

Lecture Notes in Electrical Engineering 1127

Yonghong Zhang · Lianyong Qi · Qi Liu ·  
Guangqiang Yin · Xiaodong Liu *Editors*

# Proceedings of the 13th International Conference on Computer Engineering and Networks

Volume III

 Springer

## Series Editors

Leopoldo Angrisani, *Department of Electrical and Information Technologies Engineering, University of Napoli Federico II, Napoli, Italy*

Marco Arteaga, *Departament de Control y Robótica, Universidad Nacional Autónoma de México, Coyoacán, Mexico*

Samarjit Chakraborty, *Fakultät für Elektrotechnik und Informationstechnik, TU München, München, Germany*

Jiming Chen, *Zhejiang University, Hangzhou, Zhejiang, China*

Shanben Chen, *School of Materials Science and Engineering, Shanghai Jiao Tong University, Shanghai, China*

Tan Kay Chen, *Department of Electrical and Computer Engineering, National University of Singapore, Singapore, Singapore*

Rüdiger Dillmann, *University of Karlsruhe (TH) IAIM, Karlsruhe, Baden-Württemberg, Germany*

Haibin Duan, *Beijing University of Aeronautics and Astronautics, Beijing, China*

Gianluigi Ferrari, *Dipartimento di Ingegneria dell'Informazione, Sede Scientifica Università degli Studi di Parma, Parma, Italy*

Manuel Ferre, *Centre for Automation and Robotics CAR (UPM-CSIC), Universidad Politécnica de Madrid, Madrid, Spain*

Faryar Jabbari, *Department of Mechanical and Aerospace Engineering, University of California, Irvine, CA, USA*

Limin Jia, *State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing, China*

Janusz Kacprzyk, *Intelligent Systems Laboratory, Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland*

Alaa Khamis, *Department of Mechatronics Engineering, German University in Egypt El Tagamoa El Khames, New Cairo City, Egypt*

Torsten Kroeger, *Intrinsic Innovation, Mountain View, CA, USA*

Yong Li, *College of Electrical and Information Engineering, Hunan University, Changsha, Hunan, China*

Qilian Liang, *Department of Electrical Engineering, University of Texas at Arlington, Arlington, TX, USA*

Ferran Martín, *Departament d'Enginyeria Electrònica, Universitat Autònoma de Barcelona, Bellaterra, Barcelona, Spain*

Tan Cher Ming, *College of Engineering, Nanyang Technological University, Singapore, Singapore*

Wolfgang Minker, *Institute of Information Technology, University of Ulm, Ulm, Germany*

Pradeep Misra, *Department of Electrical Engineering, Wright State University, Dayton, OH, USA*

Subhas Mukhopadhyay, *School of Engineering, Macquarie University, Sydney, NSW, Australia*

Cun-Zheng Ning, *Department of Electrical Engineering, Arizona State University, Tempe, AZ, USA*

Toyoaki Nishida, *Department of Intelligence Science and Technology, Kyoto University, Kyoto, Japan*

Luca Oneto, *Department of Informatics, Bioengineering, Robotics and Systems Engineering, University of Genova, Genova, Genova, Italy*

Bijaya Ketan Panigrahi, *Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi, Delhi, India*

Federica Pascucci, *Department di Ingegneria, Università degli Studi Roma Tre, Roma, Italy*

Yong Qin, *State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing, China*

Gan Woon Seng, *School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, Singapore*

Joachim Speidel, *Institute of Telecommunications, University of Stuttgart, Stuttgart, Germany*

Germano Veiga, *FEUP Campus, INESC Porto, Porto, Portugal*

Haitao Wu, *Academy of Opto-electronics, Chinese Academy of Sciences, Haidian District Beijing, China*

Walter Zamboni, *Department of Computer Engineering, Electrical Engineering and Applied Mathematics, DIEM—Università degli studi di Salerno, Fisciano, Salerno, Italy*

Junjie James Zhang, *Charlotte, NC, USA*

Kay Chen Tan, *Department of Computing, Hong Kong Polytechnic University, Kowloon Tong, Hong Kong*

The book series *Lecture Notes in Electrical Engineering* (LNEE) publishes the latest developments in Electrical Engineering—quickly, informally and in high quality. While original research reported in proceedings and monographs has traditionally formed the core of LNEE, we also encourage authors to submit books devoted to supporting student education and professional training in the various fields and applications areas of electrical engineering. The series cover classical and emerging topics concerning:

- Communication Engineering, Information Theory and Networks
- Electronics Engineering and Microelectronics
- Signal, Image and Speech Processing
- Wireless and Mobile Communication
- Circuits and Systems
- Energy Systems, Power Electronics and Electrical Machines
- Electro-optical Engineering
- Instrumentation Engineering
- Avionics Engineering
- Control Systems
- Internet-of-Things and Cybersecurity
- Biomedical Devices, MEMS and NEMS

For general information about this book series, comments or suggestions, please contact [leontina.dicecco@springer.com](mailto:leontina.dicecco@springer.com).

To submit a proposal or request further information, please contact the Publishing Editor in your country:

### **China**

Jasmine Dou, Editor ([jasmine.dou@springer.com](mailto:jasmine.dou@springer.com))

### **India, Japan, Rest of Asia**

Swati Meherishi, Editorial Director ([Swati.Meherishi@springer.com](mailto:Swati.Meherishi@springer.com))

### **Southeast Asia, Australia, New Zealand**

Ramesh Nath Premnath, Editor ([ramesh.premnath@springernature.com](mailto:ramesh.premnath@springernature.com))

### **USA, Canada**

Michael Luby, Senior Editor ([michael.luby@springer.com](mailto:michael.luby@springer.com))

### **All other Countries**

Leontina Di Cecco, Senior Editor ([leontina.dicecco@springer.com](mailto:leontina.dicecco@springer.com))

**\*\* This series is indexed by EI Compindex and Scopus databases. \*\***


Yonghong Zhang · Lianyong Qi · Qi Liu ·  
Guangqiang Yin · Xiaodong Liu  
Editors

# Proceedings of the 13th International Conference on Computer Engineering and Networks

Volume III

*Editors*

Yonghong Zhang  
Wuxi University  
Wuxi, Jiangsu, China

Qi Liu   
School of Computer and Software  
Nanjing University of Information Science  
and Technology  
Nanjing, Jiangsu, China

Xiaodong Liu  
School of Computing  
Edinburgh Napier University  
Edinburgh, UK

Lianyong Qi  
College of Computer Science and Technology  
China University of Petroleum (East China)  
Qingdao, Shandong, China

Guangqiang Yin  
School of Information and Software  
Engineering  
University of Electronic Science  
and Technology of China  
Chengdu, China

ISSN 1876-1100                      ISSN 1876-1119 (electronic)  
Lecture Notes in Electrical Engineering  
ISBN 978-981-99-9246-1              ISBN 978-981-99-9247-8 (eBook)  
<https://doi.org/10.1007/978-981-99-9247-8>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2024

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd. The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Paper in this product is recyclable.

# Preface

This conference proceeding is a collection of the papers accepted by the CENet 2023—the 13th International Conference on Computer Engineering and Networks held on November 3–5, 2023 in Wuxi, China.

This proceeding contains three volumes and covers four main topics: Internet of Things and Smart Systems (43 papers); Artificial Intelligence and Applications (72 papers); Communication System Detection, Analysis and Application (14 papers); and Cloud Computing and Security (32 papers).

These parts serve as valuable references for industry practitioners, university faculties, research fellows, graduate students, and undergraduates seeking to stay abreast of the latest advancements and state-of-the-art practices in the respective fields covered by the conference proceedings. Utilizing this resource will enable them to develop, maintain, and manage systems with a high level of reliability and complexity.

We extend our gratitude to the authors for their outstanding contributions and dedication, as well as to the reviewers for ensuring the selection of high-quality papers, which made this conference proceeding possible.

# Contents

Locally Verifiable Aggregate Signature Scheme for Health Monitoring Systems .....	1
<i>Ruolan Duan, Yun Song, and Xinli Gan</i>	
A Multidimensional Detection Model of Android Malicious Applications Based on Dynamic and Static Analysis .....	11
<i>Hao Zhang, Donglan Liu, Xin Liu, Lei Ma, Rui Wang, Fangzhe Zhang, Lili Sun, and Fuhui Zhao</i>	
Research on Eliminating Mismatched Feature Points: A Review .....	22
<i>Dunhua Chen, Jiansheng Peng, and Qing Yang</i>	
Current Challenges in Federated Learning: A Review .....	32
<i>Jinsong Guo, Jiansheng Peng, and Fengbo Bao</i>	
Cloud-Network Resource Scheduling for ONAP-Based IDN .....	39
<i>Xiangning Li, Yuqian Cai, Ruotong Wu, and Jingyue Tian</i>	
Abnormal Transaction Node Detection on Bitcoin .....	53
<i>Yuhang Zhang, Yanjing Lu, and Mian Li</i>	
A Review of Visual SLAM Algorithms for Fusion of Point-Line Features .....	61
<i>Yong Qing and Haidong Yu</i>	
Prediction of Self-rated Health of Older Adults by Network Services Based on Agent Simulation and XGBoost Algorithm .....	68
<i>Yue Li, Xinyue Hu, Yang Li, Chengmeng Zhang, and Gong Chen</i>	
Research on Telecommuting Security Solution Based on Zero Trust Architecture .....	82
<i>Wanli Kou, Huaizhe Zhou, and Jia Du</i>	
RLOP: A Framework Design for Offset Prefetching Combined with Reinforcement Learning .....	90
<i>Yan Huang and Zhanyang Wang</i>	
A Compliance-Enhancing Approach to Separated Continuous Auditing of Intelligent Endpoints Security in War Potential Network Based on Location-Sensitive Hashing .....	100
<i>Hanrui Zhang, Chenrong Huang, and Andrew Lyu</i>	

Design and Implementation of an Embedded Streaming Terminal ..... 120  
*Yan Shen, Tai Qin, and Min Chen*

Digital Copyright Transaction Scheme Based on Blockchain Technology ..... 130  
*Yuan Gao, Jin Wen, Peidong Miao, and Zhiqiang Wang*

Research on Network Security Situation Assessment Method ..... 140  
*Yuan Gao, Jin Wen, Pu Chen, and Zhiqiang Wang*

Enhancement of IRS-Assisted Wireless Localization System in NLOS  
Conditions ..... 153  
*Boyu Liu, Xudong Wang, Feng Gao, Yanru Wang, Yuji Qiu, and Lei Feng*

Current Situation and Prospect of Multi-energy Complementary Tidal  
Power Station Under Dual Carbon Background ..... 163  
*Mingyang Sun and Hongwei Li*

Resource Security Management Mechanism Based on Dynamic Key  
and Blockchain in Network Slicing Environment ..... 173  
*Guoyi Zhang, Yang Cao, Huihong Luo, Hailong Zhu, Feifei Hu,  
and Xubin Lin*

A Secure and Efficient Access Control Mechanism for Network Slice  
Resources in Distributed Environment ..... 182  
*Guoyi Zhang, Hailong Zhu, Huihong Luo, Yang Cao, Feifei Hu,  
and Xubin Lin*

Multicast Wireless Resource Optimization for High-Precision Clock  
Synchronization Timing Service in 5G-TSN ..... 190  
*Yue Liu, Jizhao Lu, Yanru Wang, Hui Liu, Yalin Cao, and Lei Feng*

Accurate Close Contact Identification: A Solution Based on P-RAN, Fog  
Computing and Blockchain ..... 200  
*Meiling Dai, Yutong Wang, Zheng Zhang, Xiaohou Shi, and Shaojie Yang*

Trusted Reputation System for Heterogeneous Network Resource Sharing  
Based on Blockchain in IoT ..... 210  
*Jingwen Li, Meiling Dai, Yi Lu, and Shaojie Yang*

Multi-objective Reinforcement Learning Algorithm for Computing  
Offloading of Task-Dependent Workflows in 5G enabled Smart Grids ..... 220  
*Yongjie Li, Jizhao Lu, Huanpeng Hou, Wenge Wang, and Gongming Li*



Distributed Core Network Traffic Prediction Architecture Based on Vertical Federated Learning .....	230
<i>Pengyu Li, Chengwei Guo, Yanxia Xing, Yingji Shi, Lei Feng, and Fanqin Zhou</i>	
Design and Implementation of SRv6 Routing Module in Computing and Network Convergence Environment .....	238
<i>Jing Gao, Wenkuo Dong, Lei Feng, and Wenjing Li</i>	
Reliable and Efficient Routing Management Mechanism for Power Communication Network Based on Multi-party Cooperation .....	249
<i>Zhongmiao Kang, Donghai Huang, Yuben Bao, Peiming Zhang, and Jiewei Chen</i>	
Blockchain-Based Searchable Encryption Access Control Mechanism for the Internet of Things .....	258
<i>Mengyuan Li, Shaoyong Guo, Wengjing Li, Ao Xiong, Dong Wang, Da Li, and Feng Qi</i>	
TSN Traffic Scheduling and Route Planning Mechanism Based on Hybrid Genetic Algorithm .....	269
<i>Zelin Zheng, Qian Wu, Wei Lv, Qiang Gao, Junhong Weng, and Peng Lin</i>	
An DAG-Based Resource Allocation Mechanism of Federated Learning for New Power Systems .....	281
<i>Jiakai Hao, Guanghuai Zhao, Ming Jin, Yitao Xiao, Yuting Li, and Jiewei Chen</i>	
Reliable Data Interaction Scheme Based on Oblivious Transfer Technology in Smart Grid .....	293
<i>Pengzhan Sun, Feng Qi, Xingyu Chen, Xuesong Qiu, and Yinlin Ren</i>	
Research on FlexeE Network Routing Algorithm for High Traffic Services ....	304
<i>Ruilin Wang and Zhili Wang</i>	
Network Fault Lightweight Prediction Algorithm Based on Continuous Knowledge Distillation .....	316
<i>Wei Huang, Jie Huang, Chengwen Fan, and Yang Yang</i>	
Quality of Service Oriented Power Communication Network Test Mechanism .....	326
<i>Wandi Liang, Hongguang Yu, Huicong Fan, Shijia Zhu, Jianhua Zhao, Wenxiao Li, Fan Tang, and Caiyun Li</i>	

Service Slice Resource Allocation Algorithm Based on Node Capability  
in Power Communication Network ..... 335  
*Zhen Zheng, Detai Pan, Yunzhou Dong, Zhengdong Lin, and Peng Lin*

Evaluation of Activation Functions in Convolutional Neural Networks  
for Image Classification Based on Homomorphic Encryption ..... 343  
*Huixue Jia, Daomeng Cai, Zhilin Huo, Cong Wang, Shibin Zhang,  
Shujun Zhang, Xiaoyu Li, and Shan Yang*

An Efficient Data Reduction Method for DAG Blockchain ..... 356  
*Chengyao Zhang and Dongyan Huang*

A Compact Dual-Band Directional Button Antenna Based on Metamaterial  
Lens for New Power Services ..... 366  
*Wenge Wang, Jizhao Lu, Yongjie Li, Huanpeng Hou, and Dongjiao Xu*

Energy Efficiency Maximization for RIS-Aided Multi-user MISO Systems  
in Integrated Power Communication Networks ..... 374  
*Yuqing Feng, Yalin Chen, Yutong Ji, Cong Zhu, and Yu Tian*

Multi-path Transmission Strategy for Deterministic Networks ..... 383  
*Fei Zheng, Kelin Li, Zou Zhou, Yu Hu, and Longjie Chen*

SDN-Based Efficient Consortium Blockchain Network Architecture  
for Grid Information Authentication ..... 393  
*Tian Liu, Shuang Yang, Yu Yang, Kelin Yang, Bo Li, Cong Chao,  
and Bin Sun*

Snowflake Anonymous Network Traffic Identification ..... 402  
*Yuying Wang, Guilong Yang, Dawei Xu, Cheng Dai, Tianxin Chen,  
and Yunfan Yang*

Privacy Attacks and Defenses in Machine Learning: A Survey ..... 413  
*Wei Liu, Xun Han, and Meiling He*

Metaverse Security and Forensic Research ..... 423  
*Manxuan Wang, Guangjun Liang, Meng Li, and Siyi Cao*

A Survey of Security Vulnerabilities and Detection Methods for Smart  
Contracts ..... 436  
*Jingqi Zhang, Xin Zhang, Zhaojun Liu, Fa Fu, Jianyu Nie,  
Jianqiang Huang, and Thomas Dreibholz*

A Survey of Blockchain-Based Identity Anonymity Research ..... 447  
*Fa Fu, Gaoshang Lu, Jianqiang Huang, and Thomas Dreibholz*

Blockchain-Based Central Bank Digital Currencies: A Comprehensive Survey ..... 456  
*Shuo Chen, Zhiwei Liu, Xiang Xu, Haoyu Gao, Hong Lei, and Chao Liu*

A Survey on the Integration of Blockchain Smart Contracts and Natural Language Processing ..... 467  
*Zikai Song, Pengxu Shen, Chuan Liu, Chao Liu, Haoyu Gao, and Hong Lei*

**Author Index** ..... 479



# Locally Verifiable Aggregate Signature Scheme for Health Monitoring Systems

Ruolan Duan, Yun Song<sup>(✉)</sup>, and Xinli Gan

School of Computer Science, Shaanxi Normal University, Xi'an 710062, China  
songyun09@snnu.edu.cn

**Abstract.** Edge devices of health monitoring systems are constantly generating a large amount of data. Because each piece of data is accompanied by a signature to verify its authenticity, there is an urgent need to reduce the space occupied by the signatures. In this paper, we introduce a new health monitoring system model using locally verifiable aggregate signatures to meet the need. The locally verifiable aggregate signature can compress multiple signatures into a single aggregated signature and recover all the original signatures from the aggregation. It not only reduces the space for storing signatures but also reduces the authentication cost, especially for verifying the authenticity of a single piece of data. Based on the RSA signature proposed by Seo (Information Sciences 2020), we present a concrete locally verifiable aggregate signature scheme from the RSA assumption, instead of other strong assumptions. It is proven that our scheme is secure in the standard model.

**Keywords:** RSA signature · Aggregate signature · Authentication · Health monitoring systems

## 1 Introduction

In a health monitoring system, a variety of sensors are deployed to keep track of people's physical conditions and generate data that records various physiological parameters, such as body temperature, heart rate, and mobility. With these records, doctors can gain a deeper understanding of patients and make more accurate diagnoses. In particular, patients who are monitored in real time or frequently share monitoring data with their doctors need to upload their data to the servers of their medical service providers. This requires each patient to sign their data to ensure authenticity. However, every sensor of every patient generates a large amount of data every day, and if the data is transmitted to the medical server in real time, each piece of data will be bound to a signature, which will take up a lot of space of the medical server for storage.

