of Posts and Telecommunications and Konkuk University, in 2002 and 2007 respectively, and the PhD degree from Konkuk University, Korea , in 2012. He has been an teacher in the School of Computer Science and Technology Tianjin Polytechnic University in China since 2016. His primary research interests include network security, Wireless Network Technology and Qos algorithm optimization.

A Lightweight User Authentication Scheme Based on Fuzzy Extraction Technology for Wireless Sensor Networks

Rui-Hong Dong, Bu-Bu Ren, Qiu-Yu Zhang, and Hui Yuan
(Corresponding author: Qiu-Yu Zhang)

School of Computer and Communication, Lanzhou University of Technology
No. 287,Lan-Gong-Ping Road, Lanzhou 730050,China
(Email: zhangqylz@163.com)

(Received July 9, 2019; Revised and Accepted Dec. 26, 2019; First Online Feb. 3, 2020)

Abstract

In order to improve the balanced relationships among security, privacy and design overhead for existing wireless sensor networks (WSNs) user authentication scheme, a lightweight user authentication scheme based on fuzzy extraction technology for WSNs. The present scheme combined with biometric fuzzy extraction technology and hash function to generate biometric key, which eliminates the user password factor in the existing authentication schemes. In addition, the proposed scheme can complete mutual authentication and session key agreement between legitimate users and sensor nodes only by using xor, hash and other operations with the lower computation overhead. And the heuristic security analysis, BAN logic model and random oracle model are used for security verification and performance analysis of the current scheme. The results of analysis and verification show that our scheme achieves more security and functional features, and keeps computational efficiency. Compared with other related works, our scheme is more suitable for practical application.

Keywords: BAN Logic; Biometric; Fuzzy Extraction Technology; User Authentication; Wireless Sensor Networks

1 Introduction

With the widespread popularity of short-range wireless communication technology, Wireless Sensor Networks (WSNs) has been widely deployed in environmental monitoring, agriculture, military, medical care and other fields due to its advantages [5, 10–12]. However, there are still existing a series of security problems [2, 4] owing to the limited energy resources of sensor nodes and WSNs working in wireless channels when people enjoy the convenience brought by WSNs. For example, WSNs nodes are captured and forged by an adversary easily. At present, some of the existing authentication scheme cannot fulfill the security application requirements of WSNs due to various vulnerabilities, making scholars suffer more new technical challenges which the most significant challenge in designing WSNs authentication scheme is to balance the relationships among security, privacy, and design overhead.

The essential key technologies applied in the WSNs security authentication scheme include: authentication technology based on lightweight public key algorithm, authentication technology based on pre-shared key, authentication technology based on one-way hash function and key management related technologies [7]. For the application of these technologies in the authentication scheme, researchers have done a lot of researches. Turkanović *et al.* [16] designed a user authentication scheme for heterogeneous Ad hoc WSN, in which sensor nodes were accessed by users directly. However, Amin *et al.* [1] found that the scheme [16] did nothing to prevent stolen smart card attack and user impersonation attack. Thus, Amin *et al.* [1] proposed a new WSN authentication scheme, but Wu *et al.* [19] demonstrated that the scheme [1] was in vulnerable to forgery attack by users, gateways and sensor nodes. Kumari *et al.* [8] designed a mutual authentication and key agreement scheme for WSNs by using chaotic map, but the scheme lacked of scalability. Wu *et al.* [18] proposed a lightweight authentication scheme with good security performance, however, it failed to resist DoS (Denial of Service attack). Shin *et al.* [14] suggested a two-factor authentication and key agreement scheme for 5G integrated WSN of the Internet of Things, but there existed man-in-the-middle attack in the scheme.

The application of biometric in WSNs user authentication has obvious advantages, and thence biometric-based WSNs user authentication scheme that is also a hot topic studied by researchers. Das *et al.* [3] put forward a three-factor WSNs user authentication scheme based on

multi-gateway, which solved the problem of users accessing node information across domains. Unfortunately, the scheme [3] failed to implement user anonymity. Srinivas *et al.* [15] proposed a security authentication scheme for the wireless medical architecture, but the scheme cannot prevent off-line password guessing attack. Both [6] and [13] added biometric features as new factor to existing two-factor authentication schemes, and designed an enhanced three-factor user authentication scheme, respectively. But Wang *et al.* [17] stated that the scheme [6] and [13] still cannot resist off-line password guessing attack. Li *et al.* [9] adopted the fuzzy commitment scheme to process the user's bioinformatics, who proposed a three-factor WSNs anonymous authentication scheme based on user password, smart card and biometric in the Internet of Things environment. However, their scheme has short of scalability.

Aiming at solving the problems mentioned above and improving the balanced relationships among security, privacy and design overhead of existing WSNs user authentication scheme, this paper presentd a lightweight WSNs user authentication scheme based on fuzzy extraction technology. The main contributions are as follows:

1) We propose a lightweight user authentication scheme based on fuzzy extraction technology for WSNs. The proposed scheme adopts fuzzy extraction technology to get the biometric key, which is used to replace the user password factor. Thus, the present scheme not only avoids an adversary carrying out attacks based on user password but also improves the security performance. What's more, the present scheme achieves authentication and session key agreement only by using low-cost operations such as xor and hash, where reduces the design cost of our scheme.

2) It indicates that the present scheme completes mutual authentication between legitimate users and sensor nodes through heuristic security analysis, BAN logic proof and random oracle model analysis. meanwhile, the proposed scheme is content with the ideal security requirements of user authentication scheme in WSNs, and can resist various common types of attacks. Compared with other related schemes, the scheme has a better balanced relationships among security, privacy and design overhead.

The rest of this paper is organized as follows: Section 2 introduces relevant theoretical knowledge, including one-way hash function, BAN logic model, fuzzy extraction technology, and system architecture of the present scheme. Section 3 describes the specific implementation process of the proposed WSNs security authentication scheme in detail. Section 4 and Section 5 provide security proof analysis and performance comparison analysis of the proposed scheme. Finally, it concluded our paper in Section 6.

2 Related Theoretical

2.1 One-Way Hash Function

The secure hash function converts input data of any length into a fixed-length of output data as a hash value [1]. In general, an ideal secure one-way hash function should have the following security properties:

1) Pre-image resistant: For a given hash value h, it is hard to find any message m, so that the equation $h = hash(m)$ holds.

2) Second Pre-image resistant: For a given message m_1, it is infeasible to find another existing message m_2 such that the equation $hash(m_1) = hash(m_2)$ holds.

3) Collision resistant: It is extremely difficult to find any pair (m_1, m_2) with $(m_1 m_2)$, so that the equation $hash(m_1) = hash(m_2)$ holds.

2.2 BAN Logic

Burrows-Abadi-Needham (BAN) logic plays an important role in the formal analysis of authentication scheme [1, 3, 6, 8, 9]. The symbols and rules of it's basis are shown in Table 1.

2.3 Fuzzy Extraction Technology

Fuzzy Extractor is information extraction function composed of $Gen(\cdot)$ function and $Rep(\cdot)$ function [9], which can extract uniform random strings and public information from the biometric template with given error tolerance t, and can also convert biometric information data into random values.

$Gen(\cdot)$ is the security key generation function. Input biometric information B_i, $Gen(\cdot)$ can output the secure data key σ_i and public auxiliary parameter τ_i.

$$Gen(B_i) = \langle \sigma_i, \tau_i \rangle .$$

$Rep(\cdot)$ is a secure key regeneration function. Input biometric information $B_i^{'}$ and public auxiliary parameter τ_i, $Rep(\cdot)$ can regenerate the secure data key σ_i.

$$Rep(B_i^{'}, \tau_i) = \sigma_i. \quad (1)$$

In Equation (1), only when $B_i^{'}$ is close to B_i under the allowable error tolerance t and the public auxiliary parameter τ_i is valid, can the $Rep(\cdot)$ recover the correct secure data key σ_i.

2.4 System Architecture

Figure 1 shows the proposed WSNs user authentication model. The proposed model mainly consists of three participants: multiple sensor nodes, one gateway node and one group of users. Compared with homogeneous WSNs, heterogeneous WSNs has longer network lifetime. Therefore, we adopt heterogeneous WSNs to design user authentication scheme.

Table 1: BAN logic notations and basic postulates

Symbol	Description	Rule	Description
$P \mid\equiv X$	P believes X	Message-meaning rule	$\frac{P\mid\equiv P\overset{K}{\longleftrightarrow}Q, P\triangleleft X_K}{P\mid\equiv Q\mid\sim X}$
$P \triangleleft X$	P sees X	Jurisdiction rule	$\frac{P\mid\equiv Q\mid\Rightarrow X, P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$
$P \mid\sim X$	P once said X	Nonce-verification rule	$\frac{P\mid\equiv\#(X), P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$
$P \mid\Rightarrow X$	P has jurisdiction over X	Freshness-conjuncatenation rule	$\frac{P\mid\equiv\#(X)}{P\mid\equiv\#(X,Y)}$
$\#(X)$	X is fresh	Belief rule	$\frac{P\mid\equiv Q\mid\sim(X,Y)}{P\mid\equiv Q\mid\sim X}$
$P \overset{K}{\longleftrightarrow} Q$	P and Q share secret K	Session key rule	$\frac{A\mid\equiv\#(K), A\mid\equiv B\mid\equiv X}{A\mid\equiv A\overset{K}{\longleftrightarrow}B}$

3 The Proposed Scheme

Our scheme contains three participants, user U_i, gateway GWN and sensor node SN_j. While achieving mutual authentication between U_i and SN_j, a session key for secure communication is negotiated. The detailed processing steps can be divided into six phases: pre-deployment, user registration, login and authentication, smart card revocation and reissue, biometric key update, and dynamic node addition. The detailed description of each phase is as follows. Table 2 shows the symbols used in the scheme.

3.1 Pre-Deployment Phase

The GWN generates a random secret value x_g, and then deploys nodes and cluster head nodes to the specific area for constructing a heterogeneous WSNs. After the network is set up, the GWN selects a unique identity ID_{SN_j} for each node in the network, and then calculates the shared key $k_j = h(ID_{SN_j} \,||\, x_g)$ between GWN and SN_j by using x_g. Finally, GWN stores $\langle ID_{SN_j}, k_j \rangle$ in the memory of the SN_j.

3.2 User Registration

Step 1. The user U_i selects his/her own identity ID_i and executes the registration process. Furthermore, U_i gets its own biometric information B_i with the help of hardware scanning device, and then calculates $< \sigma_i, \tau_i >= Gen(B_i)$ by using $Gen(\cdot)$ in fuzzy extraction technology, calculates $P_i = h(\sigma_i||ID_i)$ by using the obtained σ_i. Finally, U_i submits $< ID_i, P_i >$ to the GWN via the secure channel.

Step 2. After receiving the registration message from U_i, the GWN generates a random value ω and calculates $A_i = h(ID_i\|x_g\|P_i)$, $B = h(ID_i\|P_i\|\omega) \oplus A_i$, $C = h(\omega) \oplus h(ID_i\|P_i\|\omega)$, $D = h(ID_i\|P_i) \oplus \omega$, $e = E_{h(\omega)}(ID_i, P_i)$. And then GWN stores A_i into its own storage space and stores the calculated $< B, C, D, e, h(\cdot) >$ into a smart card SC_i corresponding to U_i, respectively. Subsequently, the GWN issues the SC_i with the information $< B, C, D, e, h(\cdot) >$ to the U_i via the secure channel.

Step 3. On receiving the SC_i issued by GWN, U_i embeds τ_i. $Rep(\cdot)$ into SC_i to complete the registration process of U_i.

Figure 2 shows the user registration process.

3.3 User Login and Authentication

In order to complete the authentication process, a session key is negotiated between U_i and SN_j, which will be used for secure communication after the mutual authentication. The phase is described as follows.

3.3.1 User Login

Step 1. U_i embeds his/her SC_i into the smart card reader, and then U_i inputs his/her ID_i and biometric information B_i^*. Through the secret data previously stored in SC_i, SC_i calculates $\sigma_i^* = Rep(B_i^*, \tau_i)$, $P_i^* = h(\sigma_i^*\|ID_i)$, $\omega^* = D \oplus h(ID_i\|P_i^*)$, $C^* = h(\omega^*) \oplus h(ID_i\|P_i^*\|\omega^*)$. Then SC_i verifies the validity of U_i by verifying $C^*? = C$. If the verification does not hold, the session is terminated. Otherwise, go to Step 2.

Step 2. SC_i generates a random number μ and calculates: $A_i = B \oplus h(ID_i\|P_i^*\|\omega)$, $f = A_i \oplus \mu$, $AID_i = h(A_i\|ID_i\|\mu\|T_1)$, $DID_i = h(AID_i\|A_i\|\mu\|T_1)$, where T_1 is the current timestamp selected by SC_i. Let $M_1 =< e, f, DID_i, T_1 >$, and then SC_i sends the login message M_1 to the GWN via the public channel to complete the user login process.

Figure 3 describes the user login process.

3.3.2 User Authentication

Step 1. After receiving the login message M_1 of U_i, the GWN records the current time as T_2, and then checks the validity of the timestamp, i.e. $|T_2 - T_1| \leqslant \Delta T$, where ΔT is the maximum transmission delay of the system. If $|T_2 - T_1| \leqslant \Delta T$ does not hold, the session is rejected by GWN. Otherwise, the GWN go to Step 2.

Step 2. The GWN decrypts the received message e with the aid of the random number ω, i.e. $< P_i^*, ID_i^* >\leftarrow$

Table 2: Notations and their meanings

Symbol	Description
U_i, SN_j, GWN	ith user, jth sensor node, gateway node
SC_i	ith user's smart card
ID_i, B_i, ID_{SN_j}	$U_i's$ identity, $U_i's$ biometric, $SN_j's$ identity
$Gen(\cdot)$, $Rep(\cdot)$	Probability generation function and recovery function in fuzzy extractor
σ_i, τ_i	Biometric key and public reproduction parameter
$h(\cdot)$	One-way hash function
$E_k(\cdot), D_k(\cdot)$	Symmetric encryption/decryption using key k
x_g	Secret value generated by the gateway
μ, ω, ν	Random number generated by user (smart card), gateway and sensor node
$T_1, T_2, T_3, T_4, T_5, T_6$	Current timestamp of the system
$\triangle T$	Maximum transmission delay
SK	Session key between user and sensor node
$\oplus$	Bit-wise xor operation
$\|$	concatenate operation
A	Malicious attacker