To solve the problem, aggregate signatures are introduced into the health monitoring system. The medical server only needs to store one aggregate signature, and the doctor only needs to get one signature to verify to check the authenticity of all data. However, the verification requires all the data while the doctor may only review a certain type of data or a sample of data without the need to get all the data. Therefore, a locally verifiable

aggregate signature that can extract the specific signature from the aggregate signature is needed. When the doctor asks for some data, the medical server can extract its signatures and send back them, and the doctor only needs to check the data he wants. Recently, Goyal and Vaikuntanathan [1] proposed such a locally verifiable aggregate signature. Although their scheme only supports single-signer aggregation, it can still significantly reduce the waste of server storage resources.

Considering the limited resources of the monitoring devices, it is better to construct a signature scheme under the RSA assumption because of the high computational cost of bilinear pairings. Though [1] presented such a scheme, it relies on the strong RSA assumption. In 2019, Seo [2] proposed a short RSA signature scheme without random oracle heuristics or stronger assumptions, and his scheme reduces the required number of prime-number generations in the signing algorithm to be more efficient. Since the scheme is tag-based, which increases the signature size, it is recommended to set the tag as the output of a pseudorandom function by taking as input the corresponding message and publish the pseudorandom function key as a part of the verification key. Considering the above features, we decided to use this scheme as the regular signature scheme and construct our aggregate signature scheme based on it.

After analyzing the above issues, in this paper, we introduce the concept of the locally verifiable aggregate signature into the health monitoring system and propose our system model for practical medical scenarios. Based on [1, 2] and our system model, we construct a concrete locally verifiable aggregate signature scheme from the RSA assumption and prove its security in the standard model.

## 1.1 Related Work

The first aggregate signature scheme was introduced by Boneh et al. [3]. Given  $n$  signatures on  $n$  distinct messages from  $n$  different users, the scheme is able to aggregate all signatures into a single short signature, which will prove to the verifier that the  $n$  users have indeed signed their messages. To simplify the process of obtaining the public keys and certificates of all signers in the verification phase, identity-based aggregate signatures (IBAS) [4] and certificateless aggregate signatures (CL-AS) [5] were presented. Since [4] considers a synchronized setting, the scheme is also known as a synchronized aggregate signature, and based on it, Hohenberger and Waters [6] presented the synchronized aggregate signature from the RSA assumption, which is the first secure RSA-based signature scheme with full aggregation. Recently, Goyal and Vaikuntanathan [1] presented an RSA-based aggregate signature scheme with partial aggregation, which is locally verifiable. The locally verifiable aggregate signature allows that given an aggregate signature, the verifier can extract one of the signatures involved in the aggregation for verification without knowing all the messages.

In the eHealth scenario, a bunch of solutions using aggregate signatures have emerged. Kumar et al. [7] first introduced the CL-AS into healthcare wireless medical sensor networks (HWMSNs), but their scheme was pointed out as insecure and Wu et al. [8] improved the scheme. Gayathri et al. [9] proposed an efficient pairing-free CL-AS scheme and applied it to the HWMSNs. However, their scheme is insecure too. To solve this problem, a series of schemes were presented [10–13]. In addition, Gu et al. [14] combined the aggregate signature and linearly homomorphic signatures to serve

electronic healthcare systems. Their scheme can realize double data compression and resist the coalition attack. Chen et al. [15] devised a lightweight forward secure aggregate signature scheme that provides unforgeability and forward security to health records, and has excellent performance.

## 2 Preliminaries

**Notations.** Let  $\lambda$  denote the security parameter,  $l$  denote the number of signatures that are aggregated, PPT denote probabilistic polynomial-time, and  $s \xleftarrow{R} S$  denote randomly choosing an element  $s$  from a set  $S$ . For two integers  $a \leq b$ ,  $[a, b]$  denotes a set of consecutive integers between  $a$  and  $b$ , including  $a$  and  $b$ . For a probabilistic algorithm  $A$ ,  $A(x) \rightarrow y$  (or  $y \leftarrow A(x)$ ) denotes that  $A$  takes  $x$  as input and outputs  $y$ .

### 2.1 RSA Assumption [16]

Let  $\text{poly}(\lambda)$  be a poly-bounded function mapping  $\lambda$  to the bit length of the RSA modulus. Let  $N$  be the product of two  $\text{poly}(\lambda)/2$ -bit, distinct safe primes  $p, q$ , where  $p' = (p-1)/2$  and  $q' = (q-1)/2$  are still primes. Let  $e$  be a randomly chosen positive integer less than and relatively prime to  $\Phi(N) = (p-1)(q-1)$ . We say that the RSA assumption holds on  $N$  if for any PPT algorithm  $\mathcal{A}$  given a random  $y \in \mathbb{Z}_N^*$  and  $(N, e)$ , the probability computing  $z$  such that  $z^e \equiv y \pmod{N}$  is negligible in  $\lambda$ .

### 2.2 Shamir's Trick [17]

Given  $x, y \in \mathbb{Z}_N$  together with  $a, b \in \mathbb{Z}$  such that  $x^a = y^b \pmod{N}$  and  $\gcd(a, b) = 1$ , there is an efficient algorithm for computing  $z \in \mathbb{Z}_N$  such that  $z^a = y \pmod{N}$ .

### 2.3 Birthday Problem

For a fixed positive integer  $N$ ,  $q \leq \sqrt{2N}$  elements  $y_1, y_2, \dots, y_q$  are chosen uniformly and independently from a set of size  $N$ . The probability that there exist distinct  $i, j$  with  $y_i = y_j$  satisfies  $\Pr[\exists i, j, y_i = y_j] \geq 1 - e^{-q(q-1)/2N} \geq \frac{q(q-1)}{4N}$ .

### 2.4 Locally Verifiable Aggregate Signature

We briefly review the definition of locally verifiable (single-signer) aggregate signatures introduced by Goyal and Vaikuntanathan [1]. A locally verifiable aggregate signature scheme for message space  $\mathcal{M}$  consists of six algorithms:

- **Setup** ( $1^\lambda$ )  $\rightarrow (sk, vk)$ : The **Setup** algorithm takes as input the security parameter  $\lambda$ , and generates a signing-verification key pair  $(sk, vk)$ .
- **Sign** ( $sk, m_i$ )  $\rightarrow \sigma_i$ : The **Sign** algorithm takes as input a signing key  $sk$  and a message  $m_i \in \mathcal{M}$ , and outputs a signature  $\sigma_i$ .
- **Verify** ( $vk, m_i, \sigma_i$ )  $\rightarrow 0/1$ : The **Verify** algorithm takes as input a verification key  $vk$ , a message  $m_i$ , and a signature  $\sigma_i$ . It outputs 1 for acceptance or 0 for rejection.

- **Aggregate** ( $vk, \{(m_i, \sigma_i)\}_{i \in [1, l]}\} \rightarrow \hat{\sigma} / \perp$ : The **Aggregate** algorithm takes as input a verification key  $vk$  and a sequence of message-signature pairs  $\{(m_i, \sigma_i)\}_{i \in [1, l]}$ , and checks the validity of signatures. If every signature is valid, it computes an aggregate signature  $\hat{\sigma}$ , otherwise outputs an error symbol  $\perp$ .
- **AggVerify** ( $vk, \{m_i\}_{i \in [1, l]}, \hat{\sigma}$ )  $\rightarrow 0/1$ : The **AggVerify** algorithm takes as input a verification key  $vk$ , a sequence of messages  $\{m_i\}_{i \in [1, l]}$ , and an aggregate signature  $\hat{\sigma}$ . It outputs 1 for acceptance or 0 for rejection.
- **LocalOpen** ( $vk, \hat{\sigma}, \{m_i\}_{i \in [1, l]}, j \in [1, l]$ )  $\rightarrow \sigma_j / \perp$ : The **LocalOpen** algorithm takes as input a verification key  $vk$ , an aggregate signature  $\hat{\sigma}$ , a sequence of messages  $\{m_i\}_{i \in [1, l]}$  and an index  $j \in [1, l]$ . It outputs the signature  $\sigma_j$  corresponding to the message  $m_j$ , or an error symbol  $\perp$  when the signature cannot be gotten as expected.

**Correctness.** The correctness for locally verifiable aggregate signatures is threefold:

- Correctness of signing: **Verify** ( $vk, m_i, \mathbf{Sign}(sk, m_i)$ ) = 1.
- Correctness of aggregation:  
 $\mathbf{AggVerify}(vk, \{m_i\}_{i \in [1, l]}, \mathbf{Aggregate}(vk, \{(m_i, \mathbf{Sign}(sk, m_i))\}_{i \in [1, l]})) = 1$ .
- Correctness of **LocalOpen**:

$$\mathbf{LocalOpen}(vk, \mathbf{Aggregate}(vk, \{(m_i, \mathbf{Sign}(sk, m_i))\}_i), \{m_i\}_i, j) = \mathbf{Sign}(sk, m_j).$$

**Security.** A secure locally verifiable aggregate signature should satisfy the following two security notions:

Existentially unforgeable under an adaptive chosen-message attack (EU-CMA). We say that a signature scheme is EU-CMA secure if for any PPT adversary  $\mathcal{A}$  in the following experiment, the advantage  $\text{Adv}_{\mathcal{A}}^{\text{EU-CMA}}$  is negligible.

$$\text{Adv}_{\mathcal{A}}^{\text{EU-CMA}} = \Pr \left[ \mathbf{Verify}(vk, m^*, \sigma^*) = 1 : \begin{array}{l} (sk, vk) \leftarrow \mathbf{Setup}(1^\lambda), \\ (m^*, \sigma^*) \leftarrow \mathcal{A}^{\mathbf{Sign}(sk, \cdot)}(1^\lambda, vk) \end{array} \right],$$

where  $m^*$  must not have been queried to the **Sign** oracle.

Aggregated unforgeability (AU). We say that a single-signer aggregate signature scheme has aggregated unforgeability if for any PPT adversary  $\mathcal{A}$  in the following experiment, the advantage  $\text{Adv}_{\mathcal{A}}^{\text{AU}}$  is negligible.

$$\text{Adv}_{\mathcal{A}}^{\text{AU}} = \Pr \left[ \mathbf{AggVerify}(vk, \{m_i^*\}_{i \in [1, l]}, \hat{\sigma}^*) = 1 : \begin{array}{l} (sk, vk) \leftarrow \mathbf{Setup}(1^\lambda), \\ (\{m_i^*\}_{i \in [1, l]}, \hat{\sigma}^*) \leftarrow \mathcal{A}^{\mathbf{Sign}(sk, \cdot)}(1^\lambda, vk) \end{array} \right],$$

where there exists  $i \in [1, l]$  such that  $m_i^*$  has not been queried to the **Sign** oracle.

Weak aggregated unforgeability. We say that an aggregate signature scheme has weak aggregated unforgeability if in the experiment of AU, the adversary  $\mathcal{A}$  is restricted to make all signing queries before receiving the verification key, and the relative advantage is negligible.

### 3 Construction

#### 3.1 System Model

As shown in Fig. 1, the system model consists of four main entities:

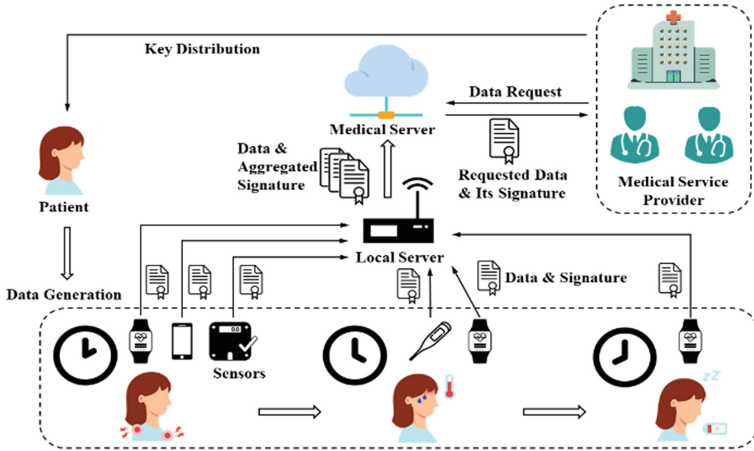


Fig. 1. System model

- Patient & sensors:** A patient gets her signing-verification key pair from a medical service provider when she first registers for the medical service. With the key pair, the patient can equip herself with a variety of sensors (e.g., smart watch, digital weighing scale) to monitor her physical condition and sign the records for uploading to the medical provider. Different sensors are used for monitoring in each time period, and each of these sensors signs its generated data using the key given by the patient and instantly transmits them to a nearby local server.
- Local server:** The local server (e.g., edge gateway) takes charge of all data and corresponding signatures generated by the sensors. Once the local server has collected a certain amount of data, it aggregates their signatures and then packages the aggregated signature and data to the medical server specified by the medical service provider. Because the local server does not have the signing key, it can only verify the signatures and cannot forge one.
- Medical server:** The medical server manages all data and aggregated signatures from individual local servers and executes the medical service provider's commands. When it receives new data and signatures, the medical server checks the authenticity of the aggregated signature and detects the original signatures of the corresponding user and determines whether the aggregation can continue based on some artificial regulations; if so, the medical server aggregates them; if not, it stores the new incoming data and signatures directly. When it receives a new data request, the medical server finds the requested data, extracts its signature from the aggregated signature, and sends them to the service provider.



- **Medical service provider:** When new patients register for the medical service, the provider distributes new key pairs to them. Afterward, the medical service provider will extract the monitoring data from the server for analysis and give medical advice and services to the patient. Before data analysis, it is necessary for the provider to verify the authenticity of every signature.

### 3.2 Our Scheme

**Setup:** The medical service provider chooses a poly( $\lambda$ )-bit RSA modulus  $N = pq$ , where  $2^{\frac{\text{poly}(\lambda)}{2}} \leq p, q \leq 2^{\frac{\text{poly}(\lambda)}{2}+1} - 1$ , and  $p, q, p' = (p-1)/2, q' = (q-1)/2$  are primes. To construct a hash function  $H : \{0, 1\}^* \rightarrow \{0, 1\}^{\text{poly}(\lambda)}$ , it chooses a random key  $k$  for the pseudorandom function (PRF)  $F_k : \{0, 1\}^* \rightarrow \{0, 1\}^{\text{poly}(\lambda)}$  and  $s \xleftarrow{R} \{0, 1\}^{\text{poly}(\lambda)}$ . Let  $H(\cdot) = F_k(\cdot || \mu) \oplus s$ , where  $\mu$  is the smallest positive integer satisfying that the XOR result is an odd prime. Finally, it chooses  $g_0, g_1 \xleftarrow{R} \mathbb{Z}_N^*$ , and distributes the signing key  $sk = (N, g_0, g_1, k, s, p, q)$  and the verification key  $vk = (N, g_0, g_1, k, s)$  to the patient.

**Sign:** For each  $m_i$ , the sensor first chooses a  $K$ -dimension tag vector  $t_i \xleftarrow{R} [0, \text{poly}(\lambda)]^K$  and  $K$  can be any function in  $\omega(1)$  (e.g.,  $K = \log \log \lambda$ ). For simplicity,  $t_i^{(j)}$  denotes the  $j$ th prefix of  $t_i$  ( $j \in [1, K]$ ), which is a  $j$ -dimension vector, and  $e_{ij}$  denotes the result of  $H(t_i^{(j)})$ . After determining the tag, the sensor computes  $e_{ij}$  and then checks whether  $e_{ij} | \Phi(N)$ . If so, it outputs  $p$  and  $q$ , otherwise computes the signature  $\sigma_i = (g_0 g_1^{m_i})^{\prod_j e_{ij}^{-1}} \bmod N$ , and sends it and the tag to the local server.

**Verify:** The verification passes iff  $\sigma_i^{\prod_j e_{ij}} = g_0 g_1^{m_i} \bmod N$ .

**Aggregate:** The server first checks the validity of the signatures. If invalid, then it outputs an error symbol  $\perp$ . If valid, then it computes the aggregate signature

$$\hat{\sigma} = \prod_i \sigma_i = \prod_i (g_0 g_1^{m_i})^{\prod_j e_{ij}^{-1}} \bmod N = g_0^{\sum_i \prod_j e_{ij}^{-1}} g_1^{\sum_i (m_i \prod_j e_{ij}^{-1})} \bmod N.$$

Note that to realize the local verification, we require only signatures whose corresponding first prefixes differ from each other can be aggregated.

**AggVerify:** The verification passes iff  $\hat{\sigma}^{\prod_i \prod_j e_{ij}} = \prod_i (g_0 g_1^{m_i})^{\prod_{h \neq i} \prod_j e_{hj}} \bmod N$ .

**LocalOpen:** To extract a single specific signature from the aggregate signature, the medical server first computes the following three terms.

$$e_{m \setminus m_r} = \prod_{i \neq r} \prod_j e_{ij}, u = \sum_{i \neq r} \prod_{h \neq \{i, r\}} \prod_j e_{hj}, v = \sum_{i \neq r} (m_i \prod_{h \neq \{i, r\}} \prod_j e_{hj}).$$

Note that since  $vk$  does not contain  $\Phi(N)$ , the three terms are computed as large integers without any modular reductions. Then the medical server computes

$$x = \hat{\sigma}^{e_{m \setminus m_r}} / (g_0^u g_1^v) \bmod N = (g_0 g_1^{m_r})^{\frac{\prod_{i \neq r} \prod_j e_{ij}}{\prod_j e_{rj}}} \bmod N,$$

and checks whether  $\gcd(\prod_{i \neq r} \prod_j e_{ij}, \prod_j e_{rj}) = 1$ . If so, it computes  $\sigma_r$  using the Shamir's trick as follows. If not, it outputs an error symbol  $\perp$ .

$$\sigma_r = \text{Shamir} \left( x, y = g_0 g_1^{m_r}, a = \prod_j e_{rj}, b = e_{m \setminus m_r} \right),$$

### Correctness.

- Correctness of signing:  $\sigma_i \prod_j e_{ij} = \left( (g_0 g_1^{m_i}) \prod_j e_{ij}^{-1} \right) \prod_j e_{ij} = g_0 g_1^{m_i} \bmod N$ .
- Correctness of aggregation:

$$\hat{\sigma} \prod_i \prod_j e_{ij} = g_0^{\sum_i \prod_{h \neq i} \prod_j e_{hj}} g_1^{\sum_i (m_i \prod_{h \neq i} \prod_j e_{hj})} = \prod_i (g_0 g_1^{m_i}) \prod_{h \neq i} \prod_j e_{hj} \bmod N.$$

- Correctness of **LocalOpen**: Recall that we require the first prefixes of the tags are different from each other in the **Aggregate** algorithm. Therefore,  $\gcd(a, b) = 1$ .

$$x^a = \left( (g_0 g_1^{m_r}) \frac{\prod_{i \neq r} \prod_j e_{ij}}{\prod_j e_{rj}} \right)^{\prod_j e_{rj}} = (g_0 g_1^{m_r})^{\prod_{i \neq r} \prod_j e_{ij}} = y^b,$$

$$\gcd(a, b) = \gcd\left(\prod_j e_{rj}, \prod_{i \neq r} \prod_j e_{ij}\right) = 1,$$

$$z^a = \left( (g_0 g_1^{m_r}) \prod_j e_{rj}^{-1} \right)^{\prod_j e_{rj}} = g_0 g_1^{m_r} = y.$$

## 4 Security Proof

Since the regular signature part of ours is a slight modification of [2], our EU-CMA security proof refers to the proof of [2] in the case where equal prefix does not exist.