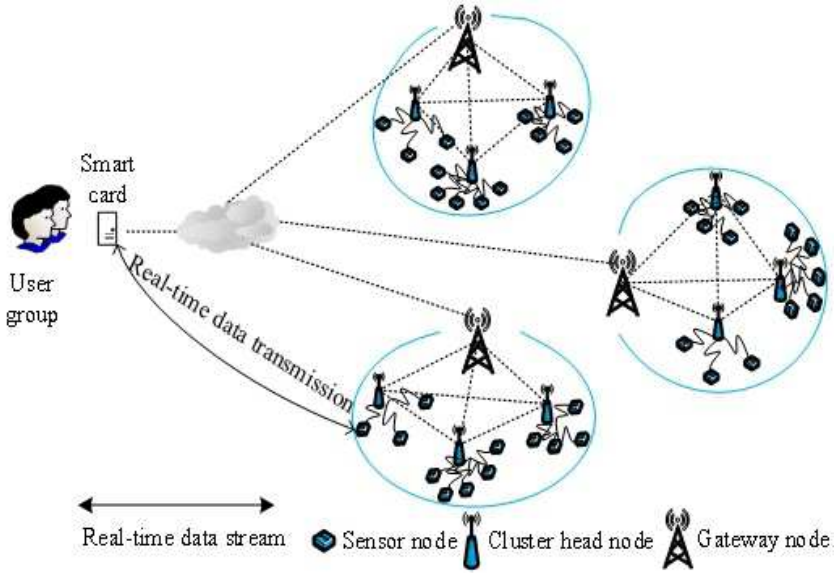


Figure 1: The proposed WSNs user authentication model

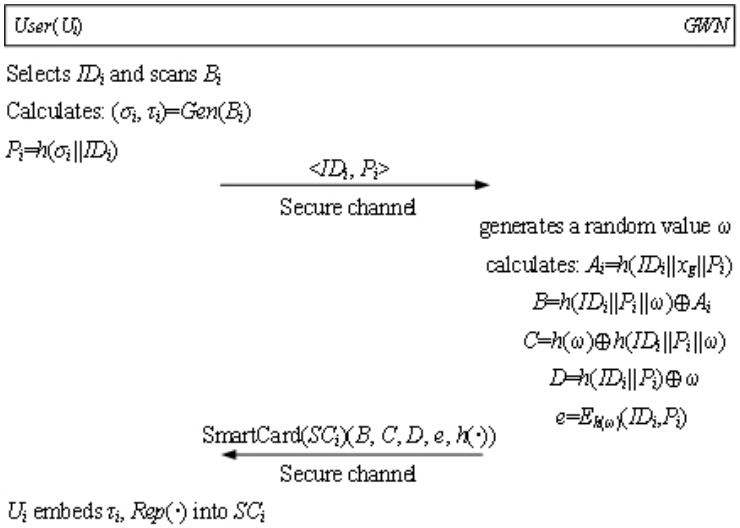


Figure 2: User registration phase

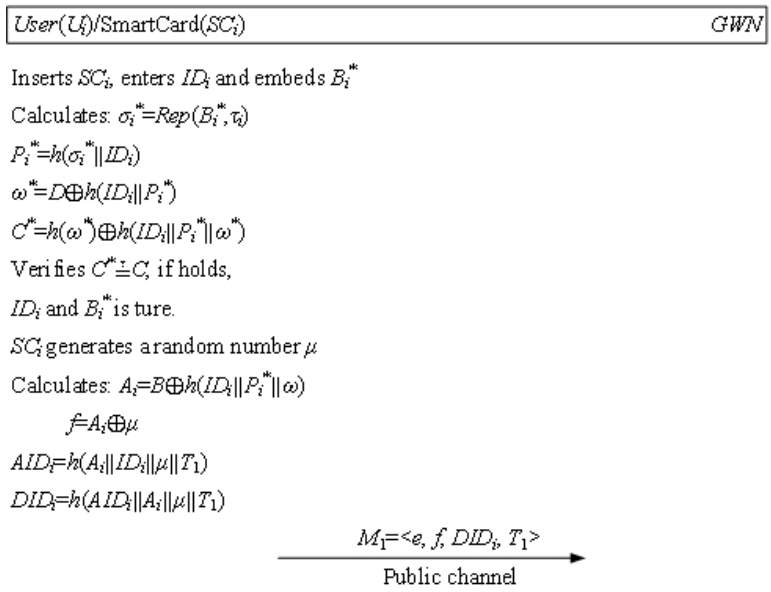


Figure 3: User login phase

$D_{h(\omega)}(e)$. After retrieving ID_i^* and P_i^* from message e, GWN calculates $G_i = h(ID_i^* \| x_g \| P_i^*)$, $\mu^* = f \oplus G_i$ and $AID_i^* = h(G_i \| ID_i^* \| \mu^* \| T_1)$. Then GWN verifies $h(G_i \| AID_i^* \| \mu^* \| T_1) \stackrel{?}{=} DID_i$, if the verification does not hold, GWN terminates the session. Otherwise, go to Step 3.

Step 3. GWN selects the current timestamp as T_3 and calculates: $J_g = h(ID_{SN_j} \| x_g)$, $L_g = J_g \oplus (AID_i^* \| \mu^*)$, $Auth = h(J_g \| AID_i^* \| \mu^* \| T_3)$. Let $M_2 =< L_g, Auth, T_3 >$, then GWN sends the message M_2 to the SN_j via the public channel.

Step 4. On receiving the message M_2 sent by the GWN, SN_j records the current time as T_4. Then SN_j verifies whether $|T_4 - T_3| \leqslant \Delta T$ holds, and if not, the connection is terminated. Otherwise, SN_j go to Step 5.

Step 5. SN_j retrieves AID_i and μ by using the previously stored k_j, i.e. $(AID_i^{**} \| \mu^{**}) = k_j \oplus L_g$. Go a step further, SN_j verifies $h(k_j \| AID_i^{**} \| \mu^{**} \| T_3) \stackrel{?}{=} Auth$, if the verification is valid, go to Step 6. Otherwise, the session is aborted.

Step 6. SN_j generates a random number ν and calculates $R = (AID_i^{**} \| \mu^{**}) \oplus \nu$, $SK = h(AID_i^{**} \| \mu^{**} \| \nu \| ID_{SN_j})$, $Auth' = h(ID_{SN_j} \| \nu \| SK \| T_5)$, where T_5 is the current timestamp selected by SN_j. Let $M_3 =< Auth', R, T_5, ID_{SN_j} >$, then SN_j sends message M_3 to U_i via the public channel.

Step 7. After receiving the feedback message M_3 sent from the SN_j, the U_i records the current time as T_6. Then U_i verifies whether $|T_6 - T_5| \leqslant \Delta T$ holds, and if $|T_6 - T_5| \leqslant \Delta T$ does not hold, the phase is terminated. Otherwise, go to Step 8.

Step 8. Through the existing AID_i and μ, U_i calculates $\nu^* = R \oplus (AID_i \| \mu)$, $SK^* = h(AID_i \| \mu \| \nu^* \| ID_{SN_j})$. Then U_i verifies $h(ID_{SN_j} \| \nu^* \| SK^* \| T_5) \stackrel{?}{=} Auth'$, if the verification does not hold, U_i terminates the session. Otherwise, it is believed that U_i and SN_j have completed mutual authentication, i.e. $SK^* = SK$. SK is the session key negotiated by U_i and SN_j, which is used to ensure the secure communication between U_i and SN_j.

Figure 4 is a detailed description of the user authentication process.

3.4 Smart Card Revocation and Reissue

When the U_i wants to reissue the smart card due to the loss of the smart card, the proposed scheme should provide the smart card revocation and reissue phase. The U_i selects a different identity ID_i^{new} to issue a new SC_i^{new} with ID_i^{new}. The process is below:

1) U_i sends the ID_i^{old} with P_i and ID_i^{new} to GWN, then GWN verifies $A_i^{old} \stackrel{?}{=} h(ID_i^{old} \| P_i \| x_g)$ by using the existing A_i^{old} in GWN. If the verification does not hold, the session is terminated. Otherwise, GWN believes that user is legitimate and calculates $A_i^{new} = h(ID_i^{new} \| x_g \| P_i)$, $B^{new} = h(ID_i^{new} \| P_i \| \omega) \oplus A_i^{new}$, $C^{new} = h(\omega) \oplus h(ID_i^{new} \| P_i \| \omega)$, $D^{new} = h(ID_i^{new} \| P_i) \oplus \omega$, $e^{new} = E_{h(\omega)}(ID_i^{new}, P_i)$.

2) Subsequently, GWN revokes A_i^{old} and storages A_i^{new}, and then updates $< B, C, D, e, h(\cdot) >$ with $< B^{new}, C^{new}, D^{new}, e^{new}, h(\cdot) >$ stored in SC_i^{new}. At least, GWN issues the new SC_i^{new} to U_i. Only by authenticating with ID_i^{new} can U_i log in to the network at next time.

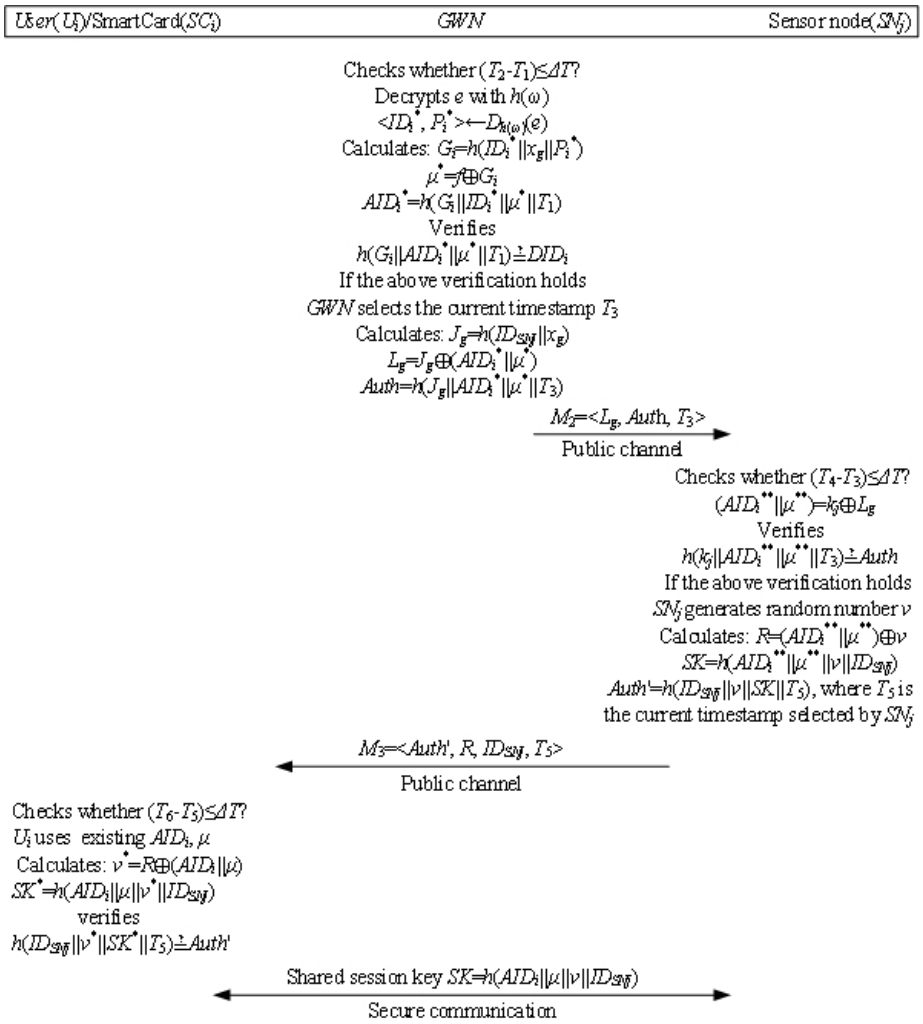


Figure 4: Mutual authentication phase

3.5 Biometric Update

U_i inputs his/her ID_i and embeds biometric information B_i^{old} into SC_i, and calculates $\sigma_i^{old} = Rep(B_i^{old}, \tau_i)$, $P_i^{old} = h(\sigma_i^{old}||ID_i)$, $\omega^{old} = D \oplus h(ID_i||P_i^{old})$, $C^{old} = h(\omega^{old}) \oplus h(ID_i||P_i^{old}||\omega^{old})$.Then the SC_i checks the validity of the c, i.e. $C^{old} \stackrel{?}{=} C$, if the verification is vaild, U_i inputs new biometric information B_i^{new} and calculates $< \sigma_i^{new}, \tau_i^{new} >= Gen(B_i^{new})$, $P_i^{new} = h(\sigma_i^{new}||ID_i)$, and then submits $< ID_i, P_i^{new} >$ to GWN.

On receiving the U_i's request message, the GWN utilizes ω to calculate $A_i^{new} = h(ID_i||x_g||P_i^{new})$, $B^{new} = h(ID_i||P_i^{new}||\omega) \oplus A_i$, $C^{new} = h(\omega) \oplus h(ID_i||P_i^{new}||\omega)$, $D^{new} = h(ID_i||P_i^{new}) \oplus \omega$, $e^{new} = E_{h(\omega)}(ID_i, P_i^{new})$. Then GWN replaces $< B, C, D, e >$ with $< B^{new}, C^{new}, D^{new}, e^{new} >$ and stores it in SC_i. Subsequently, GWN issues SC_i with $< B^{new}, C^{new}, D^{new}, e^{new}, h(\cdot) >$ to U_i. After receiving the SC_i from GWN, U_i embeds τ_i^{new}, $Rep(\cdot)$ into the SC_i, which is used to assist the U_i's login validation.

3.6 Dynamic Node Addition

After the WSNs is built, some sensor nodes may be physically captured by an adversary, so new sensor nodes need to be added to a specific area. GWN can accomplish this process by deploying new sensor nodes in the target area during the pre-deployment phase of the system. In addition, the process is executed in offline mode. The steps are as follows:

Step 1. GWN selects a unique random identity $ID_{SN_j}^{new}$ for SN_j^{new}.

Step 2. The shared key $k_j^{new} = h(ID_{SN_j}^{new}||x_g)$ between GWN and SN_j^{new} is calculated by GWN.

Step 3. Before the new node SN_j^{new} is deployed, the GWN stores parameters $< ID_{SN_j}^{new}, k_j^{new} >$ in the memory of SN_j^{new}. Finally, GWN feeds back the newly added node identity to the user so that the user can access the new sensor data.

4 Security Analysis

According to the present scheme, the user can obtain different sensor node information by single registration to the gateway. Through the informal security analysis, the security performance of the proposed scheme is analyzed. BAN logic is used to prove the validity of the proposed scheme. Then, the formal security analysis of the proposed scheme is conducted. The models used include: DolevCYao threat model [2], BAN logic model and random oracle model [6].

4.1 Heuristic Security Analysis

The Dolev-Yao threat model indicates that communication between two entities takes place on an open channel. Thus attackers can modify, delete or eavesdrop the message being transmitted. This section makes use of the extended adversary model hypothesis and based on it [17], through informal security analysis, which shows our scheme can get the following security requirements and resist the following attacks.

1) Mutual authentication. The authentication scheme must fulfill that two entities in communication can verify each other's identity. In the proposed scheme, entities involved are U_i, GWN and SN_j. In the process of participating in the three entities to negotiate authentication, GWN verifies the legitimacy of U_i by checking the DID_i in message M_1, SN_j verifies GWN directly and U_i indirectly by checking the $Auth$ in the message M_2. U_i completes the direct authentication of SN_j and the indirect authentication of GWN by checking $Auth^{'}$. Therefore, the proposed scheme realizes mutual authentication among U_i, GWN and SN_j. That is to say, our scheme achieves the security requirement of mutual authentication.

2) User anonymity. Since the communication is conducted in an insecure and open channel, an attacker may eavesdrop on request and response messages among U_i, GWN and SN_j, thereby creating malicious attacks by tracking the activities of legitimate staff. However, in this present scheme, all information related to the user identity ID_i, such as A_i, AID_i, and so on, which are protected by irreversible one-way hash function. Therefore, no attacker is able to retrieve the user's valid identity ID_i. In other words, our scheme provides anonymity for users.

3) Scalability. The proposed scheme provides a dynamic node addition function. If there is demand in the actual application, new sensor nodes can be added to the network without changing the configuration of the system. Consequently, our scheme can expand its deployment domain and meet the scalability requirements of authentication scheme.

4) Forward security. In the present scheme, it is assumed that the long-term private key x_g of the gateway node is compromised, and so an attacker attempts to retrieve the session key. Even if the long-term private key is known, the attacker is unable to generate the session key $SK = h(AID_i \| \mu \| \nu \| ID_{SN_j})$. The reason is that the session key relies on the random number generated by the smart card and the sensor node, it is difficult for an attacker to obtain the random number μ and ν. Thereby the proposed scheme ensures perfect forward security.