**Theorem 1** *If the RSA assumption holds and  $F_k$  is a secure PRF, then our locally verifiable aggregate signature scheme has weak aggregated unforgeability.*

*Proof* Suppose  $\mathcal{A}$  is an adversary whose advantage in the weak aggregated unforgeability experiment is non-negligible. We construct a simulator algorithm  $\mathcal{B}$  that takes as input  $(N, e^*, y)$ , and aims to get  $z$  such that  $z^{e^*} \equiv y \bmod N$ .  $\mathcal{B}$  proceeds as follows.

**Setup:** Let  $[1, l^*]$  denote the set of tag indexes that the corresponding signatures are contained in the forged (challenge) aggregated signature and  $Q$  denote the set of tag indexes that the tags are queried by  $\mathcal{A}$ . First,  $\mathcal{A}$  sends its queries  $\{(m_i, t_i)\}_{i \in Q}$  to  $\mathcal{B}$ . If there are tags with the same first prefix, then  $\mathcal{B}$  aborts. Otherwise,  $\mathcal{B}$  chooses a random PRF key  $k$ , and guesses that  $t_{\text{guess}}$  is one of the prefixes of the challenge tag that has not been queried, i.e.,  $t_{\text{guess}} \in \{t_i^{(j)}\}_{i \in [1, l^*] \cap \bar{Q}, j \in [1, K]}$ . Then  $\mathcal{B}$  selects an appropriate  $\mu$ , and sets  $s = F_k(t_{\text{guess}} || \mu) \oplus e^*$ . If there exist  $i \in Q, j \in [1, K]$  such that  $H(t_i) = e^*$  and  $H(t_{\text{guess}}) \neq e^*$ , then  $\mathcal{B}$  aborts. We assume that the guess of  $\mathcal{B}$  is correct in the remainder of

the proof. Let  $\pi_Q$  denote  $\prod_{i \in Q} \prod_j e_{ij}$  and  $\pi_{l^*}$  denote  $\prod_{i \in [1, l^*]} \prod_j e_{ij}$ .  $\mathcal{B}$  picks  $\alpha, \beta \xleftarrow{R} \mathbb{Z}$  such that  $\alpha \neq \beta$ ,  $\gcd(\alpha, e^*) = 1$ ,  $\gcd(\beta, e^*) = 1$ , computes  $\mathbf{g}_0 = y^{\alpha\pi_Q}$ ,  $\mathbf{g}_1 = y^{\beta\pi_Q}$ , and sends  $vk = (N, \mathbf{g}_0, \mathbf{g}_1, k, s)$  to  $\mathcal{A}$ .

**Sign:**  $\mathcal{B}$  sends  $\mathcal{A}$  the answers of the **Sign** oracle

$$\sigma_i = y^{(\alpha + \beta m_i)\pi_Q} \prod_{j \in Q} \frac{1}{e_{ij}} = y^{(\alpha + \beta m_i) \prod_{h \neq i} \prod_j e_{hj}}, \quad i \in Q$$

**Extract from forgery:** After receiving the challenge messages, tags and the forged aggregated signature from  $\mathcal{A}$ ,  $\mathcal{B}$  checks the validity of the signature. If invalid,  $\mathcal{B}$  aborts. Otherwise, the forged signature  $\hat{\sigma}^*$  satisfies that

$$\begin{aligned} (\hat{\sigma}^*)^{\frac{\pi_{l^*}}{e^*}} &= \left( \prod_{i \in [1, l^*] \cap Q} \sigma_i \cdot \prod_{i \in [1, l^*] \cap \bar{Q}} \sigma_i \right)^{\frac{\pi_{l^*}}{e^*}} \\ &= y^{\left[ \alpha \left( \sum_{i \in [1, l^*] \cap Q} \prod_{h \neq i} \prod_j e_{hj} + \sum_{i \in [1, l^*] \cap \bar{Q}} \frac{\pi_Q}{\prod_j e_{ij}} \right) + \beta \left( \sum_{i \in [1, l^*] \cap Q} m_i \prod_{h \neq i} \prod_j e_{hj} + \sum_{i \in [1, l^*] \cap \bar{Q}} \frac{m_i \pi_Q}{\prod_j e_{ij}} \right) \right] \frac{\pi_{l^*}}{e^*}}, \\ &= \frac{(\hat{\sigma}^*)^{\frac{\pi_{l^*}}{e^*}}}{y^{\left( \alpha \sum_{i \in [1, l^*] \cap Q} \prod_{h \neq i} \prod_j e_{hj} + \beta \sum_{i \in [1, l^*] \cap \bar{Q}} m_i \prod_{h \neq i} \prod_j e_{hj} \right) \frac{\pi_{l^*}}{e^*}}} \\ &= y^{\left( \alpha \sum_{i \in [1, l^*] \cap \bar{Q}} \frac{\pi_Q}{\prod_j e_{ij}} + \beta \sum_{i \in [1, l^*] \cap \bar{Q}} \frac{m_i \pi_Q}{\prod_j e_{ij}} \right) \frac{\pi_{l^*}}{e^*}} \\ &= y^{\frac{\alpha \pi_Q}{e^*} \sum_{i \in [1, l^*] \cap \bar{Q}} \prod_{h \neq i} \prod_j e_{hj} + \frac{\beta \pi_Q}{e^*} \sum_{i \in [1, l^*] \cap \bar{Q}} m_i \prod_{h \neq i} \prod_j e_{ij}} \end{aligned}$$

Let the index of the tag that one of its prefixes is the same as  $t_{guess}$  be  $i^*$ . In other words,  $e^* \in \{e_{i^*j}\}_{j \in [1, K]}$ .

$$\begin{aligned} &y^{\frac{\alpha \pi_Q}{e^*} \sum_{i \in [1, l^*] \cap \bar{Q}} \prod_{h \neq i} \prod_j e_{hj} + \frac{\beta \pi_Q}{e^*} \sum_{i \in [1, l^*] \cap \bar{Q}} m_i \prod_{h \neq i} \prod_j e_{ij}} \\ &= y^{\alpha \pi_Q \sum_{i \in [1, l^*] \cap \bar{Q}, i \neq i^*} \left( \frac{\prod_j e_{i^*j}}{e^*} \prod_{h \neq i} \prod_j e_{hj} \right) + \beta \pi_Q \sum_{i \in [1, l^*] \cap \bar{Q}, i \neq i^*} \left( \frac{m_i \prod_j e_{i^*j}}{e^*} \prod_{h \neq i} \prod_j e_{hj} \right)} \\ &\quad \cdot y^{\frac{(\alpha + \beta m_{i^*}) \pi_Q}{e^*} \prod_{i \neq i^*} \prod_j e_{ij}}. \end{aligned}$$

Finally, if  $\gcd(m_{i^*}, e^*) = 1$ ,  $\mathcal{B}$  can extract the solution  $z$  using the Shamir's trick:

$$z = \text{Shamir} \left( x = y^{\frac{(\alpha + \beta m_{i^*}) \pi_Q}{e^*} \prod_{i \neq i^*} \prod_j e_{ij}}, y, a = e^*, b = (\alpha + \beta m_{i^*}) \pi_Q \prod_{i \neq i^*} \prod_j e_{ij} \right).$$

It is obvious that  $x^a = y^b$ . Since every  $e_{ij}$  is a unique prime,  $\gcd(\pi_Q, e^*) = 1$  and  $\gcd(\prod_{i \neq i^*} \prod_j e_{ij}, e^*) = 1$ . Recall that  $\gcd(\alpha, e^*) = 1$ ,  $\gcd(\beta, e^*) = 1$ , Therefore,  $\gcd(a, b) = 1$ . If  $\gcd(m_{i^*}, e^*) > 1$ ,  $\mathcal{B}$  aborts.

**Probability Analysis:** Let  $\mathcal{A}$ 's advantage in the above weak aggregated unforgeability experiment be  $\text{Adv}_{\mathcal{A}}^{\text{weak-AU}}$  (As we assumed in the beginning of the proof,  $\text{Adv}_{\mathcal{A}}^{\text{weak-AU}}$  is non-negligible). The following six events will cause  $\mathcal{B}$  to abort: 1.  $e^*$  is

not a prime with condition  $\log(e^*) \geq \frac{\text{poly}(\lambda)}{2}$ ; 2. There are tags with the same first prefix in  $\mathcal{A}$ 's query, i.e.,  $\exists i \neq j \in Q, t_i^{(1)} = t_j^{(1)}$ ; 3. The guess of  $\mathcal{B}$  is wrong; 4.  $H(t_{\text{guess}}) \neq e^*$ ; 5.  $\exists i \in Q, j \in [1, K], H(t_i^{(j)}) = e^*$ ; 6.  $\text{gcd}(m_{i^*}, e^*) > 1$ .

Let  $\Pr[E_i]$  denote the probability of event  $i$  occurring. The probability that  $\mathcal{B}$  successfully solves the RSA problem is equal to  $\text{Adv}_{\mathcal{A}}^{\text{weak-AU}} \cdot \prod_i \Pr[E_i]$ . The specific values and calculation processes of  $\Pr[E_1]$ ,  $\Pr[E_4]$ ,  $\Pr[E_5]$  and  $\Pr[E_6]$  can be found in [2]. The other probabilities are as follows. According to the birthday problem,

$$\Pr[E_2] \geq \frac{|Q|(|Q| - 1)}{4\text{poly}(\lambda)}, \Pr[E_3] = \frac{K}{\text{poly}(\lambda) - |Q|K}.$$

Since  $\mathcal{A}$  is a PPT adversary, the number of queries  $|Q|$  is polynomial, and  $\Pr[E_2]$  is non-negligible. And recall that  $K$  is a function in  $\omega(1)$ , so  $\Pr[E_3]$  is non-negligible.

Since the probabilities of all events are non-negligible, if  $\text{Adv}_{\mathcal{A}}^{\text{weak-AU}}$  is non-negligible, then  $\mathcal{B}$  can solve the RSA problem with non-negligible probability. ■

## 5 Conclusion

This paper focused on the problem that mountains of signatures are wasting server storage resources due to frequent data generation by edge devices (e.g., sensors) in the healthcare monitoring system, and proposed a new system model to solve it. In the system model, we implemented an aggregate signature scheme to compress multiple signatures into a single one to reduce storage, and the scheme can also extract one signature from the aggregated signature to verify, which makes the healthcare monitoring system more flexible. Based on the RSA assumption, our scheme is efficient and secure in the standard model.

## References

1. Goyal, R., Vaikuntanathan, V.: Locally verifiable signature and key aggregation. In: Dodis, Y., Shrimpton, T. (eds.) CRYPTO 2022, LNCS, vol. 13508, pp. 761–791. Springer, Cham (2022)
2. Seo, J.H.: Efficient digital signatures from RSA without random oracles. *Inf. Sci.* **512**, 471–480 (2020)
3. Boneh, D., Gentry, C., Lynn, B., et al.: Aggregate and verifiably encrypted signatures from bilinear maps. In: Biham, E. (eds.) EUROCRYPT 2003, LNCS, vol. 2656, pp. 416–432. Springer, Berlin (2003)
4. Gentry, C., Ramzan, Z.: Identity-based aggregate signatures. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.) PKC 2006, LNCS, vol. 3958, pp. 257–273. Springer, Berlin (2006)
5. Gong, Z., Long, Y., Hong, X., et al.: Two certificateless aggregate signatures from bilinear maps. In: 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007), pp. 188–193. IEEE, Qingdao (2007)
6. Hohenberger, S., Waters, B.: Synchronized aggregate signatures from the RSA assumption J. In: Nielsen, Rijmen, V. (eds.) EUROCRYPT 2018, LNCS, vol. 10821, pp. 197–229. Springer, Cham (2018)

7. Kumar, P., Kumari, S., Sharma, V., et al.: A certificateless aggregate signature scheme for healthcare wireless sensor network. *Sustain. Comput.: Inf. Syst.* **18**, 80–89 (2018)
8. Wu, L., Xu, Z., He, D., et al.: New certificateless aggregate signature scheme for healthcare multimedia social network on cloud environment. In: *Security and Communication Networks 2018*, (2018)
9. Gayathri, N.B., Thumber, G., Kumar, P.R., et al.: Efficient and secure pairing-free certificateless aggregate signature scheme for healthcare wireless medical sensor networks. *IEEE Internet Things J.* **6**(5), 9064–9075 (2019)
10. Liu, J., Wang, L., Yu, Y.: Improved security of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks. *IEEE Internet Things J.* **7**(6), 5256–5266 (2020)
11. Zhan, Y., Wang, B., Lu, R.: Cryptanalysis and improvement of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks. *IEEE Internet Things J.* **8**(7), 5973–5984 (2020)
12. Qiao, Z., Yang, L., Zhou, Y., et al.: A novel construction of certificateless aggregate signature scheme for healthcare wireless medical sensor networks. *Comput. J.* (2022)
13. Zhou, L., Yin, X.: An improved pairing-free certificateless aggregate signature scheme for healthcare wireless medical sensor networks. *PLoS ONE* **17**(7), e0268484 (2022)
14. Gu, Y., Shen, L., Zhang, F., et al.: Provably secure linearly homomorphic aggregate signature scheme for electronic healthcare system. *Mathematics* **10**(15), 2588 (2022)
15. Chen, X., Xu, S., He, Y., et al.: LFS-AS: lightweight forward secure aggregate signature for e-health scenarios. In: *ICC 2022-IEEE International Conference on Communications*, pp. 1239–1244. IEEE, Seoul, Republic of Korea (2022)
16. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**(2), 120–126 (1978)
17. Shamir, A.: On the generation of cryptographically strong pseudorandom sequences. *ACM Trans. Comput. Syst. (TOCS)* **1**(1), 38–44 (1983)



# A Multidimensional Detection Model of Android Malicious Applications Based on Dynamic and Static Analysis

Hao Zhang<sup>1,2</sup>(✉), Donglan Liu<sup>1</sup>, Xin Liu<sup>1</sup>, Lei Ma<sup>1</sup>, Rui Wang<sup>1</sup>, Fangzhe Zhang<sup>1</sup>, Lili Sun<sup>1</sup>, and Fuhui Zhao<sup>1</sup>

<sup>1</sup> State Grid Shandong Electric Power Research Institute, Jinan, China

<sup>2</sup> Shandong Smart Grid Technology Innovation Center, Jinan, China  
zhanghao\_dky@163.com

**Abstract.** This paper presents an approach utilizing static and dynamic analysis techniques to identify malicious Android applications. We extract static features, such as certificate information, and monitor real-time behavior to capture application properties. Using machine learning, our approach accurately differentiate between benign and malicious applications. We introduce the concept of “Multi-dimensional features”, combining static and dynamic features into unique application fingerprints. This enables us to infer application families and target groups of related malware. Tested on a dataset of 8000 applications, our approach demonstrates high detection rates, low false positive and false negative rates. The results highlight the effectiveness of our comprehensive analysis in accurately identifying and mitigating Android malware threats.

**Keywords:** Android malware · Dynamic and static analysis · Multi-dimensional features

## 1 Introduction

The rise of smartphones and their portable, feature-rich nature has made Android the operating system of choice on over 85% of global devices [2]. However, the openness of the Android platform has led to a surge in malicious applications, resulting in security and performance issues. As the Android platform becomes more popular, the number and complexity of these harmful apps grow exponentially [7].

The multifaceted nature of these applications, covering malware types like spyware, adware, ransomware, and banking Trojans, and the ability of some to evade standard detection measures, adds to the complexity of the problem. Current techniques, such as signature-based detection and behavioral analysis, present limitations [9].

To better combat Android malware, we propose a more advanced and comprehensive approach. Our method integrates static and dynamic analysis, offering a detailed view of app behavior, and employs machine learning to classify

apps. This methodology greatly improves the detection of sophisticated Android malware.

By utilizing dynamic debugging, we gain real-time insights into the application’s behavior during execution, capturing activities like network interactions, file operations, and system calls. Complementing this, we extract static features from the applications, including certificate information, strings, and permission requests, helping indicate potentially malicious behavior.

Our method’s effectiveness has been proven by testing on a large dataset of over 8,000 malicious and benign apps, where it achieved a 96% detection rate, and false positive and false negative rates of 1%. Additionally, we identified “Multi-dimensional features” based on the patterns of permission requests made by malicious applications, improving the malware detection process.

**Contribution.** To summarize, we have made the following significant contributions:

- **Novel feature.** We innovate the malicious apps detection field by proposing “Multi-dimensional features” based on permission request patterns. This approach substantially boosts the efficiency in detecting and dealing with malicious apps.
- **Systematic Tool.** We present a ground-breaking method that merges dynamic debugging and static feature extraction. This approach enhances the precision and robustness of identifying malicious Android apps, which significantly refines current practices.
- **Experimental analysis.** We validate the efficacy of our novel method via comprehensive testing. The results affirm the method’s high precision and consistency, marking a noteworthy advance in combating malicious apps.

## 2 Background

### 2.1 Android Platform and Malware

Android, an open-source operating system developed by Google, is broadly used for mobile devices like smartphones and tablets [8]. The flexible and open-source attributes of Android make it a popular choice among both legitimate developers and malicious actors.

Malware encompasses various harmful or intrusive software types, including viruses, worms, Trojan horses, ransomware, and others, specifically designed to target Android devices [5]. They exploit system vulnerabilities, permissions, or user behavior in Android to execute harmful actions, causing issues ranging from annoying disruptions to serious damage such as data loss and privacy violation.

### 2.2 Machine Learning in Malware Detection

The limitations of traditional detection techniques have prompted the integration of machine learning in malware detection. Machine learning provides an automated way to learn from and make decisions based on data. By training a

model with labeled benign and malicious apps, the system can learn to classify unseen apps effectively.

Machine learning-based approaches typically involve feature extraction and model training, using features derived from both static and dynamic analysis, such as permissions, API calls, network interactions, and system calls. These features are then used to train the model for further classification of apps into benign or malicious categories [10]. However, the model’s performance heavily depends on the quality and variety of the features, which makes finding effective features crucial for malware detection.

### 3 Overview

This section elaborates on our systematic and iterative approach to combating Android malware. We discuss the challenges encountered during feature extraction, malicious application identification, and malware classification, which have simultaneously acted as catalysts for developing innovative solutions. Our strategies stem from an in-depth understanding of the Android platform, complex app behaviors, and the evolving landscape of Android malware.