5) Known session key security. In our scheme, U_i and SN_j are independent computation session key $SK = h(AID_i \| \mu \| \nu \| ID_{SN_j})$. Even if an attacker successfully destroys any previously negotiated session key, the attacker cannot extract any secret parameters to calculate the newly negotiated session key. The reason is that the key parameters are protected by one-way hash function during the whole authentication and key agreement process. Therefore, the proposed scheme provides known session key security.

6) Privileged-insider attack. During the registration phase of our scheme, the secret biometric credential σ_i of the new user U_i is not directly sent in plain text. Instead, the hidden pseudo-biometric $P_i = h(\sigma_i \| ID_i)$ is sent to trusted GWN via secure channel. From the attacker's point of view, since the irreversible property of one-way hash function, the insiders of the GWN are unable to export user's privacy. As a result, the proposed scheme can withstand attack from privileged-insider.

7) Password/Biometric guessing attack. The present scheme achieves mutual authentication only by using biometric information B_i and identity ID_i of user. Hence, the proposed scheme avoids the usage of passwords, and there is no password guessing attack. Moreover, since the proposed scheme does not store the biometric key P_i on SC_i, so that, an attacker wants to guess the biometric key is infeasible. Hence there is that our scheme can prevent password guessing and biometric key guessing attack.

8) Replay and man-in-the-middle attack. Suppose that an attacker steals the login request message $M_1 =< e, f, DID_i, T_1 >$ during the login process, and sends the same message to GWN after a period of time. On receiving the message, the GWN checks the validity of T_1 by the condition $|T_2 - T_1| \leqslant \Delta T$, so as to judge the validity of message M_1. If $|T_2 - T_1| \leqslant \Delta T$ holds, GWN believes that the message M_1 is new. Conversely, the GWN ensures that the received message M_1 is not a new message, in that case, the GWN will immediately discard the message. Other messages in the U_i, GWN and SN_j also ensures the validity of the transmitted messages by using timestamps. In

consequence, the present scheme is free from replay attack.

Furthermore, in the case where without knowing the authentication parameter A_i, AID_i, P_i, μ, ν, k_j of user U_i and sensor SN_j, an attacker is unable to calculate $Auth$ successfully. Therefore, the attacker cannot be authenticated by SN_j, and the attacker cannot set up a valid session with SN_j, too. In other words, the man-in-the-middle attack to our scheme can be avoided.

9) Forgery attacks. U_i forgery attack: Suppose an attacker intercepts the login message from a previous sessions, and then the attacker forges the message and sends it to GWN. When receiving the forged message, GWN calculates $< ID_i^*, P_i^* > D_{h(\omega)}(e)$, $G_i^* = h(ID_i^* \| x_g \| P_i^*)$, $\mu^* = G_i^* \oplus f$, $AID_i^* = h(G_i^* \| ID_i^* \| \mu^* \| T_1)$. Then, by verifying the condition $h(G_i^* \| AID_i^* \| \mu^* \| T_1) \stackrel{?}{=} DID_i$, GWN could judge the legitimacy of user U_i. Although the attacker could forge the login request message without the knowledge of ID_i, x_g, f, the attacker also needs to compute the valid DID_i, which is difficult. Thus, our scheme can resist U_i forgery attack.

   GWN forgery attack: In the authentication and key agreement process of the proposed scheme, it can be seen that in the authentication message $M_2 =< L_g, Auth, T_3 >$, Auth is protected by one-way hash function. Without the knowledge of $J_g = h(ID_{SN_j} \| x_g)$ and $AID_i = h(G_i \| ID_i \| \mu \| T_1)$, an attacker has no any ability to forge Auth. As a result, our scheme can withstand GWN forgery attack.

   SN_j forgery attack: If an attacker wants to forge message $M_3 =< Auth^{'}, R, ID_{SN_j}, T_5 >$, then the attacker needs to know $SK = h(ID_{SN_j} \| \nu \| \mu \| AID_i)$ for the purpose of calculating $Auth^{'}$. But the SK is protected by one-way hash function, and hence our scheme can refuse SN_j forgery attack.

10) DoS attack. In the proposed scheme, even if an attacker has a user who loses the smart card, the attacker cannot log in to the system since the attacker needs to calculate $\sigma_i^* = Rep(B_i^*, \tau_i)$, $P_i^* = h(\sigma_i^* \| ID_i)$, $\omega^* = D \oplus h(ID_i \| P_i^*)$, $C^* = h(\omega^*) \| h(ID_i \| P_i^* \| \omega^*)$. After that, SC_i validates $C^*? = C$. The attacker cannot pass the verification and update the secret parameters stored in the SC_i without knowing the valid ID_i and B_i of legitimate user U_i. Therefore, our scheme is robust against DoS attack.

11) Session key computing attack. In the present scheme, after the mutual authentication, a secret session key SK is negotiated between the user and the sensor node for secure communication. $SK = h(AID_i \| \mu \| \nu \| ID_{SN_j})$ depends on the secret parameters (AID_i, μ, ν), which are protected by a one-way hash function. Thus, an attacker cannot calculate SK without knowing these secret parameters. Therefore, there is no session key computation attack in our scheme.

12) Stolen smart card attack. The smart card of legitimate user U_i may be stolen by a malicious attacker. Assuming that an attacker can extract secret information from a smart card, he/she is still unable to log in to the network. The reason is that the attacker also needs to know the identity ID_i and biometric information B_i of the legitimate user U_i, so that he/she can generate the login message $M_1 =< e, f, DID_i, T_1 >$. Among them, $DID_i = h(A_i \| AID_i \| \mu \| T_1)$, $AID_i = h(A_i \| ID_i \| \mu \| T_1)$, $A_i = B \oplus h(ID_i \| P_i^* \| \omega)$. Even if the attacker can successfully guess the vaild ID_i of the legitimate user U_i, he/she can't calculate the valid A_i. Thus, our scheme can avoid the attack of stolen smart card.

13) Many logged-in users with the same login-id attack. In the proposed scheme, even if two or more users have the same identity ID_i, they cannot successfully log in to the network. The reason is that they also need to get the biometric information B_i of legitimate users. Only legitimate users have B_i, and other users cannot imitate and obtain B_i. Hence, our scheme can resist many logged in users having same login-id attack.

14) Node capture attack. In our scheme, GWN calculates the shared key $k_n = h(x_g \| ID_{SN_n})(n = 1, 2, \cdots, N)$ between the GWN and sensor nodes. An attacker is unable to get the shared key $k_n(n = 1, 2, \cdots, N)$ between GWN and other sensor nodes, even if the attacker obtains the shared key k_j between GWN and SN_j by physically destroying the sensor node. Because when GWN calculates $k_n(n = 1, 2, \cdots, N)$, the unique identity $ID_{SN_n}(n = 1, 2, \cdots, N)$ is assigned by GWN for different sensor nodes is different. That is to say, the $k_n(n = 1, 2, \cdots, N)$ of a single node is captured will not affect the $k_n(n = 1, 2, \cdots, N)$ of other nodes is captured. In addition, the secret session key $SK = h(AID_i \| \mu \| \nu \| ID_{SN_j})$ that is generated between the U_i and the SN_j, their ν and ID_{SN_j} are different from each other for different sensor nodes. Therefore, our scheme has the ability to prevent node capture attack.

4.2 Authentication Proof Based on BAN Logic

This section proves that the proposed scheme completes mutual authentication between U_i and SN_j by using BAN logic model.

Goals: According to the analysis process of BAN logic, the following verification goals must be met for prov-

ing the present scheme that achieves mutual authentication.

$$G_1 : SN_j \mid\equiv U_i \mid\equiv (U_i \overset{SK}{\longleftrightarrow} SN_j).$$
$$G_2 : SN_j \mid\equiv (U_i \overset{SK}{\longleftrightarrow} SN_j).$$
$$G_3 : U_i \mid\equiv SN_j \mid\equiv (U_i \overset{SK}{\longleftrightarrow} SN_j).$$
$$G_4 : U_i \mid\equiv (U_i \overset{SK}{\longleftrightarrow} SN_j).$$

Generic form: In the present scheme, the generic form of message transmission can be abbreviated as follows:

$$\begin{aligned} M_1, U_i \rightarrow GWN : e &= E_{h(\omega)}(ID_i, P_i), \\ A_i &= B \oplus h(ID_i, P_i^*, \mu), \\ f &= A_i \oplus \mu, T_1, \\ DID_i &= h(A_i, AID_i, \mu, T_1). \\ M_2, GWN \rightarrow SN_j : L_g &= J_g \oplus (AID_i^*, \mu^*), \\ T_3, Auth &= h(J_g, AID_i^*, \mu^*, T_3). \\ M_3, SN_j \rightarrow U_i : R &= (AID_i^{**}, \mu^{**}) \oplus \nu, \\ Auth^{'} &= h(ID_{SN_j}, \nu, T_5, SK), \\ SK &= h(AID_i^{**}, \mu^{**}, \nu, ID_{SN_j}) \\ & \quad T_5, ID_{SN_j}. \end{aligned}$$

Idealized form: In the proposed scheme, the idealized form of message transmission can be described as follows:

$$\begin{aligned} & M_1, U_i \rightarrow GWN : \\ & \quad < U_i \overset{h(ID_i \| x_g)}{\longleftrightarrow} GWN, \mu, T_1, ID_i >_{U_i \overset{DID_i}{\longleftrightarrow} GWN} \\ & M_2, GWN \rightarrow SN_j : \\ & \quad < GWN \overset{L_g}{\longleftrightarrow} SN_j, T_3, GWN \overset{Auth}{\longleftrightarrow} SN_j, \\ & \quad U_i \mid\sim (U_i \overset{AID_i, \mu}{\longleftrightarrow} SN_j) >_{GWN \overset{h(ID_{SN_j} \| x_g)}{\longleftrightarrow} SN_j} \\ & M_3, SN_j \rightarrow U_i : \\ & \quad < SN_j \overset{R}{\longleftrightarrow} U_i, T_5, \nu, SN_j \overset{Auth}{\longleftrightarrow} U_i, \\ & \quad SN_j \mid\sim (U_i \overset{SK}{\longleftrightarrow} SN_j) >_{SN_j \overset{AID_i}{\longleftrightarrow} U_i} \end{aligned}$$

Hypothesis: In order to analyze the proposed scheme, the following assumptions are made for the initial state:

$$\begin{aligned} A_1 &: U_i \mid\equiv \#(T_1), U_i \mid\equiv \#(\mu), U_i \mid\equiv \#(\nu), \\ &\quad U_i \mid\equiv \#(T_5). \\ A_2 &: GWN \mid\equiv \#(T_1), GWN \mid\equiv \#(\mu), \\ &\quad GWN \mid\equiv \#(T_3). \\ A_3 &: SN_j \mid\equiv \#(\nu), SN_j \mid\equiv \#(\mu), SN_j \mid\equiv \#(T_3), \\ &\quad SN_j \mid\equiv \#(T_5). \\ A_4 &: GWN \mid\equiv (U_i \overset{h(ID_i \| x_g)}{\longleftrightarrow} GWN). \\ A_5 &: GWN \mid\equiv U_i \mid\Rightarrow (U_i \overset{DID_i}{\longleftrightarrow} GWN). \\ A_6 &: GWN \mid\equiv (U_i \overset{\mu}{\longleftrightarrow} GWN). \\ A_7 &: SN_j \mid\equiv (GWN \overset{h(ID_{SN_j} \| x_g)}{\longleftrightarrow} SN_j). \\ A_8 &: SN_j \mid\equiv GWN \mid\Rightarrow (GWN \overset{L_g}{\longleftrightarrow} SN_j). \\ A_9 &: SN_j \mid\equiv GWN \mid\Rightarrow (GWN \overset{Auth}{\longleftrightarrow} SN_j). \\ A_{10} &: SN_j \mid\equiv GWN \mid\Rightarrow (U_i \mid\sim (U_i \overset{AID_i, \mu}{\longleftrightarrow} SN_j)). \\ A_{11} &: U_i \mid\equiv SN_j \mid\Rightarrow (SN_j \overset{R}{\longleftrightarrow} U_i). \\ A_{12} &: U_i \mid\equiv SN_j \mid\Rightarrow (U_i \overset{SK}{\longleftrightarrow} SN_j). \\ A_{13} &: U_i \mid\equiv (U_j \overset{AID_i}{\longleftrightarrow} SN_j). \end{aligned}$$

Based on BAN logic rules and assumptions, the idealized form of the present scheme is analyzed. The main steps are described as follows.

According to the message M_1, it is easy to get:

$$S_1 : GWN \triangleleft < U_i \overset{DID_i}{\longleftrightarrow} GWN, \mu, T_1 >_{U_i \overset{h(ID_i \| x_g)}{\longleftrightarrow} GWN.}$$

From S_1, A_4 and A_5, by applying the message meaning rule, it is easy to get:

$$S_2 : GWN \mid\equiv U_i \mid\sim (U_i \overset{DID_i}{\longleftrightarrow} GWN, \mu, T_1, ID_i, U_i \overset{h(ID_i \| x_g)}{\longleftrightarrow} GWN).$$

From S_2, A_1 and A_2, by applying the freshness-conjuncatenation rule, it is easy to obtain:

$$S_3 : GWN \mid\equiv \#(U_i \overset{\mu}{\longleftrightarrow} GWN, DID_i, T_1, U_i \overset{h(ID_i \| x_g)}{\longleftrightarrow} GWN).$$

According to S_2 and S_3, by applying the nonce-verification rule, it is easy to get:

$$S_4 : GWN \mid\equiv U_i \mid\equiv (U_i \overset{\mu}{\longleftrightarrow} GWN, DID_i, T_1, U_i \overset{h(ID_i \| x_g)}{\longleftrightarrow} GWN).$$

According to S_4 and the belief rule, it is easy to get:

$$S_5 : GWN \mid\equiv U_i \mid\equiv (U_i \overset{\mu}{\longleftrightarrow} GWN).$$

According to S_5 and A_6, applying the jurisdiction rule, it is easy to obtain:

$$S_6 : GWN \mid\equiv (U_i \overset{\mu}{\longleftrightarrow} GWN).$$

According to the message M_2, it is easy to obtain:

$$S_7 : SN_j \triangleleft < GWN \overset{L_g}{\longleftrightarrow} SN_j,\ Auth,\ U_i \overset{AID_i, \mu}{\longleftrightarrow} SN_j, T_3 >_{SN_j \overset{h(ID_{SN_j} \| x_g)}{\longleftrightarrow} GWN}$$

From S_7, A_7 and A_8, applying the message meaning rule, it is easy to get:

$$S_8 : SN_j \mid\equiv SN_j \mid\sim (GWN \overset{L_g}{\longleftrightarrow} SN_j, U_i \overset{AID_i, \mu}{\longleftrightarrow} SN_j, Auth, T_3, SN_j \overset{h(ID_{SN_j} \| x_g)}{\longleftrightarrow} GWN).$$

From S_8, A_1, A_2, A_3, by applying the freshness-conjuncatenation rule, it is easy to get:

$$S_9 : SN_j \mid\equiv \#(GWN \overset{L_g}{\longleftrightarrow} SN_j, U_i \overset{\mu}{\longleftrightarrow} SN_j, Auth, T_3, SN_j \overset{h(ID_{SN_j}\|x_g)}{\longleftrightarrow} GWN).$$

According S_8 and S_9, applying the nonce-verification rule, it is easy to obtain:

$$S_{10} : SN_j \mid\equiv SN_j \mid\equiv (GWN \overset{L_g}{\longleftrightarrow} SN_j, U_i \overset{\mu}{\longleftrightarrow} SN_j, Auth, T_3, SN_j \overset{h(ID_{SN_j}\|x_g)}{\longleftrightarrow} GWN).$$

According S_{10} and the belief rule, it is easy to get:

$$S_{11} : SN_j \mid\equiv SN_j \mid\equiv (U_i \overset{\mu}{\longleftrightarrow} SN_j).$$

According S_{11} and A_{10}, by applying the jurisdiction rule, it is easy to get:

$$S_{12} : SN_j \mid\equiv (U_i \overset{\mu}{\longleftrightarrow} SN_j).$$

From S_6, S_{12}, A_7, A_9, applying the jurisdiction rule, it is easy to get:

$$S_{13} : SN_j \mid\equiv U_i \mid\equiv (U_i \overset{SK}{\longleftrightarrow} SN_j)(G_1).$$

According to S_{13} and A_{10}, by applying the jurisdiction rule, it is easy to get:

$$S_{14} : SN_j \mid\equiv (U_i \overset{SK}{\longleftrightarrow} SN_j)(G_2).$$

According to M_3, it is easy to get:

$$S_{15} : U_i \triangleleft < SN_j \overset{R}{\longleftrightarrow} U_i, T_5, \nu, SN_j \overset{Auth^{'}}{\longleftrightarrow} U_i, SN_j \mid\sim (U_i \overset{SK}{\longleftrightarrow} SN_j) >_{U_i \overset{AID_i}{\longleftrightarrow} SN_j}$$

According to S_{15}, A_{11} and A_{13}, by applying the message meaning rule, it is easy to get:

$$S_{16} : U_i \mid\equiv SN_j \mid\sim (SN_j \overset{R}{\longleftrightarrow} U_i, \nu, U_i \overset{AID_i}{\longleftrightarrow} SN_j, T_5)_{U_i \overset{SK}{\longleftrightarrow} SN_j.}$$

From S_{16}, A_1 and the freshness-conjuncatenation rule, it is easy to obtain:

$$S_{17} : U_i \mid\equiv \#(SN_j \overset{R}{\longleftrightarrow} U_i, \nu, U_i \overset{AID_i}{\longleftrightarrow} SN_j, T_5)_{U_i \overset{SK}{\longleftrightarrow} SN_j.}$$

According to S_{16} and S_{17}, by applying the nonce-verification rule, it is easy to get:

$$S_{18} : U_i \mid\equiv SN_j \mid\equiv (SN_j \overset{R}{\longleftrightarrow} U_i, \nu, U_i \overset{AID_i}{\longleftrightarrow} SN_j, T_5)_{U_i \overset{SK}{\longleftrightarrow} SN_j.}$$

According to S_{18} and the belief rule, it is easy to get:

$$S_{19} : U_i \mid\equiv SN_j \mid\equiv (U_i \overset{SK}{\longleftrightarrow} SN_j)(G_3).$$

According to S_{19} and A_{12}, applying the jurisdiction rule, it is easy to get:

$$S_{20} : U_i \mid\equiv (U_i \overset{SK}{\longleftrightarrow} SN_j)(G_4).$$

According to S_{13}, S_{14}, S_{19} and S_{20}, our scheme achieves the goals $(G_1 - G_4)$. User U_i and sensor node SN_j can authenticate each other and share a secure session key $SK = h(AID_i\|\mu\|\nu\|ID_{SN_j})$.

4.3 Formal Security Analysis Based on Random Oracle Model

In this section, the formal security analysis of the proposed scheme is carried out by using the random oracle model. The definition of hash function has been given in the foregoing, and the random oracle model is the idealized substitute of hash function in reality.

Theorem 1. *Assuming that the hash function $h(\cdot)$ is executed as oracle, the present scheme is secure for adversary A, who tries to retrieve P_i, ID_i and μ of legitimate user U_i, x_g of GWN, ν of SN_j and the session key SK shared between U_i and SN_j.*

Proof. Suppose that an adversary A extracts information $< B, C, D, e, h(\cdot) >$ from smart card by some means, and steals authentication message $M_2 = (L_g, Auth, T_3)$ and $M_3 = (Auth^{'}, R, T_5, ID_{SN_j})$. Then, the adversary A can derive P_i, ID_i and μ of legitimate user U_i, x_g of GWN, ν of sensor node SN_j, and the session key SK. Let the adversary A execute the experimental algorithms $EXP1^{JHKAS}_{HASH,A}$ and $EXP2^{JHKAS}_{HASH,A}$ that are shown in Algorithm 1 and Algorithm 2. The probability of success of algorithms $EXP1^{JHKAS}_{HASH,A}$ and $EXP2^{JHKAS}_{HASH,A}$ are defined as $Success1^{JHKAS}_{HASH,A} = \left|Pr\left[EXP1^{JHKAS}_{HASH,A} = 1\right] - 1\right|$ and $Success2^{JHKAS}_{HASH,A} = \left|Pr\left[EXP2^{JHKAS}_{HASH,A} = 1\right] - 1\right|$, and their advantage functions become $Adv1^{JHKAS}_{HASH,A}(t_1, qR) = max_A\left\{Success1^{JHKAS}_{HASH,A}\right\}$ and $Adv2^{JHKAS}_{HASH,A}(t_2, qR) = max_A\left\{Success2^{JHKAS}_{HASH,A}\right\}$ respectively. The maximum value is determined by three factors: adversary A, the execution time t_1 or t_2, and the number of queries qR get from the Reval oracle. If $Adv1^{JHKAS}_{HASH,A}(t_1) \leqslant \varepsilon$ and $Adv2^{JHKAS}_{HASH,A}(t_2) \leqslant \varepsilon, \forall \varepsilon > 0$, then the proposed scheme is provably secure resist A to get P_i, ID_i, μ, x_g, ν, SK. According to the attack experiments described in Algorithm 1 and Algorithm 2, if an adversary A could deal with the hash function problem, then the adversary A can obtain P_i, ID_i, μ, x_g, ν, SK. However, due to the irreversible property of hash function, it is infeasible to calculate the input value of a hash function $h(\cdot)$. Furthermore, there are $Adv1^{JHKAS}_{HASH,A}(t_1, qR) \leqslant \varepsilon$ and $Adv2^{JHKAS}_{HASH,A}(t_2, qR) \leqslant \varepsilon$, since $Adv1^{JHKAS}_{HASH,A}(t_1, qR)$ depends on $Adv1^{JHKAS}_{HASH,A}(t_1)$ and $Adv2^{JHKAS}_{HASH,A}(t_2, qR)$ depends on $Adv2^{JHKAS}_{HASH,A}(t_2)$. As a result, although A obtains information in SC_i and steals authentication messages M_2 and M_3, our scheme is provably secure against the adversary A to derive P_i, ID_i, μ, x_g, ν, SK. □

Algorithm 1 $EXP1_{HASH,A}^{JHKAS}$

Extract the information $B, C, D, e, h(\cdot)$ stored in the smart card by physically monitoring the power consumption of the device.
Call the Reveal oracle. Let $h(ID_i\|P_i\|\omega) \leftarrow Reveal(C)$
Call the Reveal oracle. Let $(ID_i^*, P_i^*) \leftarrow Reveal(h(ID_i\|P_i\|\omega))$
Computes $\omega^* = D \oplus h(ID_i^*\|P_i^*)$
Computes $C^* = h(\omega^*) \oplus h(ID_i^*\|P_i^*\|\omega^*)$
if $(C^* = C)$ **then**
  Accepts P_i^*, ID_i^* as the correct P_i, ID_i of user U_i
  return 1 (Success)
else
  return 0
end if

Algorithm 2 $EXP1_{HASH,A}^{JHKAS}$

Eavesdrop the authenticated message $M_2 = (L_g, Auth, T_3)$, where $L_g = J_g \oplus (AID_i\|\mu)$, $Auth = h(J_g\|AID_i\|\mu\|T_3)$, $J_g = h(ID_{SN_j}\|x_g)$.
Eavesdrop the authenticated message $M_3 = (Auth^{'}, R, T_5, ID_{SN_j})$, where $Auth^{'} = h(ID_{SN_j}\|\nu\|SK\|T_5)$, $R = (AID_i\|\mu) \oplus \nu$, $SK = h(AID_i\|\mu\|\nu\|ID_{SN_j})$.
Call the Reveal oracle. Let $({ID_{SN_j}}^*, \nu^*, SK^*, T_5^*) \leftarrow Reveal(Auth^{'})$
if $(T_5^* = T_5)$ **then**
  Accepts ${ID_{SN_j}}^*$, ν^*, SK^* as the correct ID_{SN_j}, ν, SK of SN_j
  Call the Reveal oracle. Let $(J_g^*, AID_i^{**}, \mu^{**}, T_5^*) \leftarrow Reveal(Auth)$
  if $(T_3^* = T_4)$ **then**
    Accepts J_g^*, AID_i^{**}, μ^{**} as the correct J_g, AID_i, μ of U_i and GWN
    Call the Reveal oracle. Let $({ID_{SN_j}}^*, x_g^*) \leftarrow Reveal(J_g^*)$
    if $({ID_{SN_j}}^* = ID_{SN_j})$ **then**
      Accepts x_g^* as the correct x_g of GWN
      return 1 (Success)
    else
      return 0
    end if
  else
    return 0
  end if
else
  return 0
end if

5 Performance Comparison of Scheme

To prove the superiority of the present scheme performance, this section compares the present scheme with other related schemes in terms of security features, computation overhead, communication overhead, storage overhead and method.

5.1 Performance Comparison of Scheme

Table 3 compares the security features of our scheme with related schemes [2, 6, 9, 10, 13, 19]. In the table, "$\surd$" denotes that the related scheme can resist the corresponding attack or it supports the corresponding security attribute, " $\times$ " denotes that the related scheme cannot resist the corresponding attack or it does not support the corresponding security attribute, " $-$ " denotes that the related scheme has not analyzed the corresponding security feature.

As can be seen from Table 3, compared with the relevant schemes, our scheme provides better security features and more functional attributes, such as forward security, scalability, resisting many logged in users having same login-id attack and so on. Therefore, our scheme is better in terms of security features.

5.2 Computation Overhead

Table 4 compares the computation overhead of our scheme with related schemes [2,6,9,10,13,19] during the authentication process.

The computation overhead in Table 4 is obtained by the approximate time required for conventional cryptographic operations [2]. Since the computation complexity of xor operation can be neglected, the time occupied by xor operation is not considered. As shown in Table 4, all scheme in [2, 9, 10, 13] are designed based on the elliptic curve cryptosystem (ECC), which has a high computation overhead. Therefore, our scheme is superior to that in [2,9,10,13] in terms of computation overhead. However, compared with those schemes in [6, 19], the computation overhead of our scheme is relatively high. The reason for that for the purpose of improving the performance of our scheme, this paper adopts the fuzzy extraction technology in the stage of biometric information processing. In addition, although these schemes in [6, 19] has a low computation cost, it has few security features and cannot meet the security requirements of the design authentication scheme. Meanwhile, it can be seen that the operations with high computation overhead in our scheme are concentrated on smart card and gateway, and the calculation involved by nodes is lower than others related scheme, which meets the requirements of practical application.

5.3 Communication Overhead

The communication overhead is obtained from the amount of information required for each message [2]. In our scheme, three messages ($M1, M2, M3$) are transmitted in the process of login and authentication, and the amount of information needed to transmit messages is 1136 bits. Compared with related schemes in Table 5, it

Table 3: Comparison of security features

Security attributes \ Scheme	[2]	[6]	[9]	[10]	[13]	[19(case1)]	our
Mutual authentication	√	√	√	×	√	√	√
User anonymous	√	×	√	×	×	√	√
Scalability	√	×	×	√	×	×	√
Forward security	×	×	√	–	√	×	√
Known key security security	√	√	√	×	√	×	√
Node capture attack	√	–	√	–	–	√	√
Session key calculation attack	√	√	√	×	√	√	√
Password/biometric guessing attack	√	×	√	×	×	√	√
Forgery attack	√	×	√	×	×	√	√
Man-in-the-middle attack	√	×	√	×	×	×	√
Privileged-insider attack	√	√	√	×	√	√	√
Smart card loss attack	√	–	√	×	–	√	√
Replay attack	√	√	√	√	√	–	√
DoS attack	√	–	√	√	–	√	√
Many logged in users having same login-id attack	–	–	–	–	–	–	√

Table 4: Performance comparison with related schemes in computation overhead

Scheme	computation overhead		
	User(s)	GWN(s)	Node(s)
[2]	$2T_ecm + 10T_h + 1T_fe \approx 0.0545$	$1T_ecm + 4T_h \approx 0.01838$	$5T_h \approx 0.0016$
[6]	$11T_h \approx 0.00352$	$11T_h \approx 0.00352$	$4T_h \approx 0.00128$
[9]	$2T_ecm + 8T_h \approx 0.03676$	$T_ecm + 9T_h \approx 0.01998$	$4T_h \approx 0.00128$
[10]	$3T_h + 1T_bp + 2T_ecm \approx 0.03966$	$1T_h + 2T_bp \approx 0.00932$	$3T_h + 1T_bp \approx 0.00546$
[13]	$2T_ecm + 10T_h + 2T_fe \approx 0.0716$	$16T_h \approx 0.00512$	$4T_h + 2T_ecm \approx 0.03548$
[19($case1$)]	$9T_h \approx 0.00288$	$11T_h \approx 0.00352$	$4T_h \approx 0.00128$
our	$12T_h + 2T_fe + 1T_sym \approx 0.04364$	$5T_h + 1T_sym \approx 0.0072$	$3T_h \approx 0.00096$

can be known that the communication overhead of our scheme is significantly lower than other related schemes, which meets the lightweight requirements of WSNs authentication scheme. Therefore, our scheme is more suitable for practical application.

Table 5: Performance comparison with related schemes in communication overhead

Scheme	communication overhead	
	Number of messages	Number of bits
[2]	3	1428
[6]	4	1536
[9]	4	1856
[10]	4	1408
[13]	4	5632
[19($case1$)]	4	2688
our	3	1136

5.4 Storage Overhead

The storage overhead is derived from the amount of information required for each secret information [2]. As smart card and gateway have better storage performance relative to sensor nodes, the impact of storage overhead of smart card and gateway on the performance of the present scheme is not considered. Table 6 shows the storage overhead of each scheme in sensor nodes. According to the data in the Table 6, the storage overhead of our scheme in the sensor node is the same as that in [2, 6, 9, 13], but lower than that in [10, 19], which meets the application requirements of WSNs in the Internet of Things.

The comprehensive performance comparison between our scheme and existing related schemes is presented in Figure 5.