We detail our multi-stage workflow for detecting and classifying Android malware, from initial app behavior analysis to nuanced identification and classification of threats. We highlight our robust identification mechanism utilizing semantic and user interface recognition and an innovative classification system designed to improve detection efficiency and provide insights into malware behaviors and origins. This comprehensive overview reflects our commitment to a safer Android ecosystem.

#### 3.1 Workflow Overview

In this section, we aim to provide a panoramic view of our comprehensive process, from initial feature extraction to final report generation. This sequential methodology encapsulates the exact steps we undertake to uncover and address the complex challenges Android malware poses. Each component of the workflow contributes to the robustness of our approach, working in synchrony to offer a superior malware detection and classification system, as shown in Fig. 1.

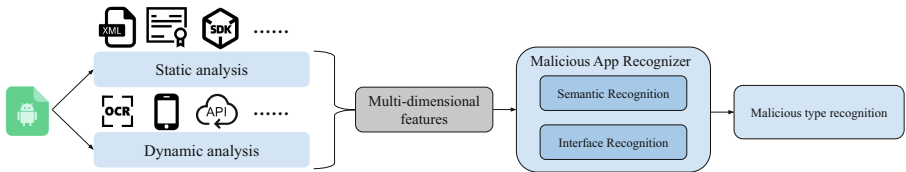


Fig. 1. Overview



Our methodology commences with Static Analysis, where we examine intrinsic properties of Android applications via the application package file (APK) contents, including Android manifest files, bytecode, and other embedded resources.

***Permission Extraction.*** We start with permission extraction, where applications’ requests for access to system resources or user data are scrutinized. We employ the AAPT tool to parse Android manifest files and accurately extract permission requests from the APK files, aiding in identifying potential malicious apps.

***Certificate Extraction.*** Certificate extraction forms a key part of our approach, validating the application and its developer’s authenticity. We use apk-tool to decompose APK files and inspect the application’s structural details. The analysis of certificates, especially from untrusted sources, can serve as red flags indicating potential security risks.

***String Extraction.*** The extraction of strings from the APK gives insight into the application’s purpose and behavior. We use a customized program based on the MobSF framework for this task. Analyzing extracted strings, including URLs, IP addresses, file paths, and hard-coded sensitive information, helps understand the application’s network communication patterns and potential malicious behavior.

### 3.2 Dynamic Analysis

In Dynamic Analysis, we observe applications’ real-time behavior in a secure environment. This process reveals potentially harmful actions that might be hidden in the static code. By logging detailed runtime data and cross-referencing it with the static analysis findings, we detect possible malicious activities.

***File Operations Monitoring.*** File Operations Monitoring is a crucial aspect of our dynamic analysis approach. It involves monitoring and analyzing file-related activities during the runtime of applications. By observing the interactions between an application and the file system, we can uncover potentially malicious actions that may not be evident through static code analysis alone.

***Function Monitoring.*** To augment our Android malware detection system, we use the Frida framework for application function monitoring. Frida allows us to inject additional code into the app and monitor its operations, thereby contributing to our understanding of its functionality and possible malicious behavior.

### 3.3 Malicious App Recognition and Classification

Our system integrates static and dynamic analyses, semantic recognition, and interface identification, with a key role played by our LSTM neural network model. This comprehensive approach enhances malware detection accuracy.

Once a malicious app is detected, our Malicious App Classifier categorizes it based on distinctive features and behaviors, aiding malware detection and countermeasure development. The Malicious Type Recognition component then categorizes the malicious app based on unique patterns and characteristics using an LSTM model.

## 4 Evaluation

In this section, we provide a comprehensive evaluation of our Android malware detection system, reviewing the static and dynamic analysis stages and the recognition stages for their accuracy and effectiveness.

*Dataset.* Our evaluation is based on a diverse dataset of 8000 applications sourced from VirusTotal and Google Play Store. This dataset comprises 60% benign and 40% malicious applications from various categories. This diverse selection enables comprehensive testing of our system’s performance across a broad range of application behaviors and malware types.

### 4.1 Static Analysis Evaluation

Static analysis forms the basis of our malware detection process, focusing on extracting key features such as permissions, certificate information, strings, SDKs, and shell fingerprints.

**Permission Extraction Evaluation** Permissions requested by an app provide insights into its functionalities and potential security risks. In our dataset, we observed a significant difference in the number and type of permissions requested by benign and malicious apps, as depicted in Table 1. Our permission extraction module successfully extracted permissions from 98.2% of the apps, signifying a robust and effective extraction process.

**Table 1.** Permission analysis

Permission type	Benign apps	Malicious apps
Sensitive permissions	5	11
Normal permissions	7	12
Signature permissions	3	6

**SDKs and Shell Fingerprint Recognition Evaluation** Our system effectively recognized SDKs in 95.6% of the apps and identified shell fingerprints in 94.3% of the apps, as illustrated in Table 2.

**Table 2.** Performance of SDKs and shell fingerprint recognition

Feature	Recognition success rate (%)
SDKs	95.6
Shell fingerprints	94.3

## 4.2 Dynamic Analysis Evaluation

**File Operations Monitoring** Monitoring file operations during dynamic analysis allows us to track the creation, modification, and deletion of files by the analyzed apps. Our system successfully monitored file operations in 95.8% of the apps, providing comprehensive visibility into their file-related activities.

Upon analyzing the dataset, we observed distinct differences between malicious and benign apps regarding file operations. Malicious apps exhibited a higher frequency of creating and modifying files than benign apps. This behavior raises concerns about the potential for unauthorized data manipulation, stealthy file-based attacks, or attempts to hide malicious payloads within the file system.

To illustrate the findings, consider the following sample comparison of file operations between malicious and benign apps:

App type	Average files created	Average files modified
Malicious	28	17
Benign	9	7

The data indicate that malicious apps tend to create and modify a significantly larger number of files compared to benign apps, as indicated by the higher averages. These findings suggest a higher likelihood of malicious intent or hidden activities within the file system.

**System Calls Monitoring** System calls monitoring enables us to gain insights into the low-level interactions between the analyzed apps and the underlying operating system. Our dynamic analysis module effectively monitored system calls, achieving a success rate of 97.2%, which allowed us to capture crucial runtime behavior details.

To illustrate the findings, consider the following sample comparison of system call frequencies between malicious and benign apps:

System call	Call frequency (per minute)
Malicious	-
open()	43.2
execve()	12.6
ioctl()	7.9
Benign	-
open()	8.4
execve()	2.1
ioctl()	1.3

Overall, our dynamic analysis module demonstrates its effectiveness in providing valuable insights into network interactions, file operations, and system calls of the analyzed apps. By monitoring these runtime behaviors, we can uncover potential malicious activities and enhance the security of app evaluation and detection processes.

### 4.3 Malicious App Recognition Evaluation

After the feature extraction phase, the extracted features are fed into our Semantic Recognizer and Interface. The results of the classification process are summarized in Table 3.

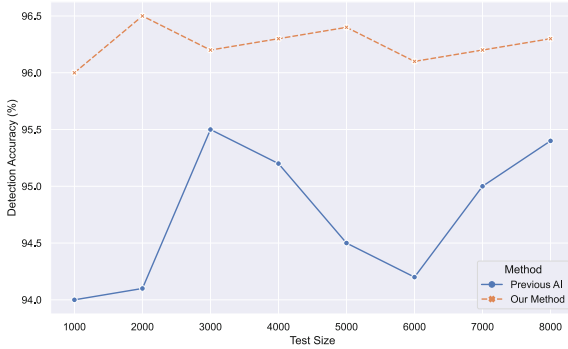
**Table 3.** Performance of semantic and interface recognizers

Recognizer	Accuracy (%)	False positive rate (%)	False negative rate (%)
Semantic recognizer	95.7	4.2	4.3
Interface recognizer	94.8	5.1	5.2

The results in Table 3 confirm the robustness and reliability of our recognizers in classifying the apps. While both recognizers exhibited high accuracy, we observed that the Semantic Recognizer had a slightly higher accuracy than the Interface Recognizer.

### 4.4 Comparison with Previous AI Method

In the ever-evolving field of Android malware detection, it is crucial to continually evaluate and benchmark new methods against existing ones to ensure their effectiveness and superiority. In line with this, we comprehensively compared our proposed method with a previously established AI method. This comparison aimed to provide a transparent and objective evaluation of our method's performance and its improvements over previous approaches. Figure 2 shows that our



**Fig. 2.** Comparison of detection accuracy over different test sizes

method consistently outperformed the previous AI method across all test sizes. Despite the increasing complexity and diversity of the test set, our method maintained a high detection accuracy of around 96%, significantly higher than the previous AI method. This result demonstrates the robustness and adaptability of our method, which can effectively handle a wide range of apps and maintain high performance.

#### 4.5 Malicious App Families

Based on our analysis using Multi-dimensional features, we have identified six distinct malicious app families. Understanding these families is crucial for developing targeted detection and prevention strategies. It is important to note that these families are determined based on the unique characteristics and behaviors observed in the Multi-dimensional features we have gathered. The following table summarizes the identified families and the number of apps associated with each family:

Malicious app family	Number of apps
com.xxx.sty	1204
com.xxx.mhfy	925
com.xxx.didi	280
com.xxx.pronha	175
com.xxx.Wose	365
com.xxx.ransom	155

These families represent different malicious behaviors found with the same developer in mobile apps. We can gain insights into their patterns and techniques by categorizing them, leading to more effective detection and prevention mechanisms.

## 5 Limitations and Future Work

*Limitations.* Despite its effectiveness, our system has certain limitations. The ever-evolving Android malware landscape presents new malicious techniques and obfuscation methods that could challenge our analysis methodologies. Dynamic analysis could be resource-intensive, potentially limiting scalability. Also, our classifier’s performance relies heavily on the quality and diversity of our training dataset. Insufficient representation of some malware types could reduce the detection rate for those categories.

*Future Work.* Despite these challenges, there are ample opportunities for future research and development. Developing a real-time system, implementing defenses against adversarial attacks, exploring privacy-preserving data analysis techniques, and creating an automated mechanism for classifier updates to accommodate emerging malware types are among the exciting prospects. By continuously evolving and improving, we aim to remain at the forefront of Android malware detection, contributing to a safer app ecosystem.

## 6 Related Work

*Detection of malicious mobile app.* A wealth of methodologies and tools for mobile software analysis have been proposed in previous works, encompassing both static and dynamic analysis approaches [1, 12]. These research endeavors have focused on a range of areas such as mobile app analysis, detection of malicious mobile software [6]. Specifically, the studies focusing on the analysis of malicious mobile adware [3, 4] have been instrumental in shaping our approach towards analyzing malicious apps of this nature. Our work continues in this trajectory, aiming to further expand the understanding of such harmful applications.

*Automation application test.* Our investigation draws from these technologies to explore the relatively uncharted territory of hacked mobile software analysis. Key elements of these previous works, such as workflow analysis of mobile software, identification of malicious mobile software, software vulnerability analysis, page layout recognition in software, and the use of automated testing tools, software vulnerability exploration [11]. all contribute to the foundation of our study.

## 7 Conclusion

In this study, we tackled the significant challenge of Android malware detection. We proposed and implemented an advanced Android malware detection system, combining static and dynamic analysis methods with semantic and interface identification. In addition, we introduced an advanced malicious type identification process, and we proposed the innovative concept of “Multi-dimensional features” based on permission request patterns. Our evaluation results, validated through widely accepted statistical measures such as Recognition Success Rate and False Positive and Negative Rates, demonstrate the robust performance of

our system in distinguishing between benign and malicious applications with high precision and accuracy. Furthermore, our classifier, trained on a diverse and up-to-date dataset, was able to categorize malicious applications into specific classes, enabling targeted response strategies. Finally, we successfully differentiated six malicious app families using the extracted “Multi-dimensional features”, demonstrating the practical utility of our proposed approach. This research represents a substantial stride forward in combating Android malware, contributing to a more secure Android app ecosystem and laying a robust foundation for future research and development in this domain.

**Acknowledgment.** This research is sponsored by the project of State Grid Shandong Electric Power Company Science and Technology Program, Project Name: Research on Key Technologies for Security Analysis of Mobile Applications for eIoT, ERP Number: 520626220019.

## References

1. Arzt, S., Rasthofer, S., Fritz, C., Bodden, E., Bartel, A., Klein, J., Le Traon, Y., Outeau, D., McDaniel, P.: Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps. *Acm Sigplan Notices* **49**(6), 259–269 (2014)
2. Chau, M., Reith, R.: Smartphone market share. IDC Corporate USA **444** (2020)
3. Crussell, J., Stevens, R., Chen, H.: Madfraud: Investigating ad fraud in android applications. In: *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services*, pp. 123–134 (2014)
4. Dong, F., Wang, H., Li, L., Guo, Y., Xu, G., Zhang, S.: How do mobile apps violate the behavioral policy of advertisement libraries? In: *Proceedings of the 19th International Workshop on Mobile Computing Systems and Applications*, pp. 75–80 (2018)
5. Dunham, K., Hartman, S., Quintans, M., Morales, J.A., Strazzere, T.: *Android Malware and Analysis*. CRC Press (2014)
6. Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D.: Android permissions: User attention, comprehension, and behavior. In: *Proceedings of the Eighth Symposium on Usable Privacy and Security*, pp. 1–14 (2012)
7. freebuf: 2023 global threat report. <https://www.freebuf.com/articles/paper/360177.html> (2023)
8. Google: Android. <https://www.android.com/> (2023)
9. Martinelli, F., Mercaldo, F., Saracino, A., Visaggio, C.A.: I find your behavior disturbing: Static and dynamic app behavioral analysis for detection of android malware. In: *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, pp. 129–136 (2016)
10. Souri, A., Rahmani, A.M., Jafari Navimipour, N.: Formal verification approaches in the web service composition: A comprehensive analysis of the current challenges for future research. *Int. J. Commun. Syst.* **31**(17), e3808 (2018)
11. Wang, L., He, R., Wang, H., Xia, P., Li, Y., Wu, L., Zhou, Y., Luo, X., Sui, Y., Guo, Y., et al.: Beyond the virus: A first look at coronavirus-themed mobile malware. arXiv preprint [arXiv:2005.14619](https://arxiv.org/abs/2005.14619) (2020)

12. Wei, F., Roy, S., Ou, X., et al.: Amandroid: A precise and general inter-component data flow analysis framework for security vetting of android apps. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 1329–1341. ACM (2014)





# Research on Eliminating Mismatched Feature Points: A Review

Dunhua Chen<sup>1</sup>, Jiansheng Peng<sup>1,2(✉)</sup>, and Qing Yang<sup>1</sup>

<sup>1</sup> College of Automation, Guangxi University of Science and Technology, Liuzhou 545000, China

sheng120410@163.com

<sup>2</sup> Department of Artificial Intelligence and Manufacturing, Hechi University, Hechi 547000, China

**Abstract.** The mismatch point elimination algorithm is a commonly used method in the field of computer vision and image processing to deal with the presence of mismatches or outliers in matched point pairs. These mismatch points may be caused by noise, occlusion, illumination changes or image distortion. In this paper, we first explain why there is a need to eliminate the mismatch points and the current state of research, and then introduce various types of feature points and describe the extraction methods of various feature points. Next, we review several methods of false match feature point elimination, such as geometric consistency verification-based methods, graph optimization-based methods, motion statistics-based methods, and learning-based methods, analyze their advantages and disadvantages as well as make comparisons, and give an outlook on future research directions. In the conclusion, we summarize the full paper and discuss the application trends of the mismatching feature point elimination algorithms. The purpose of this paper is to provide readers with a clearer and deeper understanding of false match feature point elimination algorithms, and hopefully give some reference significance to later researchers.

**Keywords:** ORB features · Mismatches · RANSAC · Machine learning

## 1 Introduction

In the field of computer vision and image processing, feature point matching is a key task used to implement several applications such as target tracking [1], object recognition [2], image stitching [3], and SLAM [4]. However, due to the influence of noise, occlusion, and illumination changes in images, the matching process often generates false match points, which reduces the accuracy and reliability of the algorithm, and in order to solve this problem, the false match point elimination algorithm is born. By Eliminate false match points, false tracking can be reduced, the quality of image stitching can be improved, the accuracy of pose estimation in SLAM systems can be improved, and the accuracy of tasks such as pose estimation and face recognition can be enhanced.

This paper first introduces the commonly used feature point extraction algorithms [5–7], and then classifies the false match point elimination techniques into four categories: methods based on geometric consistency verification, methods based on graph optimization, methods based on motion statistics, and methods based on learning. In this paper, we review the above four types of false match point detection methods and analyze various methods in terms of detection accuracy, computational speed, and robustness, pointing out the advantages, disadvantages, and applicability of each.

Despite the significant advantages of the false match point elimination algorithm in improving matching results, there are still some challenges and limitations. How to choose the appropriate threshold, model or parameters, and how to deal with noise and outliers in complex scenes are still challenges to be overcome. However, with the continuous advancement of technology and improvement of algorithms, the false match point elimination algorithm is expected to further improve the quality and reliability of image processing and bring more opportunities and challenges to various application areas.

## 2 Methods of Feature Point Extraction

### 2.1 SIFT Features

SIFT (Scale-Invariant Feature Transform) is a feature descriptor with scale invariance and illumination invariance, which is widely used in many computer vision tasks, such as image matching, object recognition and image stitching, etc. The main steps of the SIFT algorithm include:

- (1) Scale space extremum detection: at different scales, image pyramids are constructed by Gaussian filters [8], and then local extremum points are found on each scale space.
- (2) Key point localization: For each candidate polar point, the exact location of the key point is localized by computing a Gaussian difference image in scale space. The Hessian matrix is used to detect the extreme value points and exclude the points with low contrast and edge response.
- (3) Direction assignment: Assign a dominant direction to each key point to make the descriptor rotationally invariant. The gradient magnitude and direction histogram of the region around the key point are calculated, and the dominant direction is selected as the direction of the key point. The model values of the gradient  $m$  and direction  $\theta$  as in Eqs. 1 and 2:

$$m(x, y) = \sqrt{(L(x + 1, y) - L(x - 1, y))^2 + (L(x, y + 1) - L(x, y - 1))^2} \quad (1)$$

$$\theta(x, y) = \tan^{-1} \left( \frac{L(x, y + 1) - L(x, y - 1)}{L(x + 1, y) - L(x - 1, y)} \right) \quad (2)$$

- (4) Key point description: according to the scale and direction of the key point, a descriptor is constructed, i.e., this key point is described by a set of vectors. This descriptor includes not only the key point, but also the pixel points around the key point that contribute to it. The descriptor is used to represent the local image features around the keypoint.