Table 6: Performance comparison with related schemes in storage overhead

Scheme	storage overhead(bit)
[2]	176
[6]	176
[9]	176
[10]	416
[13]	176
[19($case1$)]	304
our	176

5.5 Method Comparison

In this paper, our method is further compared with those involved in relevant schemes [2, 6, 9, 10, 13, 19]. In [10, 19],

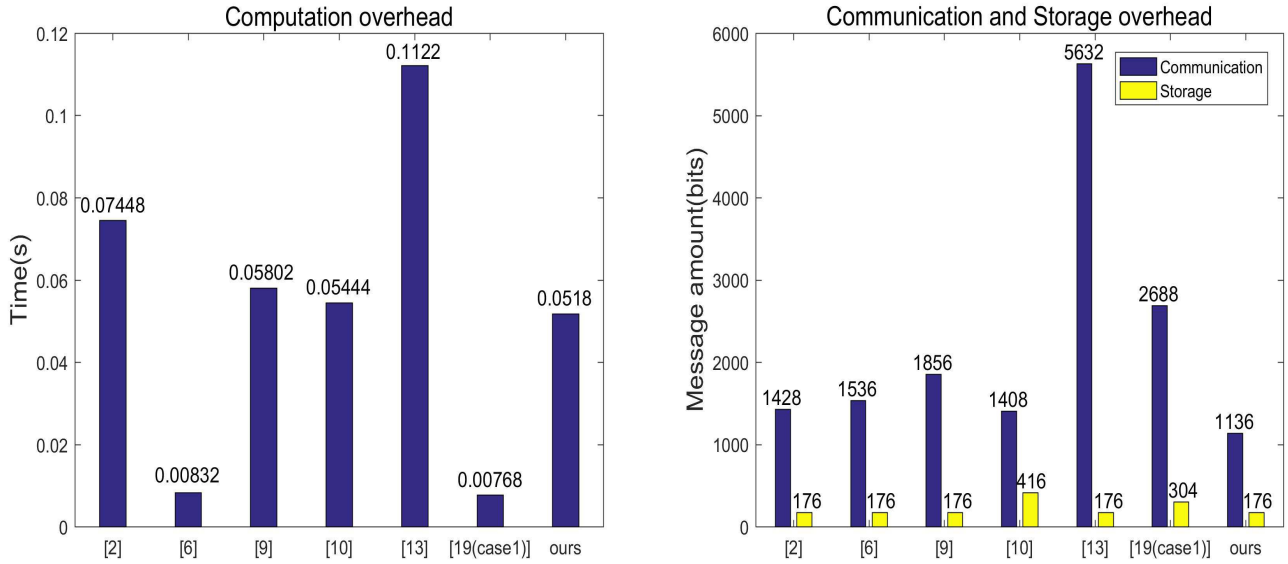


Figure 5: Comparisons of computing, communication and storage costs with related schemes

the author only used user password and smart card to design authentication and key negotiation scheme. Due to the vulnerability of password and smart card (easy to be stolen, *etc.*), the authentication scheme based on password and smart card is not very secure. In [6], the author used biological hash function to process user's biometrics. Although this operation hides user's biometrics, the biometrics are unique and stable. If the biometrics or biometric template is lost, which will still cause user's biometrics to be permanently unusable. In [9], the author utilized the fuzzy commitment mechanism to deal with user's biometrics, but user needs to transmit unprocessed biometrics to the GWN through the secure channel, which may directly lead to the loss of user's biometrics. In [2, 13], the author disposed of user's biometrics through fuzzy extraction technology, which solves the problem of permanent unavailability caused by biometric leakage. But their schemes were proposed by ECC, the calculation cost and communication cost are higher. Different from [2, 6, 9, 10, 13, 19], our scheme adopts the random key obtained by fuzzy extraction of biometrics as a biological factor replacing biometrics or biological templates directly to transmit and authenticate in the system. It can protect the biometrics and template well, and avoid permanent unusable of biometric caused by biometric leakage. Moreover, we only use the lightweight operations such as hash and xor to complete the scheme design during the negotiation process of the whole scheme. The verification method in section iv shows that we use the low-cost operation to complete the scheme design and achieve the security requirements of the authentication scheme. Therefore, the method of this paper is more superior.

6 Conclusions

To overcome the shortcomings of security authentication schemes for heterogeneous wireless sensor networks, we present a lightweight user authentication scheme based on fuzzy extraction technology. In our scheme, fuzzy extraction technique and hash operation are used to generate biometric key. Through the generated biometric key, the mutual authentication is completed between users and sensor nodes. After the mutual authentication, a shared session key is negotiated by the participants to ensure the subsequent secure communication in the network. And furthermore, in the process of whole authentication, our scheme utilizes hash, xor and other lightweight operations to realize the authentication, which reduces the design overhead. Through heuristic analysis, BAN logic proof and random oracle model verification, these show that our scheme can achieve mutual authentication between users and sensor nodes, and meet the security requirements of the authentication scheme. Compared with other related schemes, it can be seen that our scheme has more security features when the design cost is relatively low. Therefore, our scheme has a better balanced relationships among security, privacy and design overhead, and is more suitable for practical application. The drawback is that our authentication scheme has not been verified in practice. Additionally, extending the WSNs authentication scheme to 5G network architecture, and then combining 5G network architecture to design a secure and efficient authentication scheme is the focus of future research work.

Acknowledgments

The authors gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the

presentation.

References

[1] R. Amin and G. P. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Networks*, vol. 36, no. 1, pp. 58–80, 2016.

[2] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ecc-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Computers and Electrical Engineering*, vol. 69, pp. 534–554, 2018.

[3] A. K. Das, A. K. Sutrala, S. Kumari, V. Odelu, M. Wazid, and X. Li, "An efficient multi-gateway-based three-factor user authentication and key agreement scheme in hierarchical wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 13, pp. 2070–2092, 2016.

[4] 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.

[5] M. S. Hwang, E. F. Cahyadi, C. Y. Yang, and S. F. Chiou, "An improvement of the remote authentication scheme for anonymous users using an elliptic curve cryptosystem," in *IEEE 4th International Conference on Computer and Communications (ICCC'18)*, pp. 1872–1877, Dec. 2018.

[6] J. Jung, J. Moon, D. Lee, and D. Won, "Efficient and security enhanced anonymous authentication with key agreement scheme in wireless sensor networks," *Sensors*, vol. 17, no. 3, pp. 644–664, 2017.

[7] S. Kumari, M. K. Khan, and M. Atiquzzaman, "User authentication schemes for wireless sensor networks: A review," *Ad Hoc Networks*, vol. 27, no. 2015, pp. 159–194, 2015.

[8] S. Kumari, X. Li, F. Wu, A. K. Das, H. Arshad, and M. K. Khan, "A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps," *Future Generation Computer Systems*, vol. 63, no. 2016, pp. 56–75, 2016.

[9] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K. K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," *Journal of Network and Computer Applications*, vol. 103, no. 2018, pp. 194–204, 2018.

[10] C. H. Liu and Y. F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," *Computers and Electrical Engineering*, vol. 59, pp. 250–261, 2017.

[11] T. Maitra, R. Amin, D. Giri, and P. D. Srivastava, "An efficient and robust user authentication scheme for hierarchical wireless sensor networks without tamper-proof smart card," *International Journal of Network Security*, vol. 18, no. 3, pp. 553–564, 2016.

[12] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S. H. Islam, and P. Gope, "Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks," *Multimedia Tools and Applications*, vol. 77, no. 14, pp. 18295–18325, 2018.

[13] Y. H. Park and Y. H. Park, "Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks," *Sensors*, vol. 16, no. 12, pp. 2123–2139, 2016.

[14] S. Shin and T. Kwon, "Two-factor authenticated key agreement supporting unlinkability in 5g-integrated wireless sensor networks," *IEEE Access*, vol. 6, pp. 11229–11241, 2018.

[15] J. Srinivas, S. Mukhopadhyay, and D. Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," *Ad Hoc Networks*, vol. 54, no. 2017, pp. 147–169, 2017.

[16] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion," *Ad Hoc Networks*, vol. 20, no. 2014, pp. 96–112, 2014.

[17] C. Wang, G. Xu, and J. Sun, "An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks," *Sensors*, vol. 17, no. 12, pp. 2946–2965, 2017.

[18] F. Wu, X. Li, A. K. Sangaiah, L. Xu, S. Kumari, L. Wu, and J. Shen, "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," *Future Generation Computer Systems*, vol. 82, no. 2018, pp. 727–737, 2018.

[19] F. Wu, L. Xu, S. Kumari, X. Li, J. Shen, K. K. R. Choo, M. Wazid, and A. K. Das, "An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in iot deployment," *Journal of Network and Computer Applications*, vol. 89, no. 2017, pp. 72–85, 2017.

Biography

Dong Rui-hong. Researcher, worked at school of computer and communication in Lanzhou university of technology. His research interests include network and information security, information hiding and steganalysis analysis, computer network.

Ren Bu-bu. received the BS degrees in communication engineering from Lanzhou University of Technology, Gansu, China, in 2017. Currently, he is studying for his master's degree at Lanzhou University of Technology. His research interests include network and information security, wireless sensor network security authentication.

Zhang Qiu-yu. 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.

Yuan Hui. He graduated from South China University of Technology with a bachelor's degree and Beijing University of Posts and Telecommunications with a master's degree.He is now studying for a PhD at lanzhou university of technology.His research interests are machine learning, network security and intrusion detection.

Visible 3D-model Watermarking Algorithm for 3D-Printing Based on Bitmap Fonts

Changchun Yan[1], Guoyou Zhang[1], Anhong Wang[2], Li Liu[2], and Chin-Chen Chang[3]
(Corresponding author: Guoyou Zhang)
College of Computer Science and Technology, Taiyuan University of Science and Technology[1]
Taiyuan 030024, China
College of Electronic Information and Engineering, Taiyuan University of Science and Technology[2]
Department of Information Engineering and Computer Science, Feng Chia University[3]
(Email: zhangguoyou@tyust.edu.cn)
(Received Aug. 30, 2019; Revised and Accepted Jan. 6, 2020; First Online Feb. 3, 2020)

Abstract

The copyright protection of 3D model data is becoming more and more important with the development of the open Internet and 3D-priting. We propose a visible 3D-model watermarking algorithm for 3D-printing based on bitmap fonts to overcome the shortcoming that the current 3D model watermarking is visible only on a computer. First, bitmap fonts were used as input watermarking information. Then, the smooth region of the 3D model is subdivided selectively and projected onto a 2D plane based on the bitmap font. Next, the watermarking information is embedded into the 2D plane, and the corresponding region is projected onto the original meshes. Then, the watermark is embedded with a certain intensity so that it is still visible after the 3D-printing of the model. The results of experiments showed that the watermarking information including Chinese characters, English letters, and numbers is visible on the printed entities and that it is robust to common attacks.

Keywords: Bitmap Font; Three-Dimensional Model; 3D-Printing; Visible Watermark

1 Introduction

With the rapid development of 3D printing technology, 3D models are used extensively in many fields, and various 3D models can be obtained on the Internet. However, since pirates have made it easier to copy and tamper with the 3D models, obtaining copyright protection for such models has become a significant issue.

Traditional data-protection technologies, such as encryption, cannot protect the copyright of data, especially after the data are decrypted. Digital watermarking technology provides a way for protecting copyrights, *i.e.*, by embedding information, *i.e.*, a watermark, into the data [3, 4, 13]. Unlike encryption, digital watermarking does not restrict access to the data but ensures the hidden data remain inviolate and can be recovered. One form of digital watermarking, *i.e.*, 3D mesh watermarking technology, also has been used extensively for authenticating the content of 3D models and for making the content tamper proof.

The current 3D mesh watermarking techniques can be divided into invisible and visible techniques, depending on the transparency. Invisible watermarking ensures that the watermarked information does not change and rarely changes the appearance of the three-dimensional model after the information is embedded, and a specific algorithm can be used to extract the watermarking information. Ohbuchi *et al.* [12] published the first research paper related to invisible watermarking algorithms for 3D models, and they proposed two invisible watermarking schemes, *i.e.*, the triangle similarity quadruple (TSQ) scheme and the tetrahedral volume ratio (TVR) scheme. Even though the robustness of these algorithms was weak, it is notable that they were the forerunners of the subsequent 3D mesh digital watermarking technology. Generally, the invisible watermarking schemes in 3D models are focused on the transform domain [6,8,9,19] and the spatial domain [2, 5, 7, 11, 14–18]. The watermarking algorithm in the transform domain embeds watermark data in the spectrum coefficients of the Discrete Fourier Transform (DFT) [8], the Discrete Wavelet Transform (DWT) [6,19] and the Discrete Cosine Transform (DCT) [9]. The spatial domain watermarking algorithm embeds watermark data by modifying the values of the vertices or the geometric features. Cho *et al.* [5] used the vertex norm to embed the watermark into the Euclidean distance between the vertex and the reference structure, and they proposed two methods to embed the bits of the watermark by different histogram mapping functions. Later, several methods [2, 14, 16] were proposed based on different optimization methods to obtain minimal distortion of the surface in order to improve the transparency. Some of the char-

acteristics of the surface of the model were changed in order to embed watermarks and to enhance the robustness of watermarking, *e.g.*, invariant integral [15] and the curvature of the vertex curvature [18].

Visible watermarking completely maps the shape of the watermarking information to the shape of the three-dimensional model so that the user can clearly observe the watermarking information. Ohbuchi *et al.* [12] first proposed a visible watermarking algorithm for the mesh-density model. Then, Lu *et al.* [10] proposed visible watermarking for the three-dimensional mesh model in two views. However, the algorithm only gives the visible watermark effect of embedding several simple English characters. Subsequently, An *et al.* [1] proposed a visible watermarking scheme for 3D models based on adaptation of the boundary and subdivision of the mesh. The algorithm can process complex characters, and the watermark information at the edge is complete. However, the visible watermarking algorithm only can be displayed on the 3D model, and the print is not visible. Therefore, it is necessary to develop a three-dimensional watermark embedding algorithm that can make the watermark visible after 3D-printing.

Based on the analysis presented above, we propose a 3D model watermarking algorithm that would make the watermark visible in 3D-printing based on bitmap fonts to overcome the shortcoming that the watermark provided by the current 3D model is visible only on digital computers. First, a bitmap font was used to input the watermarking information. Second, the smooth region of the 3D model was subdivided selectively and projected onto a 2D plane based on the bitmap font. Third, the watermarking information was embedded into the 2D plane, and the corresponding region was projected onto the original meshes. Fourth, the watermark was embedded with a certain intensity so that it is still visible after the model is 3D-printed. The results of our experiment showed that the watermark was visible on both the 3D model and the printed entities. In addition, the approach we proposed and used was robust against common attacks.

The rest of this paper is arranged as follows. Section 2 provides the details of our algorithm. Section 3 provides the experimental results, and Section 4 presents our conclusions.

2 Our Proposed Visible Watermarking in 3D Printing

In this paper, a three-dimensional model, visible watermark embedding algorithm based on the bitmap font is proposed in order to overcome the shortcoming that 3D visible watermarks are no longer visible after 3D printing.

Figure 1 shows the flowchart of our method. The watermarking algorithm finds the corresponding 3D mesh model vertices by bitmap fonts, and it changes the position of the vertex to achieve the 3D-printing visible watermark. Note that the information for a 3D mesh model includes the coordinates of the vertices and the faces. We assumed that a 3D mesh model can be denoted as $Mod = (V, F)$,where V is the set of all vertices of the model, *i.e.*, $V = \{v_i | v_i = (x_i, y_i, z_i), x_i, y_i, z_i \in R, 1 \leq i \leq N\}$; N is the number of vertices; v_i is the vertex of the 3D model; x_i, y_i, and z_i are the horizontal, ordinate, and vertical coordinate values in the spatial coordinates, respectively; F is the set of all of the triangular faces that represent the topology of the mesh, *i.e.*, $F = \{f_i | f_i = (v_a, v_b, v_c), v_a, v_b, v_c \in V, 1 \leq i \leq N_f\}$; and N_f is the number of faces. The detailed processes are described below.