### 2.2 SURF Features

Since the SIFT algorithm is more complex and slower to compute, SURF (Speeded Up Robust Features) was proposed to increase the computational speed and maintain better robustness. SURF algorithm is mostly the same as SIFT, SURF also uses a Gaussian filter to construct the image pyramid but uses a technique called Hessian matrix [9] to detect extreme value points in the image, and determines the location and scale of the feature points by computing the Hessian matrix of the image. The biggest difference is that the SURF algorithm uses a technique called accelerated integral image (integrated image) to compute feature descriptors for the region around the key points. Compared to the SIFT algorithm, the SURF algorithm greatly increases the computational speed by using integral image and other optimization techniques. It has better performance in some real-time applications.

### 2.3 ORB Features

ORB (Oriented FAST and Rotated BRIEF) combines the FAST corner point detector [10] and the BRIEF descriptor [11], and first uses the FAST corner point detector to quickly detect key points in the image. In the neighborhood around each keypoint, the ORB algorithm uses the BRIEF descriptor to describe the local features of the keypoints, as in Fig. 1.

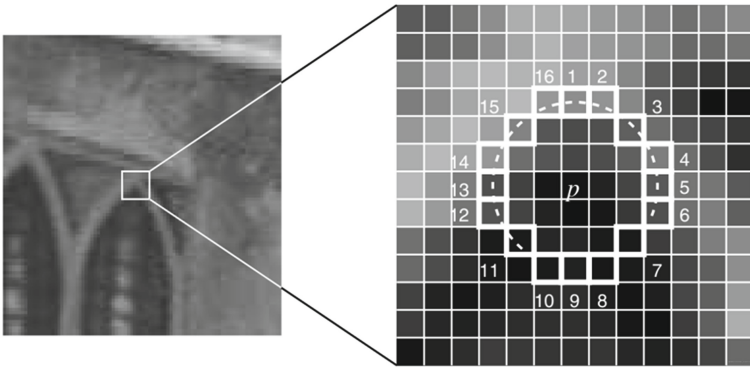


Fig. 1. ORB descriptor extraction

The ORB algorithm achieves high-speed feature extraction and matching with low computational complexity by using the FAST corner point detector and BRIEF descriptor, which is suitable for implementation on devices with limited computational resources.

## 3 Method of False Match Point Elimination

### 3.1 Method Based on Geometric Consistency Verification

Commonly used geometric consistency verification methods include RANSAC [12] (Random Sample Consensus) algorithm and PROSAC [13] (Progressive Sample Consensus) algorithm, RANSAC is a classical iterative random sampling algorithm, the basic idea is to randomly select the smallest sample set for model estimation and continuously optimizing the estimation results by iterative means. The RANSAC algorithm is used in ORB-SLAM3 proposed by Campos et al. [14]. The RANSAC algorithm eliminates the mis-matching points, and through the iterative process of RANSAC, ORB-SLAM3 can accurately estimate the camera motion and the location of map points, and eliminate those feature matching pairs that do not match the model, thus improving the accuracy and robustness of the SLAM system. Jiahui et al. [15] improved the RANSAC algorithm to reduce the number of iterations for matrix estimation by using the similarity of gray gradients around feature points to eliminate some of the mis-matching points in the initial matching, and reduced the mis-matching rate by quickly discarding the incorrect single-response matrix to reduce the interior point detection time.

PROSAC (Progressive Sample Consensus) is an improved RANSAC algorithm for estimating model parameters in datasets containing noise and outliers. PROSAC introduces an adaptive sampling strategy to better handle datasets with potential interior points and multiple models. Quanrong [16] used the Progressive Consistent Sampling (PROSAC) algorithm to replace the RANSAC algorithm to improve the ORB-SLAM2 system for fast feature point mismatch elimination. Traditional methods of false match point rejection based on geometric consistency verification usually require manual adjustment of parameters; the future trend is to optimize parameters by adaptive means. For example, self-learning algorithms or optimization algorithms are used to automatically adjust parameters according to specific tasks and data characteristics to improve the robustness and adaptability of the algorithm.

Besides the RANSAC and PROSAC algorithms, there are some other geometric consistency algorithms that have good results. Shuo et al. [17] proposed a double-constrained false match point elimination algorithm based on Pearson correlation coefficient for length and angle for RANSAC and PROSAC for the situation that RANSAC and PROSAC often eliminate some correct matching points. The first coarse elimination of the mis-matching points with large errors, and then the fine elimination of the mis-matching points with small errors by iteration, have remarkable effects. Jianwei et al. [18] proposed a strategy to remove the mis-matched feature points in a multi-eye fisheye vision SLAM system to solve the problem of degraded localization accuracy due to significant distortion and obvious viewpoint differences in fisheye images.

### 3.2 Graph Theory-Based Approach

The graph theory-based approach adjusts the positions of matching points by optimizing the cost function. In this approach, a graph is first constructed with nodes of the graph representing feature points or key frames and edges representing matching relationships

or constraints. Then, the positions of the nodes or camera poses of the graph are optimized by minimizing the reprojection error or constraint error to obtain a more accurate matching result. This method is able to globally consider the relationships between feature points and is suitable for handling large-scale datasets and complex scenes.

In the paper [19], sparse matching points are used as nodes, and the sum of similarity of the triangles corresponding to each node is used as the attribute value to locate the mis-matching points using the similarity relationship of triangles, which has higher recognition rate and lower false positive rate for mis-matching points compared with the widely used random sampling consistency coarse difference detection method. Wenfei [20] proposed a new GSIFT-RANSAC algorithm using the graph theory principle, which combines the graph theory algorithm with the classical RANSAC algorithm for coarse difference elimination. Tang [21] proposed a graph theory-based method for automatic detection of laser image mismatch points, using the scale-invariant feature transform to detect the extreme value points of laser images to complete feature point extraction, normalize the feature points, calculate the distance between the extracted feature points, construct the complete map of laser images according to the distance for the extracted feature points; build the exported map of laser images, and automatically detect the mismatch points by iteratively processing the exported map, and get The result of false match rate is low and the proportion of internal points is high. The method has a low mis-matching rate, good robustness to illumination, and good matching when rotation occurs.

### 3.3 Methods Based on Motion Statistics

Motion statistics-based method is a technique used to eliminate mismatch points, which is based on the motion information between adjacent frames to determine the accuracy of matching points. Zhao et al. [22] introduced a pole-pole geometric constraint (EGC) model with projection error function and proposed an improved GMS-PROSAC image mismatch elimination algorithm. It consists of the traditional GMS algorithm and the improved PROSAC algorithm. First, the GMS algorithm is used to select some matching pairs with the highest similarity to obtain the parameters of the EGC model. Using the calculated parameters, the improved PROSAC algorithm is performed, and experiments show that the combination of the two methods can obtain more high-quality matching pairs. Liu et al. [23] then proposed an adaptive feature matching algorithm based on grid motion statistics (GMS), which also uses the GMS algorithm to do the initial mismatch point elimination first and then uses the random sampling consistency algorithm to filter out the exact matches, in response to the problem that the performance of the grid motion statistics (GMS) algorithm depends on the number of feature points and there is a concentration of mis-matches when there are fewer feature points detected, combined with the idea of consistency constraints. Zhang [24] proposed a redundant point mismatch removal method based on Oriented Rapid Rotation Simplified (ORB) for visual simultaneous localization and mapping system. On the one hand, the grid-based motion statistics (GMS) algorithm reduces the processing time of key frames with more feature points and greatly improves the robustness of the original algorithm in complex environments. On the other hand, the random sample consistency (RANSAC)

algorithm is used to optimize and correct the GMS algorithm for the situation that it is prone to mismatching when there are fewer symmetric feature point pairs.

It can be seen that the method based on motion statistics is generally used in combination with the geometric consistency method, because the method is less effective for scenes without significant motion or where accurate motion cannot be estimated, so it needs to be combined with other methods to compensate for its shortcomings.

### 3.4 Learning-Based Approach

The learning-based approach to Eliminating false matches is a method that uses machine learning techniques to automatically learn and identify false matches. Prediction and elimination are performed by training models without manually setting thresholds or rules, reducing the need for manual intervention. The learning method can learn the general pattern of feature point pairs from a large amount of sample data, and has a certain degree of robustness to handle the mis-match points under different scenes and changing conditions.

Machine learning can classify feature points well, and Wu et al. [25] proposed the KNN-PROSAC algorithm, which uses the Hamming distance between descriptors as a similarity measure, and the K-most-neighborly method treats those with small distances as the same class, and performs coarse matching first, and then fine-matching is completed using PROSAC, with substantial improvement in matching quality. Youwen [26] proposed a machine learning-based method for comparing feature vectors to replace existing matching methods with pattern classification problems. Yang [27], on the other hand, proposed a lattice-weighted representation strategy learning model to address the problem that most feature matching methods have difficulty in maintaining applicability in vision tasks. GWMLR combines a lattice structure with a supervised-based approach, and the matching results in complex scenes are significantly better than other algorithms.

Deep learning, as a subfield of machine learning, has developed rapidly in recent years, and deep neural networks, which can access semantic information in images and provide better understanding of the surrounding environment, have also started to be applied to feature point matching. Kun [28] proposed a multiscale loss function. For each candidate match, this loss function is constrained at three levels of single-sample classification correctness, local neighborhood structural consistency and global geometric consistency, respectively, and the LGC deep neural network is trained for error matching elimination using supervised learning, and the LGC network structure is shown in Fig. 2.

Deep learning has made significant progress in image feature point matching. Future models are likely to be more sophisticated and powerful, capable of better learning and representing features in images, with global information and a larger context for false match point rejection. Future learning-based methods for false match point rejection will leverage the development of deep learning techniques, weakly supervised learning, nonlocal matching, cross-modal processing, and migration learning to improve accuracy, adaptability, and scalability, driving further development of false match point rejection techniques.

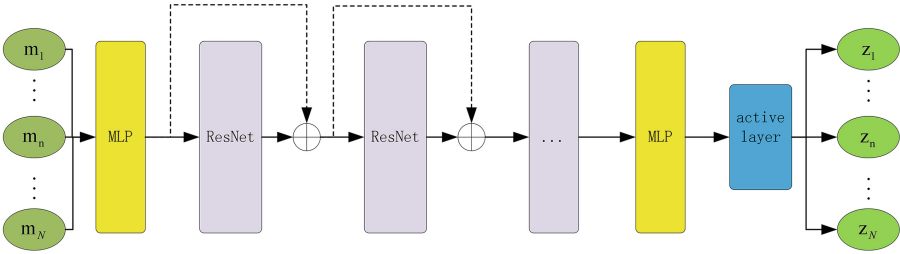


Fig. 2. LGC network structure

## 4 Analysis, Comparison and Prospect of False Match Point Elimination Methods

Figure 3 shows the matching effect of four classic mismatching removal methods on ORB features. The RANSAC algorithm, as the most mainstream feature point matching algorithm, has superior effect and is faster. KNN-PROSAC is a combined algorithm with the highest matching accuracy and the largest number of matches, but is slower due to the use of two algorithms.

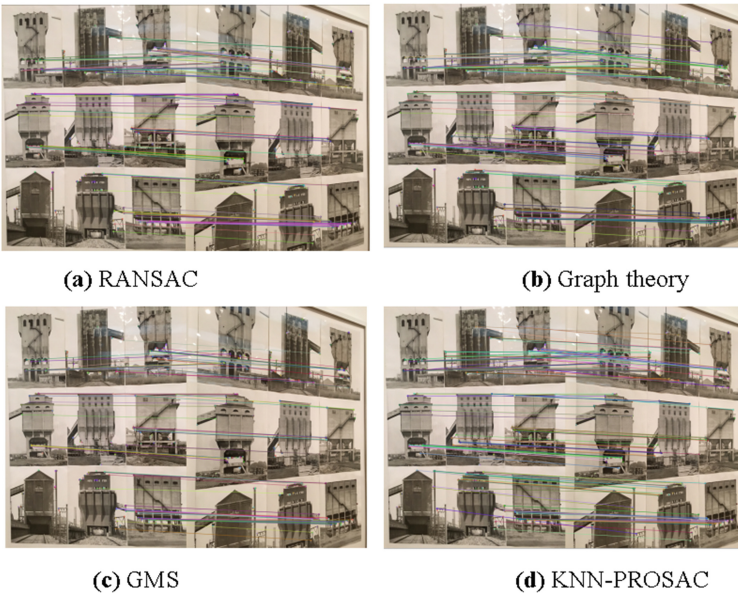


Fig. 3. Comparison of the effects of four classical false match point elimination algorithms

Table 1 compares the four types of methods in terms of principle, characteristics, and performance. Geometric consistency-based methods are the most common and moderate in all aspects, while learning-based methods have higher accuracy and robustness, but slow computation speed and large storage overhead. Each method has its own advantages

**Table 1.** Comparison of the four types of false match point elimination methods

	Geometry-based methods	Graph theory-based approach	Motion statistics-based approach	Learning-based approach
Basic Principle Introduction	Estimating the correct matching relationship by computing a geometric model	Create a graph of connection relationships between feature points	Determine whether two matched pairs match consistently by the angle between their motion vectors	Train a model to determine accuracy by matching relationship of feature points
Features	Suitable for scenes with obvious geometric constraints, less effective in complex scenes	Good robustness, but not efficient enough for large data sets	Better results in complex scenes, with certain requirements for the accuracy of the motion model	Can be adapted to different scenarios, but requires rich computational resources
Matching accuracy	***	**	**	****
Matching speed	***	**	***	*
Robustness	**	***	***	****
Storage Overhead	*	***	*	*****

and limitations in terms of false match elimination. A comprehensive selection and combination of different methods can achieve better false match elimination results according to the needs of specific application scenarios.

## 5 Conclusion

Feature description algorithms such as SIFT, SURF and ORB perform well in image matching, but still suffer from the problem of mis-matching. The mis-matched feature points may be caused by factors such as image noise, occlusion, and similar structures. Combining geometric constraints, graph optimization and statistical learning can deal with the mis-matching problem more comprehensively and improve the accuracy and robustness of feature matching. In addition to the combination of multiple methods, the future may also develop from the following directions: deep learning model improvement, multi-scale and multi-view matching, and multi-sensor fusion matching.

In conclusion, for the problem of mis-matched feature point elimination, studies have shown that better results can be achieved by using a combination and integrated application of multiple methods. The selection of the appropriate method depends on the



specific application scenario and requirements. In addition, the performance of different methods may be affected by parameter settings, characteristics of the dataset, and noise and outliers, so appropriate tuning and parameter selection are required for practical applications. The removal of mis-matching points is widely used in several fields of 3D reconstruction and AR, visual SLAM, image stitching, and target tracking and recognition. With the continuous development of algorithms and technologies, the method of eliminating false match points will play a more important role in these application fields and promote further development of related fields.

**Funding Statement.** The authors are highly thankful to the National Natural Science Foundation of China(NO.62063006), the Natural Science Foundation of Guangxi Province (NO.2023GXNSFAA026025), to the Innovation Fund of Chinese Universities Industry-University-Research (ID:2021RYC06005), to the Research Project for Young and Middle-aged Teachers in Guangxi Universities (ID: 2020KY15013), and to the Special research project of Hechi University (ID:2021GCC028). This research was financially supported by the project of outstanding thousand young teachers' training in higher education institutions of Guangxi, Guangxi Colleges and Universities Key Laboratory of AI and Information Processing (Hechi University), Education Department of Guangxi Zhuang Autonomous Region.

## References

1. Tan, F., Mu, P., Ma, Z.X.: A multi-target tracking algorithm based on YOLOv3 detection and feature point matching. *J. Metrol.* **42**(02), 157–162 (2021)
2. Jingjing, X., Dongbao, Z., Yue, D., Lianhai, C., Xiangrong, G.: Multi-source homonymous residential ground target identification and its homonymous feature point matching method. *Geography Geograph. Inf. Sci.* **38**(05), 9–15 (2022)
3. Jiahua, H., Chong, S., Jun, T., Jun, L.: A fast image stitching method based on improved ORB-GMS-SPHP algorithm. *Navigat. Position. Timing* **10**(02), 108–116 (2023)
4. Liu, C., Dang, S., Chen, L.: An improved feature matching and dense map building algorithm based on ORB-SLAM3. *Comput. Appl. Res.* 1–8 (2023)
5. Lowe, D.G.: Distinctive image features from scale-invariant key points. *Int. J. Comput. Vis.* **60**(2), 91–110 (2004)
6. Bay, H., Tuytelaars, T., Van Gool, L.: Surf: Speeded up robust features. *Lect. Notes Comput. Sci.* **3951**, 404–417 (2006)
7. Rublee, E., Rabaud, V., Konolige, K., et al.: ORB: An efficient alternative to SIFT or SURF. In: 2011 International Conference on Computer Vision, pp. 2564–2571. IEEE (2011)
8. Yibo, G., LeRong, M.A., JinRong, H.E.: A review of image pyramid model application research. *J. Yan'an Univ. (Nat. Sci. Ed.)* **42**(01), 83–89 (2023)
9. Yang, Z., Fei, W., Dai, W., Li, C., Zou, J., Xiong, H.: Mixed-precision quantization with dynamical hessian matrix for object detection network. In: 2021 International Conference on Visual Communications and Image Processing (VCIP), Munich, Germany, pp. 1–5 (2021)
10. Rosten, E., Drummond, T.: Machine learning for high-speed corner detection. In: Proceedings of the 9th European Conference on Computer Vision. Graz, Austria: Springer, pp. 430–443 (2006)
11. Csurka, G., Dance, C., Fan, L., et al.: Visual categorization with bags of keypoints. In: Workshop on Statistical Learning in Computer Vision, ECCV **1**(1–22), 1–2 (2004)
12. Derpanis, K.G.: Overview of the RANSAC Algorithm. *Image Rochester NY* **4**(1), 2–3 (2010)

13. Chum, O., Matas, J.: Matching with PROSAC-progressive sample consensus. In: 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), vol. 1, pp. 220–226. IEEE (2005)
14. Campos, C., Elvira, R., Rodríguez, J.J.G., et al.: Orb-SLAM3: an accurate open-source library for visual, visual-inertial, and multimap SLAM. *IEEE Trans. Robot.* **37**(6), 1874–1890 (2021)
15. Jiahui, L., Fengsheng, Z., Haoyang, C.: A single-strain matrix estimation method with improved RANSAC algorithm. *Softw. Guide* **19**(02), 149–152 (2020)
16. Quanrong, G.: Improved ORB-SLAM2 Mis-match Elimination Algorithm and Map Construction. Liaoning University of Engineering and Technology (2022)
17. Shuo, L., Yingdong, H., Shuang, W., Kun, L., Junfeng, J., Tiegen, L.: Image mis-match point elimination algorithm based on Pearson correlation coefficient. *Adv. Laser Optoelectron.* **58**(08), 263–273 (2021)
18. Jianwei, C., Yuanlie, H., Mingzhen, H., Feng, L.: Multi-eye fisheye vision SLAM feature point mis-matching for elimination optimization. *J. Dalian Univ. Technol.* 1–12(2023)
19. Xiuxiao, Y., Wei, Y., Shiyu, C.: Automatic detection method of remote sensing image mis-matching points based on graph theory. *J. Wuhan Univ. (Inf. Sci. Ed.)* **43**(12), 1854–1860 (2018)
20. Wenfei, X., Zhengtao, S., Guozhu, L.: Coarse difference elimination of UAV image matching feature points by graph theory algorithm. *Mapp. Bull.* **2020**(04), 6–10 (2020)
21. Tang, T., Tan, F.: Automatic detection of laser image mis-match points based on graph theory. *Laser J.* **44**(05), 210–214 (2023)
22. Zhao, P., Ding, D., Wang, Y., et al.: An improved GMS-PROSAC algorithm for image mismatch elimination. *Syst. Sci. Control Engin.* **6**(1), 220–229 (2018)
23. Liu, C.-A., Ai, Z., Zhao, L.-J.: Adaptive image feature matching algorithm based on grid motion statistics. *J. Huazhong Univ. Sci. Technol. (Nat. Sci. Ed.)* **48**(01), 37–40+54 (2020)
24. Zhang, D, Zhu, J, Wang, F, Hu, X, Ye, X.: GMS-RANSAC: A Fast Algorithm for Removing Mismatches Based on ORB-SLAM2. *Symmetry* 2022, vol. 14, p. 849 (2022)
25. Wu, Y.W., Zuo, T., Zhang, J.B., et al.: Multi-robot SLAM map fusion algorithm based on KNN-PROSAC and improved ORB. *High Tech Lett.* **31**(7), 7 (2021)
26. Youwen, H., Ce, Y.: A learning-based algorithm for mis-matched feature point elimination. *Technol. Square* **2016**(02), 5–8 (2016)
27. Yang, L.J., Huang, Q., Huang, Y., Zhang, Y.: A grid-weighted representation strategy learning model for mis-match elimination. *China Sci. Technol. Paper* **17**(03), 274–280 (2022)
28. Kun, S., Wen, D.: A mis-match elimination method based on multi-scale loss function. *J. Shanxi Univ. (Nat. Sci. Ed.)* **45**(03), 641–648 (2022)



# Current Challenges in Federated Learning: A Review

Jinsong Guo<sup>1</sup>, Jiansheng Peng<sup>1,2(✉)</sup>, and Fengbo Bao<sup>1</sup>

<sup>1</sup> College of Automation, Guangxi University of Science and Technology, Liuzhou 545000, China

sheng120410@163.com

<sup>2</sup> Department of Artificial Intelligence and Manufacturing, Hechi University, Hechi 547000, China

**Abstract.** Federated learning is a privacy-preserving solution for distributed machine learning, allowing participants to solve machine learning problems collaboratively without transmitting their local data to a central server. Instead, they exchange model parameters to achieve the desired outcomes. However, recent scholarly research has revealed several challenges in the traditional federated learning framework. This paper aims to address the issues of communication efficiency, privacy leakage, and client selection algorithms within the federated learning paradigm while exploring potential future research directions.

**Keywords:** Federated learning · Communication efficiency · Privacy leakage · Client selection

## 1 Introduction

After the release of ChatGPT in November 2022, the world was stunned by its powerful capabilities. Artificial intelligence (AI) development has caused a crisis for real-life practitioners in certain industries and has opened people's eyes to the powerful potential that AI holds. However, even the powerful ChatGPT 4.0 is currently facing many problems that need to be solved. For example, the large number of users who constantly provide data for ChatGPT every day will inevitably leak their own personally identifiable information, and when there is a security breach, it will hurt users' privacy. So the privacy issue is an important problem that AI is currently facing.

The unprecedented growth in data volume in recent years has seen an increasing number of fields using machine learning to analyze data and build decision systems. Federated learning (FL), an important tool in machine learning to address privacy issues, has been widely studied over the years. FL, as an emerging machine learning method, allows model training with guaranteed data privacy and security. Using the features of federation learning, if all hospitals are federated to build machine learning models, a huge amount of data can train better models. However, with the application of FL and continuous research, it has been found that FL faces problems such as expensive communication costs, privacy leakage and system heterogeneity.

## 2 Federated Learning

Federated Learning (FL) is a new machine learning paradigm that enables data security and privacy protection. FL can be used in a wide range of applications in finance, biomedicine, computer vision, and natural language processing. Traditional machine learning has limited ability to handle large-scale data, and distributed machine learning can handle large-scale data but has the problem of privacy leakage of clients, and FL provides a solution to these problems. Federated learning mainly consists of a server and several clients, and the main processes of FL are: (1) the server screens the clients participating in FL; (2) the server side delegates the global model that needs to be trained; (3) the clients receive the global model and start local training; (4) the clients upload the trained local model parameters to the server; (5) the server performs all model parameters aggregation to update the global model; (6) repeat steps 1–5 until the model meets the conditions; as shown in Fig. 1. From the workflow of FL, we can see that the server and the client only pass the model training parameters without sending the local data from the client to the server, which effectively avoids the leakage of local privacy and also solves the problem that machine learning cannot handle large-scale data, but there are still many problems to be solved in FL.

FL can be divided into Horizontal Federated Learning, Vertical Federated Learning and Federated Transfer Learning, as shown in Fig. 2. Horizontal Federated Learning is suitable if the participants have more overlapping feature dimensions in their data distribution, e.g., two identical banks in different regions, i.e., having similar features (banks). Vertical Federated Learning is appropriate if the participants' data distribution has more overlapping sample dimensions, e.g., two related companies in the same region, i.e., with similar samples (customers). Federated Transfer Learning can be performed if both feature dimension and sample dimension crossover are small.

## 3 Problems Faced

In this section, we present the problems faced by FL and summarize the current solutions. As shown in Table 1.

### 3.1 Communication Efficiency Issues

In FL the server may communicate with a large number of clients, and each client often has different signal conditions as well as bandwidth. Since clients and servers need to communicate frequently during FL, communication efficiency is one of the issues that affect FL. The main causes of FL communication problems are as follows:

1. The number of clients is huge: more users added to FL is beneficial for model training because the larger the amount of data the better the trained model. But more clients means a larger communication cost per model training round.
2. Differences in client network bandwidth: Differences in the network bandwidth of different clients make them differ in model upload and download speed. After a round of local training, some clients may not be able to upload the model parameters to the server due to network bandwidth problems, resulting in the model loss.

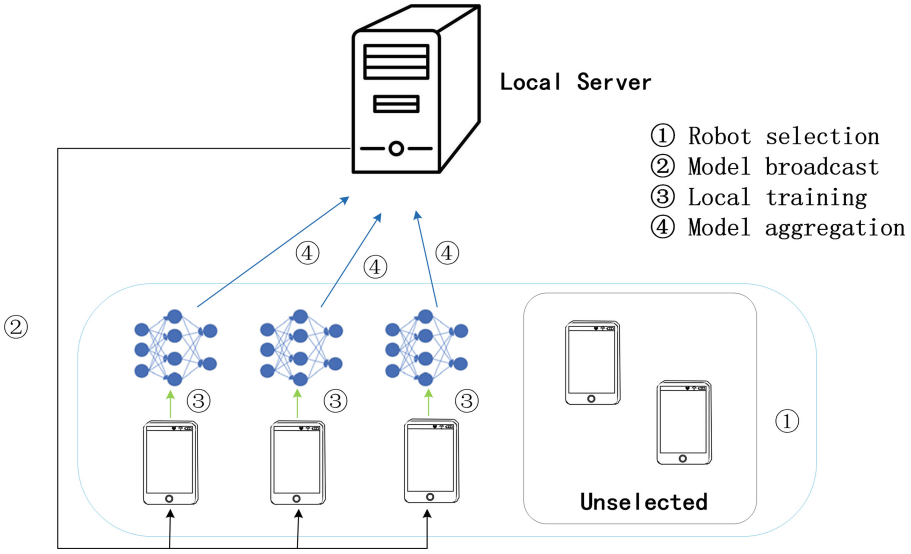


Fig. 1. FL workflow

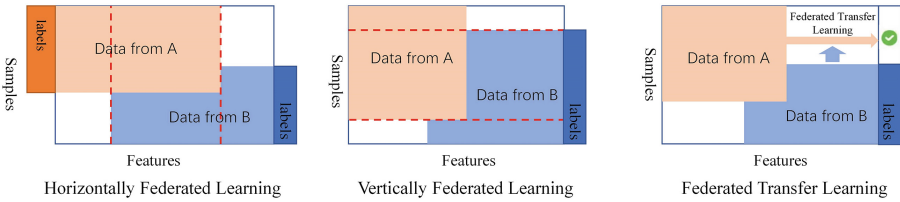


Fig. 2. Classification of Federated learning

There are two main means to solve the communication problem of FL, one is gradient compression. In FL, the model parameters are usually computed in multiple clients and are transmitted in the form of gradients. Gradient compression improves the efficiency of the transmitted gradients by reducing the representation accuracy of the gradients or by setting some elements to zero, etc. In the literature [1] the authors use lossy compression when exchanging gradients between the server and the client, and they mention in the paper that passing only a subset of the global model to the client can effectively improve the communication efficiency of FL. Literature [2] In the authors' proposed FetchSGD, the algorithm can effectively reduce the communication cost of FL with Non-IID at the time of client data and the algorithm has good scalability. Although the gradient compression approach can reduce the communication cost between the server and the client, incomplete gradient information sacrifices a large amount of performance.

Another approach is model distillation, which can speed up the renewal of local models, improve performance and cost less communication by transferring the knowledge of the global model to the local model. In the literature [3] the authors proposed a variant of model distillation called distillation. This method uses online distillation to improve

the speed of fitting large-scale datasets and experiments show that distillation has faster training speed compared to distributed SGD. The authors in the literature [4] discarded the traditional FL global model update method and used knowledge distillation to upload the client model predictions to the server to avoid uploading complex model parameters, thus improving the communication efficiency of FL. The authors in the literature [5] propose a new framework for FL that effectively protects data privacy while improving communication efficiency by fusing Differential Privacy with federal model distillation.

### 3.2 Privacy Leakage Issues

A huge advantage of FL over traditional distributed learning is that FL has stronger privacy, but it has been found that malicious participants in FL can reconstruct participants' private data through frequent model parameter passing between server and clients [6]. There are two main directions to address the FL privacy leakage problem:

1. Data blurring: privacy-preserving effects, such as Differential Privacy (DP), are achieved by adding noise to the data exchanged between participants. However, noise affects the performance of the model while protecting privacy, so the main research direction of the approach using data fuzzing is to achieve a trade-off between privacy and model efficiency.
2. Data encryption: The way of encrypting data using keys is another scheme to protect data privacy, such as Homomorphic Encryption (HE). But data encryption consumes more computational resources and affects the efficiency of FL's model updates. So the main research direction of the method using data encryption is to reduce the extra resource loss caused by encryption algorithms.

Literature [7] proposed LDP-Fed, in which the authors used LDP (Local Differential Privacy) to protect the privacy of the participants, each participant initializes the privacy budget according to their preferences, assigning a different level of privacy protection to each, reducing the effect of noise on the efficiency of the model. Literature [8] The authors combine Differential Privacy with secure multi-party computation to achieve a trade-off between privacy and accuracy through tunable trust parameters. Literature [9] in which the authors propose a FL protocol LDPFL applied to industrial environments, firstly the implementation of the method does not require complex prerequisites and assumptions, while experimentally the method is shown to have excellent model performance with the addition of noise.

The authors in the literature [10] proposed BatchCrypt as a solution to the problem faced by HE. This method uses a batch encryption method for gradient values to reduce the computational burden and storage pressure caused by HE. Specifically, it first quantizes the gradient data into integer form, and then, encodes the batch of quantized values into a long integer and encrypts them all at once. This method is also applied to the industrial FL framework FATE. Homomorphic Encryption using the same key increases the risk of privacy leakage, and in the literature [11] the authors propose a privacy-preserving scheme for multi-key Homomorphic Encryption, which enhances the ability to resist privacy leakage caused by collusion of multiple malicious clients by assigning different keys to participants.

### 3.3 System Heterogeneity

FL participates in a large number of devices, and often each device has different storage, computing and communication capabilities due to memory, network connectivity and power supply, and the heterogeneity between different devices affects the performance of FL. This problem can be solved by optimizing the client selection algorithm of FL. The traditional FL uses a random way to select clients, and this selection method brings a series of problems: on the one hand, the computational power gap will make the clients that have completed local training need to wait for other clients to finish training; on the other hand, some clients with poor signal conditions will fail to upload model parameters and affect the accuracy of the model trained by the FL. Therefore, FL needs to consider all aspects in the client selection stage. The client selection method of FL is divided into two types: biased selection and unbiased selection.

The authors in the literature [12] proposed FedCS, where the client sends its local wireless channel state and computational power to the server before performing client selection, and the server uses a greedy algorithm to select as many clients as possible for local training while setting a deadline for the client's model upload. Experiments show that this method can complete the training task in a shorter time under a variety of conditions. In the literature [13] the authors proposed a biased client selection algorithm called POWER-OF-CHOICE, where the authors confirmed that selecting clients with higher local loss values can accelerate model training and improve accuracy. The literature [14] proposes a grouped client aggregation approach. Firstly, clients need to send their local data categories to the server before the start of FL, and the server divides the clients with the same category of data into a group, and selects a group of clients for training in each round of model update. Experiments show that there is still a high convergence speed and model accuracy in the case of unbalanced data distribution. In the literature [15], the authors consider the problem of unexpected client withdrawal. In the paper, the authors introduce the concept of "friendship", where clients with similar data distribution will become friends, and if a client unexpectedly quits FL due to network and power problems, the local update of the friend's client will be used instead. This approach mitigates the negative impact of unexpected client exit.

## 4 Summary and Outlook

Nowadays, the development of artificial intelligence is unstoppable, and the emergence of FL has broken the data silos. As one of the current popular research directions in the field of machine learning, its emergence solves the problems of privacy protection, huge communication overhead and inability to train large-scale models faced by distributed learning, but the current FL still has many problems that need to be solved in the future.

Sending small messages or model updates during training, instead of full model update messages, or reducing the number of communication rounds is an important means to address the expensive communication cost of FL.

The use of the HE algorithm in FL needs to consider the additional computational and communication costs associated with this algorithm, and HE can be combined with methods such as gradient compression to provide privacy protection for FL. The main

**Table 1.** Problems faced by FL

Problem description	Solutions	Advantages	Disadvantages	References
Communication efficiency	Gradient compression	Reduce communication overhead	Decreased training performance	[3, 4]
	Model distillation	Accelerated Reasoning	Additional data required	[5–7]
Privacy leakage	Blurred data	Enhanced privacy	Decreased training performance	[9–11]
	Data encryption	Enhanced privacy	High computational overhead	[12, 13]
System heterogeneity	Unbiased client selection	Data Balance	Slow convergence	[14]
	Biased client selection	Fast convergence	Data Bias	[15–17]

problem of using DP to protect FL privacy is that it affects model accuracy, and adding eliminable noise may be the main research direction of DP in the future.

The impact of system heterogeneity on FL can be solved by optimizing the client selection algorithm. In the future, the client selection needs to integrate the storage, computing and communication capabilities of the client devices for selection.

**Funding Statement:** The authors are highly thankful to the National Natural Science Foundation of China(NO.62063006), the Natural Science Foundation of Guangxi Province (NO.2023GXNSFAA026025), to the Innovation Fund of Chinese Universities Industry-University-Research (ID:2021RYC06005), to the Research Project for Young and Middle-aged Teachers in Guangxi Universities (ID: 2020KY15013), and to the Special research project of Hechi University (ID:2021GCC028). This research was financially supported by the project of outstanding thousand young teachers' training in higher education institutions of Guangxi, Guangxi Colleges and Universities Key Laboratory of AI and Information Processing (Hechi University), Education Department of Guangxi Zhuang Autonomous Region.

## References

1. Caldas, S., Konečný, J., McMahan, H.B., et al: Expanding the reach of federated learning by reducing client resource requirements. arXiv preprint [arXiv:1812.07210](https://arxiv.org/abs/1812.07210) (2018)
2. Rothchild, D., Panda, A., Ullah, E., et al.: Fetchsgd: communication-efficient federated learning with sketching. In: International Conference on Machine Learning. PMLR, pp. 8253–8265 (2020)
3. Anil, R., Pereyra, G., Passos, A., et al: Large scale distributed neural network training through online distillation. arXiv preprint [arXiv:1804.03235](https://arxiv.org/abs/1804.03235) (2018)
4. Sui, D., Chen, Y., Zhao, J., et al.: Feded: federated learning via ensemble distillation for medical relation extraction. In: Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing (EMNLP), pp. 2118–2128 (2020)



5. Sun, L., Lyu, L.: Federated model distillation with noise-free differential privacy. arXiv preprint [arXiv:2009.05537](https://arxiv.org/abs/2009.05537) (2020)
6. Zhu, L., Liu, Z., Han, S.: Deep leakage from gradients. *Adv. Neural Inf. Process. Syst.* 32 (2019)
7. Truex, S., Liu, L., Chow, K. H., et al.: LDP-fed: federated learning with local differential privacy. In: *Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking*, pp. 61–66 (2020)
8. Truex, S., Baracaldo, N., Anwar, A., et al.: A hybrid approach to privacy-preserving federated learning. In: *Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security*, pp. 1–11 (2019)
9. Chamikara, M.A.P., Liu, D., Camtepe, S., et al.: Local differential privacy for federated learning in industrial settings. arXiv preprint [arXiv:2202.06053](https://arxiv.org/abs/2202.06053) (2022)
10. Zhang, C., Li, S., Xia, J., et al.: Batchcrypt: efficient homomorphic encryption for cross-silo federated learning. In: *Proceedings of the 2020 USENIX Annual Technical Conference (USENIX ATC 2020)* (2020)
11. Ma, J., Naas, S.A., Sigg, S., et al.: Privacy-preserving federated learning based on multi-key homomorphic encryption. *Int. J. Intell. Syst.Intell. Syst.* **37**(9), 5880–5901 (2022)
12. Nishio, T., Yonetani, R.: Client selection for federated learning with heterogeneous resources in mobile edge. In: *ICC 2019–2019 IEEE International Conference on Communications (ICC)*. IEEE, pp. 1–7 (2019)
13. Cho, Y.J., Wang, J., Joshi, G.: Client selection in federated learning: convergence analysis and power-of-choice selection strategies. arXiv preprint [arXiv:2010.01243](https://arxiv.org/abs/2010.01243) (2020)
14. Cao, M., Zhang, Y., Ma, Z., et al.: C2S: class-aware client selection for effective aggregation in federated learning. *High-Confiden. Comput.* **2**(3), 1–9 (2022)
15. Wang, H., Xu, J.: Friends to help: saving federated learning from client dropout. arXiv preprint [arXiv:2205.13222](https://arxiv.org/abs/2205.13222) (2022)



# Cloud-Network Resource Scheduling for ONAP-Based IDN

Xiangning Li<sup>(✉)</sup>, Yuqian Cai, Ruotong Wu, and Jingyue Tian

China Telecom Beijing Research Institute, Beijing, China

lixn68@chinatelecom.cn, caitlin.yu@126.com, {472967971,158155978}@qq.com

**Abstract.** In the 5G and 5G+ scenario, a large number of devices access to the network and a large number of different services are demanded by different vertical industries. To maintain the QoS and satisfy such a lot of demands, MEC (mobile edge computing) deployment and IDN (Intent-Driven Network) scheduling are necessary. MEC could upload the third-part App to the cloud servers, which could save the calculate force in the local UE (user equipment). And IDN could identity and integrate UE intents in natural language and translate them into cloud-network scheduling policy to implement them and manage cloud-network resources. ONAP as the platform for orchestrating, manages and automating network and edge computing services. This paper introduces the intent instance management model of ONAP and IDN, introduces the MEC, containers and slices management and designs intent-and-resource -weighted algorithms to make the policies and ensure the QoS.