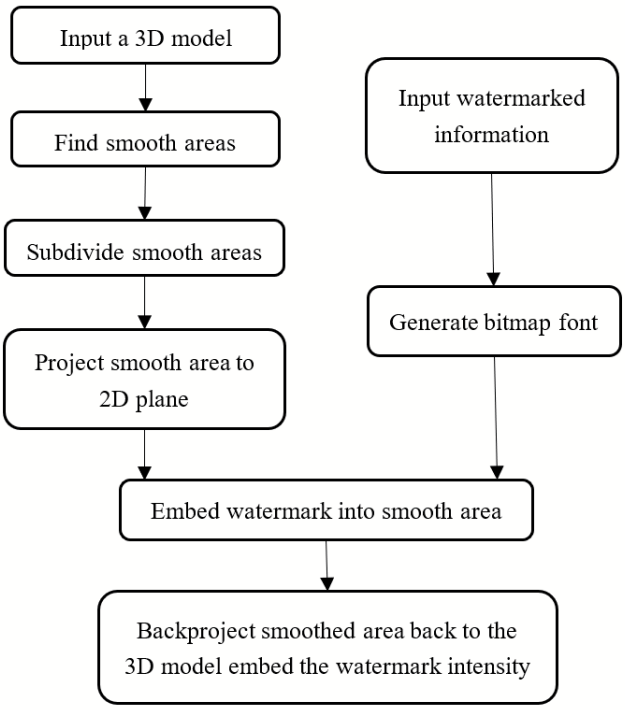


Figure 1: Flowchart of embedding the visible watermark

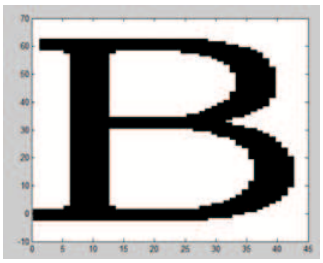
2.1 Generating the Bitmap Fonts for Watermark Information

A bitmap font divides each character into a number of points, and then it uses the value of each point to represent the outline of the character. The advantage of bitmap fonts is that there is very little change in the topology of the 3D mesh model, and the watermark information that is generated has little effect on subsequent printing of the model. Therefore, in this paper, we used the internal font structure LOGFONT in the Windows system to generate three-dimensional visible watermarks that included Chinese characters and English characters and numbers, which solved the problem of how to draw different language characters.

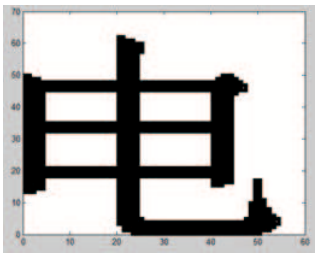
Assuming that the watermark information to be embedded is W, $W = (\alpha, \beta)$, where α is the watermark vertex pixel information, *i.e.*, $\alpha = \{0, 1\}$; β is

the watermark information vertex coordinate point, *i.e.*, $\beta = \{\beta_i | \beta_i = (x_i^w, y_i^w), 1 \leq i \leq Num\}$; (x_i^w, y_i^w) the coordinates of the plane watermark pixel, and Num is the number of vertices of the watermark information.

For example, after setting the height of the embedded watermark information – "B" character and "electric" Chinese character be 70 pixels, these two characters were parsed into the coordinate information and pixel information of each vertex of character outline by the GetGlyphOutline() function of Windows from the website. Figure 2 shows the watermark information to be embedded drawn by MATLAB after obtaining the "B" and Chinese character vertex coordinate information. The black portion is an area in which the bitmap font α is 1, and the white portion is an area in which the bitmap font α is 0.



(a) English character



(b) Chinese character

Figure 2: Bitmap fonts to be embedded

2.2 Processes of Embedding the Visible Watermark

The embedding of the visible watermark after 3D printing is done by changing the position of a vertex on a 3D model. The concrete watermark embedding process consists of the following six steps:

1) For each vertex $v_i (i = 1, 2, \ldots, N)$ of the 3D mesh model, find the vertex v_{max} as the smooth center point, $v_{max} = max(D(v))$ and its normal vector $\vec{n}(x_{max}, y_{max}, z_{max})$, $D(v_i)$ according to Equations (1) and (2).

$$d(v_i) = \frac{\sum_{v_j \in N_i} \cos(\vec{n}_{v_i}, \vec{n}_{v_j})}{N_i}, \quad (1)$$

$$D(v_i) = \sum_{n=p} d(v_i), \quad (2)$$

where N_i is the number of neighbors of the vertex v_i; $\vec{n}_{v_i}$ is the normal vector of the vertex v_i; $\vec{n}_{v_i}$ is the adjacent vertex normal vector; and p is the order number of neighbouring vertex of v_i. The area formed by the smooth center point, v_{max}, and its pth order neighborhood vertices is a smooth area $S = (V^m, F^m)$, where V^m is the vertex of the smooth area; $V^m = \{v_i^m | v_i^m = (x_i^m, y_i^m, z_i^m), x_i^m, y_i^m, z_i^m \in R, 1 \leq i \leq N_i \times p\}$, x_i^m, y_i^m, z_i^m are the values of the v_i^m coordinate; F^m are the faces of the smooth area, *i.e.*, $F^m = \{f_i^m | f_i^m = (v_1, v_2, v_3), v_1, v_2, v_3 \in V^m, 1 \leq i \leq N_i \times p\}$.

2) Traverse each triangular face in the smooth region, S, determine the center of gravity of each triangular face, and connect the center of gravity to each vertex of the triangular face to get three new triangular faces and form a new smooth area. Figure 3 shows the effect of triangle mesh subdivision. The red line shows the original faces of the 3D model, and the black line shows the subdivided faces.

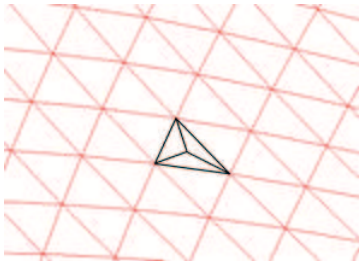


Figure 3: Triangle mesh subdivision

3) The Z-axis direction is transformed into the normal vector direction of the center point $\vec{n}(x_{max}, y_{max}, z_{max})$ when the origin of the coordinate system is unchanged, and the three-dimensional smooth region is projected onto the two-dimensional plane by the rotation matrix formula, which can be expressed as

$$\begin{bmatrix} X \\ Y \end{bmatrix} = R_x(\theta_a) R_y(\theta_b) \begin{pmatrix} x \\ y \\ z \end{pmatrix}, \quad (3)$$

where X, Y are the coordinates of the plane after two-dimensional transformation; R_x, R_y are the rotation matrices corresponding to x and y axes, respectively; x, y, z are the coordinate values of the smooth region; θ_a, θ_b are the angles between $\vec{n}(x_{max}, y_{max}, z_{max})$ and the real coordinate system of a three-dimensional model $y \cdot z$ plane and $x \cdot z$ plane.

4) Traversing the two-dimensional smooth region to determine the maximum and minimum values of the vertices in the smooth region, which are denoted by X_{max}, X_{min}, Y_{max}, and Y_{min}, respectively. Traversing the watermark information, W, to determine the

maximum and minimum values of the vertices in W, which are denoted by x^w_{max}, x^w_{min}, y^w_{max}, and y^w_{min}, respectively. Multiplying each vertex in the two-dimensional smooth region by the scaling factor, γ, to satisfy the conditional expression as $X_{max} - X_{min} > x^w_{max} - x^w_{min}$ and $Y_{max} - Y_{min} > y^w_{max} - y^w_{min}$.

The translation distances (D_x, D_y) between the center point of the smooth region and the vertex of the watermark information center were obtained by Formula (4). Move all of the vertices in the 2D smooth region as $v_i = (X_i + D_x, Y_i + D_y)$, where v_i is the vertex of a two-dimensional smooth region.

$$\begin{cases} D_x = X_0 - x_0 \\ D_y = Y_0 - y_0 \end{cases} \tag{4}$$

5) The bitmap font is composed of black and white. It is considered that black is 1 and white is 0. The bitmap font watermark information, W, is traversed, and the position information of the previous vertex is taken in the opposite direction of the X and Y axes, forming a rectangular area when the vertex marked with 1 is detected. As shown in Figure 4, Point A is to detect the point where α is 1, B is the previous vertex, and the red square is the rectangular area.

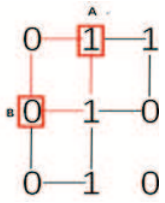


Figure 4: Rectangular area of the bitmap font

6) Traverse the two-dimensional smooth region, find all the points in the red rectangular region, project these points back into the three-dimensional space, and embed the watermark intensity, h, to the normal vectors of these points. A new coordinate is generated based on the embedding intensity by Formula (5).

$$\begin{cases} x'_i = x_i - \frac{h\vec{n}_{x_i}}{\sqrt{\vec{n}^2_{x_i}+\vec{n}^2_{y_i}+\vec{n}^2_{z_i}}} \\ y'_i = y_i - \frac{h\vec{n}_{y_i}}{\sqrt{\vec{n}^2_{x_i}+\vec{n}^2_{y_i}+\vec{n}^2_{z_i}}} \\ z'_i = z_i - \frac{h\vec{n}_{z_i}}{\sqrt{\vec{n}^2_{x_i}+\vec{n}^2_{y_i}+\vec{n}^2_{z_i}}} \end{cases}, \tag{5}$$

where $R_i(x_i, y_i, z_i)$ is the three-dimensional vertex after back projection, $\vec{n}_{R_i}(\vec{n}_{x_i}, \vec{n}_{y_i}, \vec{n}_{z_i})$ is the normal vector of the three-dimensional vertices, and x'_i, y'_i, z'_i is the coordinate value of the three-dimensional vertex after embedding the watermark.

3 Experiments and Analyses of the Results

In this section, we conduct three groups of experiments to evaluate the visibility and robustness of our proposed algorithm. The experiments were developed on the Visual Studio 2012 development platform, and they used the OpenGL library display 3D models. The format of a 3D model is an OFF file, with three 3D models, *i.e.*, Bunny, Venus, and Rabbit, as shown in Figure 5.

Since there are no standards that can evaluate the performances of visible watermarks, in this paper, we used the number of changed vertices in the smoothed area to evaluate the effect of embedding the visible watermark. Table 1 shows the number of vertices, the number of triangular faces, and number of changed vertices in the smooth area and the ratio of vertices to the changed vertices for the three models. Table 1 shows that the number of vertices that must be modified in the embedding models was less than 2% of the vertices of the original model and the number of triangular faces. Therefore, the watermarking algorithm proposed in this paper requires very little modification of the original model, and it will not affect the normal use of the model.

3.1 The Evaluation of a Visible Watermark in the 3D Model

Figure 6 shows the effect of embedding the watermark with the mixed numbers and English characters, "KD 3D", on three different models, an Figure 7 shows the effect on three different models of embedding the watermark with the Chinese character for "electricity." Figure 8 shows the effect of embedding the watermark with the Chinese characters and the English characters on three different models after 3D-printing. Figure 9 shows the effect of embedding the watermark with the trademark on the Rabbit model. Watermark information was clearly and completely displayed on these models after embedding the watermark.

3.2 The Evaluation of the Robustness to Attack

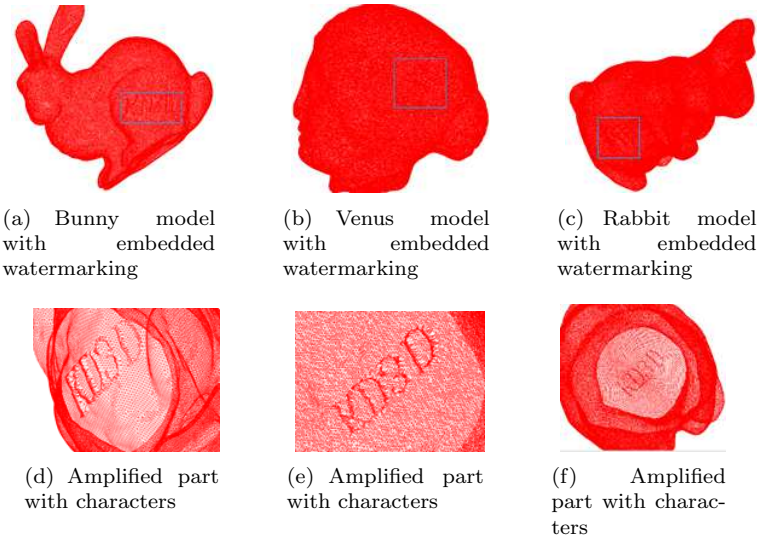
The proposed method is based on mesh subdivision, hence, when the watermarked model is subjected to an attack that only changes the coordinate position of the vertices in the model without changing the topology of the model, the model can resist the corresponding attack effectively. Therefore, the proposed algorithm is robust to common attacks, such as translation, rotation, scaling, smoothing, and noise. The results of the attacked Bunny models are listed in Figures 10 and 11.

(a) Bunny model (b) Venus model (c) Rabbit model

Figure 5: Original models used in the experiment

Table 1: Three models

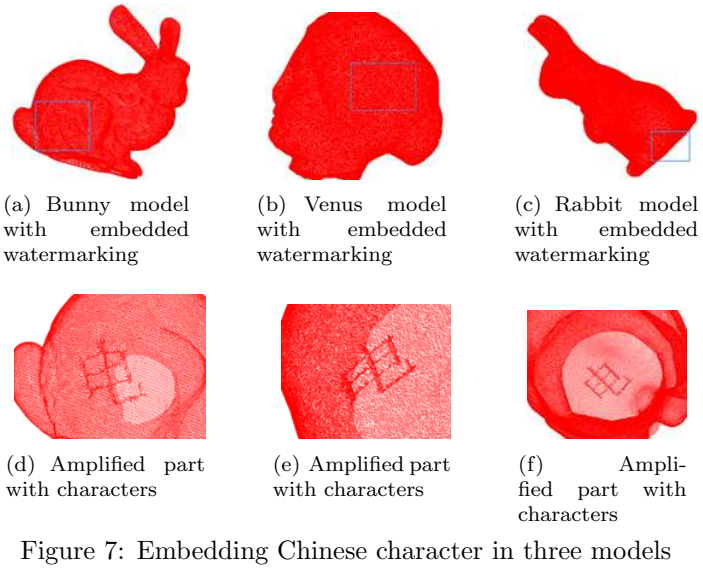
Model	Number of vertices	Number of triangular faces	Number of changed vertices in smooth area	Number of changed vertices in smooth area / Number of vertices
Bunny	34835	69666	587	1.69%
Venus	100759	201514	426	0.42%
Rabbit	70658	141312	564	0.80%



(a) Bunny model with embedded watermarking (b) Venus model with embedded watermarking (c) Rabbit model with embedded watermarking

(d) Amplified part with characters (e) Amplified part with characters (f) Amplified part with characters

Figure 6: Embedding English characters in three models



(a) Bunny model with embedded watermarking (b) Venus model with embedded watermarking (c) Rabbit model with embedded watermarking

(d) Amplified part with characters (e) Amplified part with characters (f) Amplified part with characters

Figure 7: Embedding Chinese character in three models

(a) English watermark printing result of Bunny model

(b) English watermark printing result of Venus model

(c) English watermark printing result of Rabbit model

(d) Chinese watermark printing result of Bunny model

(e) Chinese watermark printing result of Venus model

(f) Chinese watermark printing result of Rabbit model

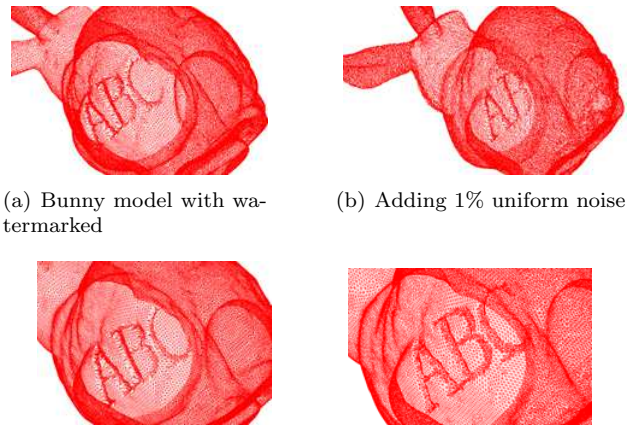
Figure 8: Embedding watermarking in three models after 3D-Printing

(a) Trademark image

(b) Trademark in Rabbit model

(c) Trademark printing result of Rabbit model

Figure 9: Embedding trademark in Rabbit model after 3D-Printing



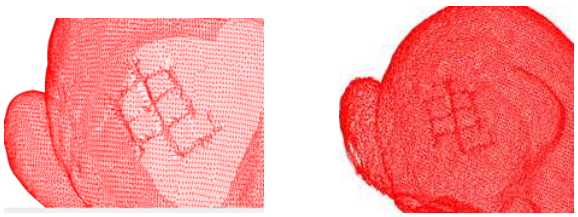
(a) Bunny model with watermarked

(b) Adding 1% uniform noise

(c) Smoothing with iteration of 50

(d) Three times subdivisions

Figure 10: The performances of embedded English watermark model under attacks



(a) Bunny model with watermarked

(b) Adding 1% uniform noise

(c) Smoothing with iteration of 50

(d) Three times subdivisions

Figure 11: The performances of embedded Chinese watermark model under attacks

4 Conclusions

In this paper, we proposed a visible 3D model watermark embedding algorithm based on the bitmap font. The algorithm implements a visible watermark by modifying the vertices of the smooth region of the 3D model according to the bitmap font. The experimental results showed that the proposed watermarking algorithm can retain the visible watermark in both the 3D mesh model and after 3D-printing. In addition, the algorithm is robust to common attacks, such as geometric transformation, noise, smooth, and subdivision. However, the algorithm proposed in this paper does not deal with the boundary of watermark information very smoothly, and it has certain influence on the appearance of the model. These issues will be addressed in future research.

Acknowledgments

This study was supported by the Shanxi Natural Science Foundation under Grand (No.201801D121133, No.201801D121129), National Natural Science Foundation of China (No.61672373, No.61501315), Scientific and Technological Innovation Team of Shanxi Province (No.201705D131025), Key Innovation Team of Shanxi 1331 Project(2017015), Collaborative Innovation Center of Internet+ 3D Printing in Shanxi Province(201708). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] X. C. An, R. Ni, and Y. Zhao, "Visible watermarking for 3D models based on boundary adaptation and mesh subdivision," *Journal of Applied Sciences*, vol. 34, no. 5, pp. 503–514, 2016.

[2] A. G. Bors and M. Luo, "Optimized 3D watermarking for minimal surface distortion," *IEEE Transactions on Image Processing*, vol. 22, no. 5, pp. 1822–1835, 2013.

[3] C. Chang, K. F. Hwang, and M. S. Hwang, "A feature-oriented copyright owner proving technique for still images," *International Journal of Software Engineering and Knowledge Engineering*, vol. 12, no. 3, pp. 317–330, 2002.

[4] C. Chang, K. F. Hwang, and M. S. Hwang, "A robust authentication scheme for protecting copyrights of images and graphics," *International Journal of Software Engineering and Knowledge IEE Proceedings Vision, Image and Signal Processing*, vol. 149, no. 1, pp. 43–50, 2002.

[5] J. W. Cho, R. Prost, and H. Y. Jung, "An oblivious watermarking for 3D polygonal meshes using distribution of vertex norms," *IEEE Transactions on Signal Processing*, vol. 55, no. 1, pp. 142–155, 2007.

[6] S. Kanai, H. Date, and T. Kishinami, "Digital watermarking for 3D polygons using multi-resolution wavelet decomposition," in *Proceedings of the 6th IFIP WG 5.2 International Workshop on Geometric Modeling: Fundamentals and Applications (GEO)-6*, pp. 296–307, 1998.

[7] K. Kim, M. Barni, and H. Z. Tan, "Roughness-adaptive 3D watermarking based on masking effect of surface roughness," *IEEE Trans. on Information Forensics and Security*, vol. 5, no. 4, pp. 721–733, 2010.

[8] L. Li, H. k. Li, W. Q. Yuan, J. F. Lu, X. Q. Feng, and C. C. Chang, "A watermarking mechanism with high capacity for three-dimensional mesh objects using integer planning," *IEEE MultiMedia*, vol. 25, no. 3, pp. 49–64, 2018.

[9] L. Li, Z. G Pan, and D. Zhang, "A public mesh watermarking algorithm based on the addition property of the fourier transform," in *Third International*

Conference on Image and Graphics (ICIG'04), 2004. DOI: 10.1109/ICIG.2004.22.

[10] C. Lu, C. Q. Zhu, and Y. H. Wang, "Visible watermarking for three-dimensional mesh model in two views," *Journal of Image and Graphics*, vol. 19, no. 7, pp. 1068–1073, 2014.

[11] A. M. Molaei, H. Ebrahimnezhad, and M. H. Sedaaghi, "Robust and blind 3D mesh watermarking in spatial domain based on faces categorization and sorting," *3D Research*, vol. 7, no. 2, pp. 1–18, 2016.

[12] R. Ohbuchi, H. Masuda, and N. Aono, "Watermarking three-dimensional polygonal models," in *Proceedings of the ACM International Multimedia Conference & Exhibition*, pp. 261–272, 1997.

[13] E. Prawn, H. Hoppe, and A. Finkelstein, "Robust mesh watermarking," in *Proceedings of the 26th annual conference on Computer graphics and interactive techniques*, pp. 49–56, 1999.

[14] M. M. Soliman, A. E. Hassanien, and H. M. Onsi, "A robust 3D mesh watermarking approach using genetic algorithms," *Advances in Intelligent Systems and Computing*, vol. 323, pp. 731–741, 2015.

[15] Y. P. Wang and S. M. Hu, "A new watermarking method for 3D models based on integral invariants," *IEEE Transactions on Visualization and Computer Graphics*, vol. 15, no. 2, pp. 285–294, 2009.

[16] Y. Yang, R. Pintus, H. Rushmeier, and I. Ivrissimtzis, "A 3D steganalytic algorithm and steganalysis-resistant watermarking," *IEEE Transactions on Visualization and Computer Graphics*, vol. 23, no. 2, pp. 1002–1013, 2016.

[17] Z. Q. Yu, H. H. S. Ip, and L. F. Kwok, "A robust watermarking scheme for 3D triangular mesh models," *Pattern Recognition*, vol. 36, no. 11, pp. 2603–2614, 2003.

[18] Y. Z. Zhan, Y. T. Li, X. Y. Wang, and Y. Qian, "A blind watermarking algorithm for 3D mesh models based on vertex curvature," *Journal of Zhejiang University Science C (Computers & Electronics)*, vol. 15, no. 5, pp. 351–362, 2014.

[19] J. M. Zhang, X. M. Zhou, and X. Y. Wang, "Transform domain-watermarking scheme of 3D models based on local feature points," *Journal of Image and Graphics*, vol. 19, no. 4, pp. 613–621, 2014.

Biography

Changchun Yan is a graduate student of Taiyuan University of Science and Technology. He is mainly engaged in the research of 3D watermarking.

Guoyou Zhang received his MEng in Computer Application Technology from Taiyuan University of Technology in 2003 and PhD in Control Theory and Engineering at Lanzhou University of Technology in 2013. His current research interest includes swarm intelligence and swarm robotics

Anhong Wang was born in Shanxi Province, P. R. China in 1972. She received the Ph. D. degree in the Institute of Information Science, Beijing Jiaotong University in 2009. She is now the director of Institute of Digital Media and Communication, Taiyuan University of Science and Technology. Her research interest includes image/video coding and secret image sharing.

Li Liu received her B.E. degree in communication engineering in 2002, from Lanzhou Railway University and M.E. degree in communication and information system in 2006, from Lanzhou Jiaotong University. Now, she is a Ph. D student in Northwestern Polytechnical University. Her current research interests include information hiding and secret sharing.

Chin-Chen Chang received his B.E. degree in applied mathematics in 1977 and the M.E. degree in computer and decision sciences in 1979, both from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph. D in computer engineering in 1982 from the National Chiao Tung University, Hsinchu, Taiwan. Since February 2005, he has been a Chair Professor of Feng Chia University. In addition, he has served as a consultant to several research institutes and government departments. His current research interests include database design, computer cryptography, image compression and data structures.

Analysis of Rear-End Collision Accident of Urban Traffic Based on Safety Pre-warning Algorithm

Sizhuo Wang, Wei Li, and Chunyu Kong
(Corresponding author: Chunyu Kong)

Guangdong Polytechnic Normal University
No. 293, West of Zhongshan Avenue, Tianhe District, Guangzhou, Guangdong 510665, China
(Email: ky43f0@yeah.net)

(Received July 28, 2019; Revised and Accepted June 6, 2020)

Abstract

With the increase of per capita car ownership, traffic accidents frequently occur, in which rear-end collision accounts for 30% to 40% of the total accidents; thus, rear-end collision has become the primary factor of traffic environment deterioration. Therefore, how to improve road traffic safety and reduce the probability of rear-end collision has become a primary social concern. In this study, based on the safety pre-warning algorithm, a vehicle collision model was built, and a vehicle anti-collision warning system was established. The calculation was performed based on the sample data to obtain the prediction value of vehicle collision time under different driving speeds to provide drivers with adequate response time and reduce the casualties and property losses caused by a vehicle collision. The experimental results showed that the pre-warning accuracy rate reached 80% when the speed was regarded as a variable. The simulation results showed that the early pre-warning or delayed pre-warning rate was very low. The timeliness rate reached 89%, enabling drivers to react quickly in the appropriate time and effectively reduces the risk of vehicle rear-end collision.

Keywords: Early Warning Algorithm; Rear-End Collision; Safe Collision Time

1 Introduction

With the increase in automobile production and ownership, traffic problems have become the city's fundamental problem. Rear-end collision accident is the most common traffic problem and the most significant loss problem. Due to the vehicle warning system's imperfection, drivers often can not respond the first time, resulting in the loss of life and property. Therefore, it is necessary to study the analysis and early warning of rear-end collision. Scholars at home and abroad have put forward their views on this.

Lee and Abdel-Aty [5] used the generalized estimation equation with a negative binomial link function to model the rear-end collision frequency at signalized intersections. They found that there was a high correlation between longitudinal or spatial related rear-end collisions. Hendricks *et al.* [4] applied the seven-step collision problem analysis method to the rear-end collision. They defined and explained the countermeasure action by the front end analysis of the rear-end crash. Based on the artificial immune mechanism, Yi *et al.* [6] put forward an early warning model to identify and determine the trend caused by abnormal vehicle state, which is a theoretical basis for the safe operation and management of highway tunnel group.

Huang *et al.* [2] studied and simulated the human body's dynamic response in the vehicle with rear-end collision and established the human body's nonlinear mathematical model and restraint system. They complied with the model's motion equation using the Kane equation and the multi-body dynamic analysis program developed by Houston. They found that the model was in good agreement.

This study used the vehicle speed based safety pre-warning algorithm. It simulated the effect of the anti-collision system through data calculation and simulation, especially the response to the early and late pre-warning triggered under the change of speed per hour, to quantify the impact of warning on collision safety benefit measures and ensure the accuracy and timeliness of the system.

2 Safety Pre-Warning System

2.1 Rear-end Collision

Rear-end collision is a kind of straight-line collision in the state of the car following. It refers to the situation that the head of one vehicle collides with another vehicle's tail [8], as shown in Figure 1.

$\angle 1$ is denoted as θ_1, and $\angle 2$ is denoted as θ_2. $\angle 1$ and $\angle 2$ represent the angle between the connecting line of the central coordinates of the front and rear vehicles and the vehicle's driving direction, respectively. ν_1 represents the rear vehicle's speed, ν_2 represents the front vehicle's speed, d represents the distance between the two vehicles'

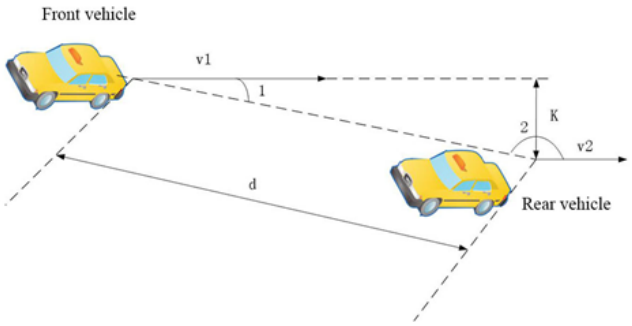


Figure 1: The schematic diagram of rear-end collision

central position, K refers to the transverse distance of the two vehicles.

Only when the transverse distance between the two vehicles is smaller than the car body's width, i.e., $K \geq |d \sin \theta_1|$, the rear-end collision between the two vehicles is possible. When $K \geq |d \sin \theta_1|$ is detected, the system needs to compare the time required for vehicle rear-end collision with time-to-collision (TTC) to determine whether there is a risk of rear-end collision. The rear-end collision of two vehicles can be active or passive. The time required for rear-end collision is assumed to be t. When rear-end collision occurs, i.e., the rear vehicle's speed exceeds that of the front vehicle, and when $\nu_1 > \nu_2$ and $|\theta_1| < |\theta_2|$ are met, the time required for rear-end collision is:

$$t = 3.6 \times |(d \times |\cos \theta_1| - 5)|/(\nu_1 - \nu_2).$$

2.2 Safety Anti-collision

TTC is the shortest time required for drivers to know the danger and react to avoid collision [15]. In driving, the calculation and processing module of the pre-warning system needs to calculate the reserved safety time in real-time according to the vehicle status data returned by the detection instrument; then, it can be compared with the time required for rear-end collision [14]. The smaller the TTC is, the greater the risk of rear-end collision is. The basic formula of TTC can be expressed as

$$TTC = \frac{d - L}{|V_{rear} - V_{front}|},$$

where L refers to the vehicle's length, and V_{front} and V_{rear} are the real-time speed of the front and rear vehicles, respectively.

Considering that the vehicle's acceleration is constant and the speed of the rear vehicle is higher than that of the front vehicle, then the acceleration of the front vehicle is expressed as a_{front}, and the acceleration of the rear vehicle is expressed as a_{rear}.

To simplify the calculation, let the relative speed between the front and rear vehicles ($|V_{rear} - V_{front}|$) be V_rel, let the relative acceleration ($|a_{rear} - a_{front}|$) be a_{rel}, let $TTC = t_0$, and the safe stopping distance is assumed to be s.

Considering the front-vehicle's real-time motion state, it is assumed that the front vehicle still has the speed when the rear-end collision accident occurs, i.e., $\Delta = V_{rel}^2 + 2a_{rel}d \geq 0$, the two vehicles may rear-end. Under this condition, when the front vehicle runs at a constant speed, i.e., $a_{front} = 0$, and $V_{front}t_0 + (d - s) > V_{rear}t_0 + \frac{1}{2}a_{rear}t_0^2$, the rear-end collision will not happen; when the rear vehicle continuously runs, i.e., $a_{rear} = 0$,

$$TTC = t_0 = \frac{d - s}{V_{rel}}.$$

When the rear vehicle has acceleration, i.e., $a_{rear} \neq 0$,

$$TTC = t_0 = \frac{-V_{rel} + \sqrt{V_{rel}^2 + 2a_{rear}(d - s)}}{a_{rear}}.$$

It is assumed that the front vehicle no longer has speed at the time of rear-end collision, i.e., the front vehicle completely stops it stops. When $(d - s) > V_{rea}t_0 + \frac{1}{2}a_{rear}t_0^2$ is satisfied, the collision will not happen when the rear vehicle runs constant, i.e., $a_{rear} = 0$,

$$TTC = t_0 = \frac{d - s}{V_{rear}}.$$

When the rear vehicle has accelerated, i.e., $a_{rear} \neq 0$,

$$TTC = t_0 = \frac{-V_{rear} + \sqrt{V_{rear}^2 + 2a_{rear}(d - s)}}{a_{rear}}.$$

2.3 Structure of the Pre-warning Algorithm

The comparison between the time of vehicle rear-end collision and TTC is showed that when TTC is smaller than the time required for rear-end collision, the collision will not occur.