**Keywords:** 5G · IDN · ONAP · Cloud-network · Cloud resource management · Slice management

## 1 Introduction

As the development of 5G and 5G+, a large number of devices access to the network, the cloud-computing network and intend-driven network become the novel research trends among the network operators and devices suppliers in recent years. MEC (mobile edge computing) is a novel cloud-computing model with large prospect, which provides UE (user equipment) accessed to RAN (radio access network) cloud-computing functions, extends computing, telecommunication and buffers to the network edges, and supports low-delay, high-reliability, high-mobility and other features. MEC is distributed around UEs densely and deployed with the CU (central unit) of BBU (base-band unit), which is the main part of BS (base station) and composed by CU and DU (distributed unit), and Near RT-RICs (real-time RAN intelligent controller) on the same BS servers.

---

Supported by the 2020 National Key R&D Program “Broadband Communication and New Network” special “6G Network Architecture and Key Technologies” 2020YFB1806700.

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2024  
Y. Zhang et al. (Eds.): CENet 2023, LNEE 1127, pp. 39–52, 2024.  
[https://doi.org/10.1007/978-981-99-9247-8\\_5](https://doi.org/10.1007/978-981-99-9247-8_5)

The ONAP-based IDN is a network that can manage and control itself based on user intents and ONAP (Open Network Automation Platform), which is a kind of open-source platform faces to the network operators, cloud service providers and enterprises for network and edge cloud service orchestration, management and automation.

In this paper we explore the methods to schedule MEC cloud resource and BBU network resource in the ONAP together. The motivation of this paper is to design a system high-efficiency managing the RAN slices and MEC computing and storage resources (CPU, memory and disk and so on) based on user intents, which will solve the problems of low QoE (quality of experience) because of resource shortage. To address such problems, we research amount of modern contributions such as cloud computing, intent-driven networking, ONAP architecture and recent novel technologies. The focus of this paper is the design of an self-organizing, intent-driven scheduling system to optimize cloud-networking resources efficiency based on user intents.

### 1.1 Problem Description

The ONAP and MEC in 5G network scenario face to a large number of devices access with distinct requirements, the cloud computing resources such as CPUs, memories, disks, accelerators and bandwidths, and slice resources configuration together become complex. An automating and optimal cloud-network resource management according to the UE intents is necessary. However, nowadays resource management system is not qualified for such a challenging task. Hence, a series of well-designed algorithms and patterns for the ONAP is required that can automate the cloud and network configurations process flexibly by translating and identifying diverse UE intents requirements. The work proposes an automated configuring solution for multiple intents of UE to generate different cloud-network resources configuration based on bi-close-loop architecture of ONAP natural language processing mechanism.

### 1.2 Solution Framework

ONAP-based IDN is a reliable solution which can manage network configuration and orchestrate network slice resource blocks based on user intents. The work proposes the unified cloud-network resource management system design of ONAP-based IDN. It unifies the cloud and network resources scheduling together in the ONAP, the scheduling policies based on varying UE requirements. The intent-driven ONAP and RAN system follow bi-loop architecture. It translates UE NLP intents into configuration policies and monitor the cloud-network status to guarantee the QoS. The system performs resource management LCM step-by-step, while translating, creating, storing, monitoring, analyzing, updating, implementing the network slices and MEC.

### 1.3 Major Contribution

The contributions of the paper are as follows:

- We design a cloud-network system to realize the 3 objectives for self-organizing resource management of ONAP-based intent-driven network.
- We design the bi-loop architecture to implement self-organizing and close-loop slice and cloud resource management.
- We design a set of procedures and algorithms to define the policies which manage slice and cloud resources of MEC and RAN for the ONAP. The algorithms weight resources and UE intents instances are for scheduling and defining policies.

The rest of the paper is organized as follows: we introduce background knowledge and review recent years related work and articles in Sect. 2, starting with intent-driven network and ONAP followed by network slice and cloud container scheduling. In Sect. 3, we present intent instance management model, consider the bi-loop architecture of ONAP and procedure of intent instance management; and design intent-and-resource -weighted algorithms, consider the slice, CPU, memory and user intent together to make the policies and ensure the QoS. Finally, in Sect. 4, we provide the conclusion.

## 2 Background

### 2.1 Intent-Driven Network

IDN (Intent-Driven Network) is an “autopilot” network which automates application intent with decoupled network control logic and closed-loop orchestration techniques. It can transform, validate, deploy, configure and optimize automatically to achieve the target network state according to the operator’s intent, and can resolve abnormal events to ensure network reliability. IDN provides full lifecycle management of network elements with the premise of collecting network state. In IDN, network administrators no longer focus on network details or implementation techniques, but simply express their needs, and the network system automatically translates the intent and completes subsequent operations, and verifies for a real-time verification that the actual network state matches the state expected by the business intent.

### 2.2 ONAP

ONAP is a comprehensive platform for orchestrating, managing and automating network and edge computing services for network operators, cloud storage and enterprises. It provides product-independent capabilities for the design, creation and life-cycle management of network services. ONAP provides a unified operational framework for policy-driven design, implementation, analysis and life-cycle management of large-scale loads and services. With ONAP, network operators can synchronize the orchestration of physical and virtual network functions.

### 2.3 Slice Scheduling

Network slice virtualizes network resources, shares them among UEs, and schedules them to improve the network efficiency. There are 3 kinds of slice resources management mechanism. QoS scheduling, resource reservation, and carrier isolation.

When the policy based on QoS scheduling, RAN doesn't reserve the RB for the slices, but when the network resources are short, the high-prior business could use network resource, when there is congestion, high-prior could be affected. QoS scheduling is based on 5QI only or based on 5QI and slice ID.

When the policy based on the resource reservation scheduling, the ONAP groups the slices as the slice groups, and scheduling or managing the RB based on the slice groups, sharing and isolating the radio resource among slices flexibly, satisfying the requirement of slice-level guarantee for the radio resource. There are 3 ways to reserve RB, max-RB ratio, dedicated-RB ratio and min-RB ratio.

- Max-RB ratio: the maximum RB ratio assigned by ONAP for the slice group, and ONAP will not assign more RBs for the slice group, even if the demand of slice group is larger than max-RB ratio.
- Dedicated-RB ratio: the minimum RB ratio assigned by ONAP for the slice group, and the RBs are only used by the UEs in the group. The dedicated RBs are reserved for the slice group, and are not able to be used by UEs in other slice groups, even if the demand of slice group is smaller than dedicated-RB ratio.
- Min-RB ratio: the RBs between dedicated-RB ratio and min-RB ratio are the prior RBs for the slice group. The UEs in the slice group could use the prior RB preferentially, if there is part of prior RBs having not been used by UEs in the slice group, that part of RBs could be used by UEs in other slice groups. If the demand of slice group is larger than min-RB ratio, ONAP will assign more RBs for the slice group, but without priority.

Carrier isolation, there is a carrier in the BS dedicated for a slice, which is high-security level and high-bandwidth requirement.

### 2.4 MEC and Container Management

MEC as the upgrading version of the cloud computing, deploys APPs from data centre to the edge of network, and reduces the delay of UE because of the storage and computing ability in the edge of network. Container as the light-weight virtualization technology is faster and higher resource utilization than VMs (virtual machine). As the development of IoT (Internet of Things), a large number of UEs access to the MEC nodes, the traffic of MEC and demands of containers in the MEC are modified with the motivation of UEs.

Kubernetes container as the most widely used container management system in the edge-computing scenarios, its core components are API Server, the interface of resource operation; Scheduler, which responds to schedule the resources, schedule pods to the adapt node followed the policy; ETCD database, which

saves the status information of the cluster. Node is the workload of Kubernetes, which is composed by VM of physical server; and the Pod, as the minimum scheduling unit, is the application instance, which composed by at least one container.

Normal scheduling policy of Kubernetes is that filters out all the nodes which do not fit the minimum resources demands of UE intents at first. And then weighted left CPU use rate and left memory use rate as index to score the nodes, the node with highest score will be chosen to deploy the container and application. There are 2 kinds of management policies of Kubernetes Pods, one is HPA (Horizontal Pod Autoscaling), the other is VPA (Vertical Pod Automotivation).

HPA means that Pod scales container copies based on the resource use rate, such as CPU, disk, memories and bandwidth dynamically. When the workload of pod reaches the upper limit, HPA will produce more pods to reduce the stress of the single pod based on the management policies. When the workload of pod is idle, HPA will reduce pods based on the management policies.

VPA means that UE will limit the computing resources use rate of pods reasonably, based on resource status of cluster, when UE configures Pod. There are 2 kinds of computing resources management of Pod, one is the resource request, the other is the resource limits. The value of resource request is the minimum value of computing resources assigned to the Pod, if the resources of a node are less than the resources request of the Pod, the Pod will not be scheduled to that node; The value of resource limits is the maximum value of computing resources the Pod can occupy, and it is the reference value of Pod migration policy.

## 2.5 Related Work

In [1], Li FL and Fan GY studied the intent-based network to solve the network autonomy problem. The article introduced the descriptions of IDN scope and architecture in academia and industry, and outlined the closed loop of IDN implementation, including intent acquisition, intent translation, policy verification, intent distribution and execution, real-time feedback and optimization; elaborated the research status of key IDN technologies according to the closed loop of IDN; illustrated the application of IDN in network measurement and network service orchestration with examples. Container cluster dynamic scalable scheme based on mixed load is investigated in [2] by Zhong Yang. For computation-intensive services, a responsive scaling strategy is used, and for network-intensive services, a predictive scaling strategy is used, through the coordination of these two strategies together to complete the dynamic scaling of the service and ensure the stability of the service.

The problem of scheduling virtual resources in container cloud is investigated in [3] by QiruiLi. A two-stage adaptive placement algorithm for virtual resources based on secondary bin packing was proposed. At the VMs placement stage, use BDF algorithms. At the containers placement stage, improve the BFD-based bin algorithms to achieve the adaptive placement of the containers on VMs. The experimental results show that the proposed algorithm can efficiently improve

the data center’s computing resources utilization. Containers resource allocation in dynamic cloud environments is investigated in [4] by Oren Katz. The algorithm allocate for each container an available engine to execute it, and provide a constant worst-case approximation bound using the Local Ratio technique. Evaluations based on real-world scenarios show that the performance of algorithm is up to a factor of two better than the performance of existing scheduling algorithms when available resources are scarce. Kubernetes resource scheduling strategy based on load prediction is investigated in [5] by Yong Tang. A combined load prediction model EMD-TCN based on Empirical Mode Decomposition (EMD) and Time Convolutional Network (TCN) was established, which can effectively reduce the request response time of applications. In the Pod scheduling process, appropriate target nodes are selected for scheduling according to different types of Pods, thus eliminating the bottleneck of a single resource on the node and improving the load balance of the node.

A centralized Self-Organising Networks (SON) architecture is investigated in [6] by Carolina Fernández. It designs and implements Multi-Pronged Monitoring and Intent-Based Engine, which can deploy in the verticals condition on the network. A generic intent-based system that can automatically orchestrate and manage network lifecycle over multiple domains, sites and orchestrators is investigated in [7] by Talha Ahmed Khan. As the number of devices grows rapidly, the complexity of orchestrators and platforms increases. The IBN based E2E slice orchestration and platform address the challenge of multi-domain with full automation. The system keeps the network slices stable throughout their lifecycle. A novel E2E network slice management framework is investigated in [8] by Enrique Chirivella-Perez. The main contributions of the work are as follows: allow Industry 4.0 to create ad-hoc customized Network Slices Templates (NST) for their digital transformation; allow Industry 4.0 to interconnect different suppliers, warehouses and manufacturers on demand end-to-end; allows Industry 4.0 to manage the life-cycle of network slice instances (NSI).

### 3 System Design

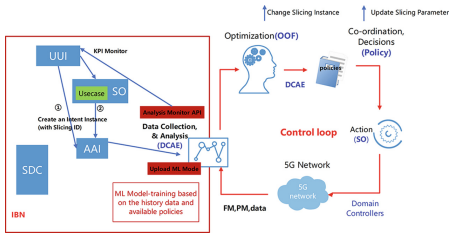
In this section, we propose an intent-driven architecture for ONAP cloud-network resource management system in flow chart given in Figs. 1 and 2 explain the use case in the series of weighted algorithm. The ONAP-based intent-driven network system with bi-loop architecture in Fig. 1 and the procedures and algorithms defines the policies which manage slice and cloud resources of MEC and RAN for the ONAP. The system is composed of intent interaction loop and intent guarantee loop.

#### 3.1 Intent Instance Management Model

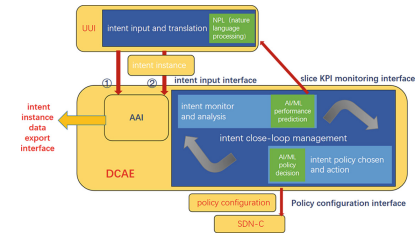
ONAP-based Intent-Driven Network is bi-loop architecture composed by the user loop and the network loop as Fig. 1. The user loop means UEs input user intent and operators input operation intent to UI in natural language, the

UII translates the natural language into cloud-network intent demands, which include configurations demands, QoS demands, by BERT algorithm and other AI algorithms. And then UII creates an intent instance with intent instance ID to SO, SO save the intent instance as scenario usecase ID in AAI, DCAE monitor UE intent instance from AAI. The network loop means DCAE monitors cloud-network status from MEC and RAN by the PM and FM (performance matter and fault matter), when the cloud-network status cannot meet UE demands, the policies will be changed, the slice and cloud configuration instance will be modified. SO implements the policies to the 5G network slices and MEC cloud resources. Finally DCAE inputs the cloud-network status to the UEs as feedback.

To simple the procedure of cloud-network resource management, the bi-loop architecture can translate into intent instance management model based on ONAP as Fig. 2.



**Fig. 1.** Bi-loop architecture of ONAP-based intent-driven network



**Fig. 2.** Intent instance management model based on ONAP open source architecture

Intent instance management means intent instance specification and related user intent storage and interaction updates, intent translation result parameters storage, read and update, network state feedback information storage, etc. Intent closed-loop management and network state monitoring of user intent closed-loop is aware feedback.

Intent instance management provides the aggregation and export function of user information desensitized data such as user original intent interaction information, intent translation result information and network state feedback information, and establishes standard data specification, which can provide the data basis for the training and application of subsequent intent network related intelligent algorithm models.

Components of intent instance management model are as follows:

- Active and Available Inventory (AAI): storage of intent instances;
- Use Case User Interface (UII): user interaction interface and intent translation;
- Data Collection Analytics and Events (DCAE): querying user intent updates from the AAI;



- Service orchestration (SO): scenario usecase management, in which the scenario usecase is responsible for reading the intent information from UUI and save it in the AAI.

Such intent instance management model can also be treated as a kind of business-use-case-decoupled intent monitoring interaction and assurance model, which can support various different slices of business usecases through open interfaces to achieve user intent assurance.

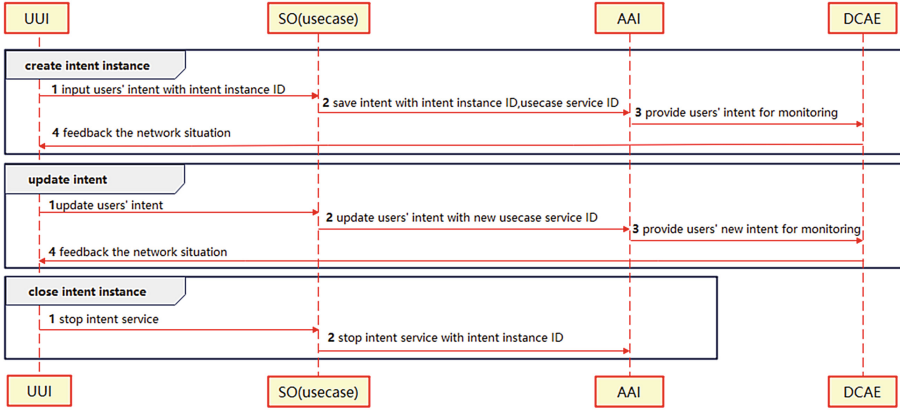
- UUI module: obtains natural language information input by users, parses network intent requirements, selects intent instance creation interfaces according to business usecase design, sends user intent to DCAE module and creates intent instances in the AAI; receives network status information fed by DCAE through slice KPI monitoring interface, provides network status feedback and interaction to users, sends new network intent requirements and completes slice update in a timely manner.
- DCAE module: based on the intent instance to achieve the intent closed-loop management function, access network status feedback and interact with the user through the slice KPI monitoring interface, sends user new network requirement intent and updates the slice configuration timely.
- Intent monitoring and analysis module: predicting future network performance based on real-time network status data and the latest UE intent;
- Intent decision and execution module: when the network performance is predicted can not meet the demand of UE, provides network slice configuration modification policy based on the match result of available policy and user intent.
- Policy distribution execution interface: provide network slice configuration modification policy for business usecase, and the business usecase invokes the policy to complete slice change and distribution.

There are 2 kinds of intent instance management process, one is intent instance management based on scenario usecase, the other is intent instance management based on intent management models.

The flows of intent instances management based on scenario usecase are as Fig. 3.

Intent instance creates:

- 1 The UUI sends the UE intent with its newly intent instance ID to the scenario use case in SO;
- 2 The SO binds the intent, intent instance ID and usecase service ID and saves them in the AAI;
- 3 The AAI provides user intent monitoring interface for DCAE to monitor the latest user intent in real time.



**Fig. 3.** Intent instances management based on scenario usecase

Intent updates:

- 1 The UI updates the user intent to the scenario usecase in the SO;
- 2 The scenario usecase binds the new usecase service ID to the user intent to be saved in the AAI for association with the existing intent instance.

Intent instance closes:

- 1 The UI sends the user stop service request to the scenario usecase in the SO;
- 2 The scenario usecase closes the intent service to the AAI.