On the contrary, when TTC is more extensive than or equal to the time required for rear-end collision, there is a risk of rear-end collision. Therefore, the pre-warning system should be connected with the detection equipment to transmit the vehicle's real-time information in the process of driving to the database, especially the speed of the vehicle and the distance and angle with the vehicle ahead [12]. The calculation module calculates the rear-end collision time and TTC, respectively, and transmits the judgment result to the processing center. If there is a risk, the driver shall be warned in time by sending out visual or auditory signals [1] to remind the driver to slow down; if the risk is removed, the signal is canceled. The structure of the pre-warning algorithm system is shown in Figure 2.

3 Experiment Model

3.1 Experimental Methods

The virtual rear-end collision experiment analysis and the construction of components, such as road network, vehi-

Table 1: Pretest results

	Group 1	Group 2	Group 3	Group 4	Group 5
Speed of the front vehicle (km/h)	30	40	52	59	42
Speed of the rear vehicle (km/h)	40	55	64	68	53
Acceleration of the front vehicle (km/)	6	6	7	6.5	7
Acceleration of the rear vehicle (m/)	8	6	8.5	7.5	9
Distance between two vehicles (m)	15	10	7	5	9
$\sin\theta_1$	$\sin 175$	$\sin 10$	$\sin 15$	$\sin 160$	$\sin 12$
$\cos\theta_1$	$\cos 175$	$\cos 10$	$\cos 15$	$\cos 160$	$\cos 12$
The time required for rear-end collision t(s)	1.26	1.75	0.79	0.5	4.45
TTC (s)	1	1.9	1.56	1.52	1.83
Rear-end collision hazard judgment	Safe	Danger	Danger	Danger	Safe
Whether the pre-warning alarm sounds	No	Yes	Yes	Yes	No

Note: 1 km/h = 0.28 m/s

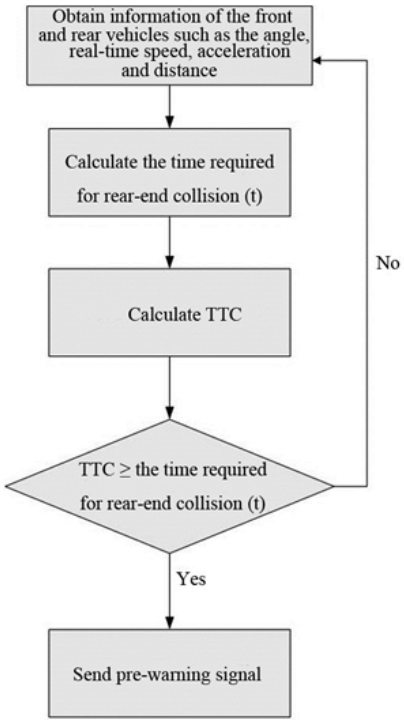


Figure 2: The working structure of the security pre-warning system

cle, and signal lamp, were realized by MATLAB computer simulation software [10]. The intersection was selected as the virtual center section, and the finite element model and Computer-Aided Design (CAD) model of the necessary vehicle parts were input [3].

SANTANA model was selected as the simulated vehicle as the alarm time of the model was relatively moderate. In constructing the internal security pre-warning system, VanetMobisim, the generation tool of moving node trajectory, was adopted to establish a V2V communication scene and compile the OTCL simulation script. After the vehicle simulation rear-end collision model was built, the calculation was performed by Pam-Crush software, and the result was output. Ten experienced drivers with little difference in driving years were recruited for manual assessment.

3.2 System Pretest

In the actual process, considering the cost, it is impossible to make the vehicle present the violent collision scene of a rear-end collision. Therefore, to ensure the experiment's scientificity, it is necessary to carry out a pretest on the pre-warning system. The length, width, and height of the vehicle body used in the experiment were 4.5 m, 2 m, and 1.7 m, respectively. All vehicles were under the same road condition.

The safe stopping distance of the vehicle was 3 m. Firstly, the rear-end collision time and TTC were calculated manually by the formula. Whether there was a risk of rear-end collision was determined based on the calculation result. Then, the pre-warning system's feasibility was detected by comparing it with the actual response of the pre-warning alarm. Five groups of data were randomly selected for the pretest. The test results are shown in Table 1.

In Table 2, the comparison of the time required for rear-end collision and TTC showed that the rear-end collision accidents in the first and fifth groups would not

Table 2: Simulation results of the accuracy of the security pre-warning algorithm

		Collision		No Collision	
Rear Vehicle	Front Vehicle	Pre-Warning	No Pre-Warning	Pre-Warning	No Pre-Warning
Low Speed	Low Speed	75	0	1	74
Moderate Speed	Moderate Speed	70	5	2	73
High Speed	High Speed	62	8	15	55
False Alarm Rate			11%		
Missing Alarm Rate			9%		
Accuracy Rate			80%		

occur, and the pre-warning system signal did not ring. However, in the 2^{nd}, 3^{rd} and 4^{th} group, $TTC > t$, the risk was assessed as dangerous, and the pre-warning system was required to prompt the driver to decelerate promptly and brake. All three alarms sounded. The alarm response was correct in the test of the five groups of data, which showed that the pre-warning system was feasible. After passing the pretest, the next experiment was carried out.

4 Experimental Results

4.1 Pre-warning Accuracy

The simulation vehicles were randomly divided into three groups, including low-speed, medium-speed, and high-speed groups, with five vehicles in each group. The vehicles were controlled to run at a low speed (10 $\sim$ 20 km/s), moderate speed (30 $\sim$ 40 km/s) and high speed (50 $\sim$ 60 km/s) respectively. When the two vehicles touched and the time when the pre-warning signal of the vehicle interior warning system sounded were observed and recorded.

The correct alarm and false alarm of the pre-warning system in the case of signal display and the correct avoidance and alarm failure in no signal display were recorded. Two different collision results of this experiment were set in the simulation system in advance. The collision group and the non-collision group were repeated five times under the same conditions, 75 times in each case, and finally, 150 times of pre-warning data were obtained in total. The simulation results of the accuracy of the safety pre-warning algorithm are shown in Table 2.

Note: the false alarm rate = the sum of pre-warning times in the case of no collision/total times; the missing alarm rate = the sum of the times of no pre-warning in the case of collision/total times; the accuracy rate = the sum of the times of pre-warning in the case of collision + the sum of the times of no pre-warning in the case of no collision/total times.

It was seen from Table 1 that the safety pre-warning algorithm system that took speed as the primary benchmark was accurate in predicting the risk of vehicles at a low speed, followed by vehicles at a moderate speed. Due to the large centrifugal force of the high-speed vehicle, the friction coefficient with the ground was relatively reduced. Thus the pre-warning algorithm had a large error, leading to the alarm in the case of no collision or no alarm in the high-speed group's case; the frequency of false alarm and missing alarm in the high-speed group was the highest. Also, the false alarm rate and missing alarm rate of vehicles at all speeds were controlled at a low level, 11% and 9%, respectively, and the accuracy rate of vehicles at the low speed was nearly 100%. The results showed that the safety system based on the pre-warning algorithm could accurately calculate and compare the difference between the rear-end collision time and TTC, judge the risk of rear-end collision at the first time, and feedback to the driver. The real-time reminding and controlling of the driving speed can significantly improve the safety of the driving process.

4.2 Timeliness Rate of Pre-warning

Under the same conditions of the simulation experiment on the accuracy of the safety pre-warning algorithm, ten real drivers were asked to evaluate the rear-end collision time of low speed, medium speed, and high-speed groups, respectively. The output module of the simulation system was controlled by the real drivers assigned to each group. According to their experience, the time required for rear-end collision was estimated. Then each driver submitted the demand for braking response in the simulation system according to their judgment.

The time of the braking reaction of the divers was recorded. Starting from the moment of the braking action, 0 $\sim$ 2 s was the pre-braking stage, 2 $\sim$ 4 s was the braking stage, and 4 6 s was the post-braking stage. The alarm of the pre-warning system before, during, and after braking was observed. To avoiding the influence of the individual driving inertia, the rotation system was adopted, and the test was repeated five times, 50 times each group. Finally, 150 groups of data were obtained. The timeliness rate of the safety pre-warning algorithm is shown in Table 3.

Note: early rate = the sum of times before braking/total times; delay rate = the sum of times after braking/total times; timeliness rate = the sum of times during braking/total times.

From Table 2, the vehicles at the low speed had the

Table 3: The timeliness rate of the security pre-warning algorithm

Front Vehicle	Rear Vehicle	Before Braking	During Braking	After Braking
Low Speed	Low Speed	0	50	0
Moderate Speed	Moderate Speed	2	45	3
High Speed	High Speed	4	37	8
Early Rate		4%		
Delay Rate		7%		
Timeliness Rate		89%		

lowest early and delay rates and the highest timeliness rate. The high-speed group had an apparent fluctuation of the safety pre-warning signal's appearance time before and after braking. The high-speed group's early and delayed alarm rates were 8% and 16%, respectively, which were twice as high as the average values. Moreover, the frequency of time deviation after braking was relatively high, i.e., the pre-warning system's decay rate was higher than the early rate. Overall, the safety pre-warning system maintained a timeliness rate of 89%, showed a high sensitivity in the rear-end accident judgment, and kept a good synchronization with the experienced drivers [13]. This study provides proof for the efficient analysis and timely feedback of the safety pre-warning algorithm and offers a more powerful guarantee for applying the safety pre-warning system to avoid vehicle rear-end collision.

5 Discussion

1) The driver should control the speed. It was seen from the experimental results of this study that the speed was the most direct and critical factor affecting the probability of rear-end collision [11]. The simulation experiment also verified that there was still a deviation in the accuracy rate and timeliness rate in high-speed driving even when the pre-warning system was used for preventing rear-end collision. Therefore, only when the driver controls the speed carefully can the problem be solved fundamentally.

2) The driver should regularly check whether the vehicle braking performance is good. If the braking performance deteriorates, the braking reaction will be slowed down. The braking duration will be shortened, which will shorten the time before the occurrence of rear-end collision accidents and more likely to cause traffic accidents [9].

3) The vehicle should keep a distance. According to the calculation results of the time required for rear-end collision, the smaller the distance between vehicles is, the less reaction time left for drivers is. Moreover, the close collision is more likely to increase the severity of the accident. When the speed is low, the distance with the front vehicle in the same lane should be appropriately shortened, but the minimum distance shall not be smaller than 50 m [7].

6 Conclusion

In this study, we focus on preventing urban rear-end collision accidents. This study has analyzed the influencing factors of rear-end collision accidents. We also proposed a safety pre-warning algorithm with running speed as the primary variable, established a safety pre-warning system, and verified the system's accuracy and timeliness in predicting the risk of rear-end collision accident simulation experiments. The results showed that:

1) Vehicle speed was an essential factor affecting the occurrence of rear-end collision;

2) The safety pre-warning algorithm based pre-warning system had strong feasibility for the analysis and judgment of rear-end collision accidents, which was manifested in high accuracy and high timeliness rate;

3) The application of the safety pre-warning algorithm has a good prospect in avoiding the rear-end collision accident in urban traffic, which is conducive to reduce the collision risk and ensure personal safety and traffic safety to the greatest extent.

References

[1] F. P. Chee, S. F. Angelo, A. Asmahani, J. Dayou, C. H. W. Jackson, "An intelligent safety warning and alert system (iswas) for automobile vehicle," *ASM Science Journal*, vol. 11, no. 3, pp. 7-17, 2018.

[2] S. C. Huang, "Analysis of a model to forecast thermal deformation of ball screw feed drive systems," *International Journal of Machine Tools & Manufacture*, vol. 35, no. 8, pp. 1099–1104, 1995.

[3] E. Jeong, C. Oh, G. Lee, H. Cho, "Safety impacts of intervehicle warning information systems for moving hazards in connected vehicle environments," *Transportation Research Record: Journal of the Transportation Research Board*, vol. 2424, no. 1, 2014.

[4] P. R. Knipling, D. L. Hendricks, J. S. Koziol, J. C. Allen, L. Tijerina, C. Wilson, "A front-end analysis of rear-end crashes," in *Proceedings of the IVHS America of Surface Transportation and the Information Age*, 1992.

[5] C. Lee, M. Abdel-Aty, "Comprehensive analysis of vehicle-pedestrian crashes at intersections in Florida," *Accident Analysis and Prevention*, vol. 37, no. 4, pp. 775–786, 2005.

[6] Y. Lei, C. Peng, L. Zeng, Q. Han, X. Liu, D. Chen, C. Du, "Experimental analysis of cluster-based multichannel mechanism for inter-vehicle safety warning message transmission," *Journal of Communications*, vol. 11, no. 1, pp. 33–41, 2016.

[7] K. Nagatani, S. Kiribayashi, R. Yajima, Y. Hada, T. Izu, A. Zeniya, H. Kanai, J. Minagawa, Y. Moriyama, "Micro-unmanned aerial vehicle-based volcano observation system for debris flow evacuation warning," *Journal of Field Robotics*, vol. 35, no. 8, pp. 1222-1241, 2018.

[8] O. Raddaoui, M. M. Ahmed, S. M. Gaweesh, "Assessment of the effectiveness of connected vehicle weather and work zone warnings in improving truck driver safety," *IATSS Research*, vol. 44, no. 3, pp. 230–237, 2020. 2020.

[9] P. Rahimian, E. E. O'Neal, S. Zhou, J. M. Plumert, J. K. Kearney, "Harnessing Vehicle-to-Pedestrian (V2P) communication technology: Sending traffic warnings to texting pedestrians," *Human Factors*, vol. 60, no. 6, 2018.

[10] H. Rakha, G. M. Fitch, M. Arafeh, M. Blanco, R. J. Hanowski, "Evaluation of safety benefits from a heavy-vehicle forward collision warning system," *Transportation Research Record: Journal of the Transportation Research Board*, vol. 2194, no. 1, 2010.

[11] W. J. Song, Y. Yang, M. Fu, F. Qiu, M. Wang, "Real-time obstacles detection and status classification for collision warning in a vehicle active safety system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 3, pp. 758–773, 2018.

[12] Z. Y. Song, H. Jin, D. Ling, "Design of in-vehicle safety monitoring and remote warning system based on raspberry Pi," *Microcontrollers & Embedded Systems*, 2019.

[13] W. R. Townsend, *Connected Vehicle Traffic Safety System and a Method of Warning Drivers of a Wrong-Way Travel*, US Patents, US20180018877A1, 2018.

[14] Y. Wu, M. Abdel-Aty, J. Park, J. Z. Zhu, "Effects of connected-vehicle warning systems on rear-end crash avoidance behavior under fog conditions," *Transportation Research Part C: Emerging Technologies*, vol. 95,pp. 481–492, 2018.

[15] X. Zhang, M. M. Khan, "Vehicle driving safety technology based on IVP," in *Principles of Intelligent Automobiles*, pp. 17–109, 2019.

Biography

Sizhuo Wang, born in 1984, graduated from Northeast Forestry University. She was major in vehicle operation engineering. She is working in Guangdong Polytechnic Normal University as a lecturer. She is interested in vehicle-road collaborative vehicle safety experimental study.

Wei Li, born in 1989, graduated from Southwest Jiaotong University. She is a lecturer in Guangdong Polytechnic Normal University as a lecturer. She is interested in resident travel behavior.

Chunyu Kong, born in1980, graduated from Hunan University. She is an associate professor in Guangdong Polytechnic Normal University as a lecturer. She is interested in vehicle safety.

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.