The process for managing intent instances from the intent management model is shown in the Fig. 4:

Intention instance creates:

- 1 UI collects the usecase service ID;
- 2 Save the intent with newly created user intent instance ID and the reading usecase service ID in AAI;
- 3 The AAI provides user intent monitoring interface for DCAE to monitor the latest user intent in real time.

Intent updates:

- 1 UI reads the new usecase service ID;
- 2 Save the newly bind usecase service ID bind with the new user intent into AAI to associate with the existing intent instance.

Intent instance closes: UI closes the intent service to AAI directly.

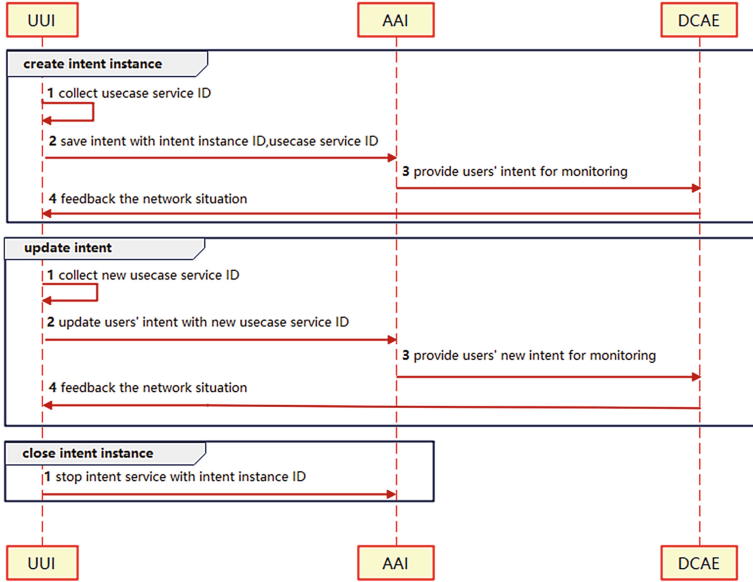


Fig. 4. Managing intent instances from the intent management model

### 3.2 Resource Management Procedure and Algorithms

Based on the above intent instance management process, we design a set of algorithms to define the policies which manage slice and cloud resources of MEC and RAN for the ONAP. The algorithms weight cloud resources (CPU, disk, memories and bandwidth), slice resource of MEC&BS nodes, UE intents instances use-cases priority and number of UEs for scheduling and defining policies.

The MEC&BS platform is composed by Kubernetes nodes, pods and containers. The containers with same intents instances use-cases are deployed in the same Pod with the policies. The RAN of BS is a isolating Pod. The Near-RT RIC authorize UE to use the xApp. The system model consists 3 main parts, calculating UE intents instances use-cases priority, scheduling slice instances, scheduling cloud resources.

The slice scheduling method used in the work is combines QoS scheduling and Min-RB ratio resource reservation, ONAP assigns the RB based on the  $W_u$ , and ONAP set the dedicated-RB ratio and min-RB ratio for each slice, if there is part of prior RBs having not be used by UEs in the slice group, that part of RBs could be used by UEs in other slice group.

Each use-case priority weight  $W_u$  is defined by UE number of invoking the use case service and the default priority level of use case service. We define  $W_u$  as:

$$W_u = \frac{L_{5QI}}{10} + \lg N_{UE} \tag{1}$$

where  $L_{5QI}$  is the default priority level of use case service, and  $N_{UE}$  is UE number of invoking the use case service. The value of  $W_u$  is rounding.

The resource allocation matrix  $\alpha$  can be expressed as cloud resources and radio resource RB, according to the real-time status allocated for the intent instants use-cases cluster in the same pod, each scheduling will based on that. Suppose each column of matrix stands for a resource type, and the pod No. is  $u$ , then:

$$\alpha = \begin{pmatrix} CPU_1 & MEM_1 & DISK_1 & BW_1 & RADSLI_1 \\ CPU_2 & MEM_2 & DISK_2 & BW_2 & RADSLI_2 \\ \dots & \dots & \dots & \dots & \dots \\ CPU_u & MEM_u & DISK_u & BW_u & RADSLI_u \end{pmatrix} \quad (2)$$

In the beginning, the value of  $\alpha$  is

$$\alpha_0 = \frac{RE_{node}}{W_u} \quad (3)$$

where  $RE_{node}$  is the resource total amount of the UE accessing node of MEC&BS.

The  $\beta$  is the resource utilization matrix of pods and slices according to the load of the Pod and slice based on the CPU occupation time, data amount in the memory and disk, the data rate of the application and threads in the container and the RB occupation of each slice then:

$$\beta = \begin{pmatrix} cpu_1 & mem_1 & disk_1 & bw_1 & radsl_1 \\ cpu_2 & mem_2 & disk_2 & bw_2 & radsl_2 \\ \dots & \dots & \dots & \dots & \dots \\ cpu_u & mem_u & disk_u & bw_u & radsl_u \end{pmatrix} \quad (4)$$

The intent instants use-cases pod resource utilized rate matrix of Pod is as follows

$$P_u = \frac{\beta}{\alpha} \quad (5)$$

The resource utilization rate matrix of nodes means the CPU, memory, disk, bandwidth and slices utilization rate of each node in percent. Suppose each column of matrix is a resource type, and the node No. is  $n$ .

$$P_n = \begin{pmatrix} P_{cpu1} & P_{mem1} & P_{disk1} & P_{bw1} & P_{radsl1} \\ P_{cpu2} & P_{mem2} & P_{disk2} & P_{bw2} & P_{radsl2} \\ \dots & \dots & \dots & \dots & \dots \\ P_{cpun} & P_{memn} & P_{diskn} & P_{bwn} & P_{radslin} \end{pmatrix} \quad (6)$$

The pod scheduling method used in the work combines VPA least requested priority function among the nodes in the clusters and HPA inner the node self, ONAP assigns the resources based on the  $\alpha_0$  in the beginning, and ONAP set the maximum limitation and minimum limitation of  $P_u$  for each pod, if there is part of cloud resources have not be used by containers in the pods, that part of resources could be used by other pods.

The problem of pods and slices weighted inner the node is solved by the following iteration procedure, given as Algorithm 1, the output of the algorithm is Pod and slice weight  $W_{p\&u}$ .

---

**Algorithm 1** Pod and Slice Weighted
 

---

**Input:**  $P_u$ 
**Output:**  $W_{p\&u}$ 

```

for  $i = 1 \rightarrow u$  do
  for  $j = 1 \rightarrow 5$  do
    if  $P_u(i, j) > 90\%$  then  $W_{p\&u}(i, j) = 5$ 
    else if  $P_u(i, j) > 70\%$  then  $W_{p\&u}(i, j) = 4$ 
    else if  $P_u(i, j) > 50\%$  then  $W_{p\&u}(i, j) = 3$ 
    else if  $P_u(i, j) > 30\%$  then  $W_{p\&u}(i, j) = 2$ 
    else if  $P_u(i, j) > 10\%$  then  $W_{p\&u}(i, j) = 1$ 
    else  $W_{p\&u}(i, j) = 0$ 
    end if
  end for
end for

```

---

The problem of source node and destination node selection is solved by following Algorithm 2, the output of Algorithm 2 is the node weight  $W_n$ .

---

**Algorithm 2** Node Weight
 

---

**Input:**  $P_n$ 
**Output:**  $W_n$ 

```

for  $i = 1 \rightarrow n$  do
  for  $j = 1 \rightarrow 5$  do
    if  $P_n(i, j) > 90\%$  then  $W_n(i, j) = 0$ 
    else if  $P_n(i, j) > 70\%$  then  $W_n(i, j) = 1$ 
    else if  $P_n(i, j) > 50\%$  then  $W_n(i, j) = 2$ 
    else if  $P_n(i, j) > 30\%$  then  $W_n(i, j) = 3$ 
    else if  $P_n(i, j) > 10\%$  then  $W_n(i, j) = 4$ 
    else  $W_n(i, j) = 5$ 
    end if
  end for
end for

```

---

The problem of scheduling is solved by the following Algorithm 3. The results of algorithm are source node of Pod extending from  $n_{src}$ , the destination node

of Pod extending to  $n_{des}$ , the pod/slice needed to be migrated  $p_{mig}$ , and the pod/slice needed to increase scale  $p_{inc}$  or decrease scale  $p_{dec}$ .

---

**Algorithm 3** Scheduling Algorithm
 

---

**Input:**  $W_{p\&u}\&W_n$

**Output:**  $n_{src}, n_{des}, p_{mig}, p_{inc}, p_{dec}$

```

for  $i = 1 \rightarrow u$  do
  for  $j = 1 \rightarrow 4$  do
    if  $W_{p\&u}(i, j) = 5$  then  $p_{mig} = \arg(W_{p\&u}(i, j) = 5, p)$ 
    else if  $W_{p\&u}(i, j) < 2$  then  $p_{dec} = \arg(W_{p\&u}(i, j) < 2, p)$ 
    else  $p_{inc} = \arg(W_{p\&u}(i, j), p)$ 
    end if
  end for
end for
for  $k = 1 \rightarrow n$  do
  for  $j = 1 \rightarrow 4$  do  $n_{des} = \arg\max(W_n, n); n_{src} = \arg\min(W_n, n)$ 
  end for
end for
for  $i = 1 \rightarrow u$  do
  for  $j=5$  do
    if  $W_{p\&u}(i, j) > 4$  then  $p_{inc} = \arg(W_{p\&u}(i, 5) > 4, p)$ 
    else if  $W_{p\&u}(i, j) < 2$  then  $p_{dec} = \arg(W_{p\&u}(i, 5) < 2, p)$ 
    end if
  end for
end for
end for

```

---

## 4 Conclusion

In this paper we introduce the architecture and components of ONAP and IDN, the MEC, containers and slices management and analyse the cloud-network resources scheduling algorithm based on ONAP and IDN, that aims at automating making the weighted policies in the ONAP to manage the cloud computing resources and slice radio resource blocks together. Our approach considers each intent instance in the AAI, corresponding to a slice and a pod in the containerized cloud. Based on each resources parameter, the weights are determined and the scheduling algorithms are design.

**Acknowledgment.** This work was supported by National Key R&D Program of China (No. 2020YFB1806700).

## References

1. Li, F., Fan, G., Wang, X., Liu, S., Xie, K., Sun, Q.: State-of-the-art survey of intent-based networking. Ruan Jian Xue Bao/J. Softw. **2020**, 31(8), 2574–2587 (2020) (in Chinese). <http://www.jos.org.cn/1000-9825/6088.html>

2. Zhou, Y., Yan, S., Peng, M.: Intent-driven 6G radio access network. *J. Internet Things* **4**(01), 72–79 (2020)
3. Li, Q., Peng, Z., Cui, D., He, J.: A two-stage approach for virtual resources adaptive scheduling in container cloud. In: 2020 IEEE 5th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA), pp. 90–95. Chengdu, China (2020)
4. Katz, O., Rawitz, D., Raz, D.: Containers resource allocation in dynamic cloud environments. In: 2021 IFIP Networking Conference (IFIP Networking), pp. 1–9. Espoo and Helsinki, Finland (2021)
5. Fernández, C., Cárdenas, A., Giménez, S., Uriol, J., Serón, M., Giraldo-Rodríguez, C.: Application of multi-pronged monitoring and intent-based networking to verticals in self-organising networks. In: 2022 5th International Conference on Advanced Communication Technologies and Networking (CommNet), pp. 1–10. Marrakech, Morocco (2022)
6. Zhan, K., Yang, H., Li, J., Zhao, G., Wang, B., Zhang, J.: Demonstration of intent defined optical network: toward artificial intelligence-based optical network automation. In: 2020 International Wireless Communications and Mobile Computing (IWCMC), pp. 874–877. Limassol, Cyprus (2020)
7. Khan, T.A., Abbass, K., Rafique, A., Muhammad, A., Song, W.-C.: Generic intent-based networking platform for E2E network slice orchestration & lifecycle management. In: 2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS), pp. 49–54. Daegu, Korea (South) (2020)
8. Chirivella-Perez, E., Salva-Garcia, P., Ricart-Sanchez, R., Calero, J.A., Wang, Q.: Intent-based E2E network slice management for industry 4.0. In: 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), pp. 353–358. Porto, Portugal (2021)



# Abnormal Transaction Node Detection on Bitcoin

Yuhang Zhang, Yanjing Lu<sup>(✉)</sup>, and Mian Li

Systems Engineering Institute, AMS, PLA, Beijing, China  
kapala@aliyun.com, yanjinglu@qq.com, 326734183@qq.com

**Abstract.** The emergence of blockchain-based anonymous and encrypted digital currencies has brought with it a rapid increase in financial crimes. However, the regulation and detection of financial crimes requires the detection of abnormal transactions in the scenario of blockchain-based anonymous and encrypted digital currencies, where traditional methods are not applicable. In this paper, we propose an abnormal transaction node detection method on bitcoin based on outlier ranking of transaction communities. The public key addresses in bitcoin transactions are merged according to whether they belong to the same user in order to form a user transaction graph, which is used as the input of our method. This graph is then divided into smaller communities. The abnormal transaction nodes are detected by ranking each node with its inter/intra-community link outlier value. By conducting experiments on a subset of bitcoin transactions, it shows that the proposed method is able to effectively detect known abnormal nodes involved in financial crimes.

**Keywords:** Outlier · Abnormal detection · Bitcoin · Transaction

## 1 Introduction

With the raise of blockchain-based digital currencies such as bitcoin, there is also a rapid increase of financial crimes associated with it because of its anonymity. The main reason is the pseudo anonymous provided by the underlying blockchain technology, i.e. the public key addresses used for transactions are associated with the real users. In order to identify the controllers of the financial crimes, it is not enough to determine the communities that involve in the financial crimes, it also requires to identify the core nodes in the communities that are more likely to control the transactions inter/intra the communities, i.e. the abnormal transaction nodes.

In order to detect abnormal transaction nodes, many researchers try to de-anonymize the public key address using heuristic methods or external information such as websites, forums and IP addresses [6–8, 10, 13, 14]. Furthermore, some researchers take a step forward to further identify the abnormal transaction nodes [1, 3–5, 11]. Hirshman et al. propose a unsupervised learning method



to detecting anomalous behavior in the bitcoin transaction network based on k-means and RolX [9]. Meiklejohn et al. perform an empirical studies on detecting transaction nodes involved in crimes [10]. Pham et al. propose an anomaly detection approach in bitcoin network based on three different unsupervised learning techniques [12]. Cai et al. proposes a minimal weighted infrequent itemset mining-based outlier detection approach for uncertain data stream [2].

Because gambling, money laundering, and fraud account only contribute to a very low proportion of all transaction data, the crime nodes we focus on are undoubtedly outliers when comparing to the large amount of normal transaction nodes. The ideal behind the algorithm is the assumption that people tend to frequently use their known and preferred services, and only have digital currency transaction with a fixed number of service providers. We believe that these behaviors also exist in the bitcoin network. Thus, we design the abnormal transaction node detection algorithm based on outlier identification technology. According to the experimental results, the proposed abnormal transaction node detection algorithm can effectively detect known abnormal nodes involved in financial crimes.

## 2 Abnormal Transaction Node Detection

Firstly, if we view all transactions as a network, the user transaction graph represents a social network with many communities. We believe that users with a prominent number of inter-community connections compared to other users are the active nodes in the transaction network, which are more likely to be the core nodes involving illegal activities, such as gambling, money launder, and so on. Secondly, from the perspective of the abnormal transaction community, it can be found that the users with more inter-community connections are more likely to be the organizers of the abnormal transaction community as well as the internal contacts. In other words, these users are the backbones of the criminal network.

Consequently, the first step of abnormal transaction node detection is to divide the user transaction graph into connected smaller communities (sub-graphs) which are disjoint with each other. There are many graph partition algorithms that can be used for such purpose. So we choose a widely-used classic community discovery algorithm Louvain, which has been integrated in the GraphX library of the Apache Spark data analytic platform [15] and is very efficient for processing large-scale graphs. For the convenient of discussion, let us denote the communities obtained by the Louvain algorithm as the set  $\mathcal{C} = \{C_1, C_2, \dots, C_k\}$ .

According to the affect of communities in the network topology, the features of the inter-community and intra-community links can be utilized to discover the nodes of abnormal transaction behavior in a community. These nodes are mainly organizers and major participants of illegal activities. Consequently, these abnormal users identified by our algorithm provide a reference for the regulatory agency of crypt digital currency.

## 2.1 Inter-community Link Based Outlier Detection

**Definition 1.** (*Outlier list*) The outlier list is a collection of triples constituted by a node, outlier rank of the node and total amount of money transfer through the node.

$$Outlierlist = \{(v, OR, value) \mid v \in V, OR \in [0, 1]\}, \quad (1)$$

where  $v$  is a node,  $V$  is the node set of the current community,  $OR$  is the outlier rank, and  $value$  is the total amount of money transferred through the node.

For a set of community  $\mathcal{C} = \{C_1, C_2, \dots, C_k\}$ , an algorithm for identify outliers by the inter-community outlier rank  $OR_1$  is described as follows:

(1) The Eq. (2) is used calculate the mean inter-community outlier rank  $m_k$  for all user nodes within a community  $C_k$ :

$$m_k = \frac{\sum_{u_i \in C_k} \sum_{u_j \in C_k (i \neq j)} |Count(u_i) - Count(u_j)|}{2n_{C_k}}, \quad (2)$$

$u_i$  represents a user node in community,  $C_k$  represents a community,  $n_{C_k} = |C_k|$  is the number of nodes in  $C_k$ , and  $Count(u_i)$  represents the number of communities that have connection with the user  $u_i$  in the user transaction graph.

(2) Traverse all nodes in the community  $C_k$ , and use the Eq. (3) to calculate the inter-community outlier rank  $OR_1$  for each node:

$$OR_1(u_i) = \frac{\sum_{u_j (j \neq i)} f(u_i, u_j)}{n_{C_k}}, \quad (3)$$

where  $n_{C_k} = |C_k|$  and  $f(u_i, u_j)$  is a judgment function defined as the following Eq. (4):

$$f(u_i, u_j) = \begin{cases} 0, & \text{if } |Count(u_i) - Count(u_j)| \leq 2m_k \\ 1, & \text{otherwise.} \end{cases} \quad (4)$$

(3) Get a set of nodes and inter-community outlier rank pairs  $Outlierlist_1 = \{(v, OR_1(v)) \mid v \in V, OR_1(v) \in [0, 1]\}$ .

## 2.2 Intra-community Link Based Outlier Detection

The algorithm proposed above is based on the inter-community links of the nodes, which ignores links between nodes within a community. However, some abnormal nodes may not be responsible for “external contact” but for “internal control”, which are mainly concern about only intra-community links. For example, in a money laundering or gambling community, these nodes are also central nodes which belong to a criminal group. In order to determine the possibility of a node being a such outlier, we define the intra-community outlier rank  $OR_2(v)$  for a node  $v$  in community  $C_k$  as the page rank value of  $v$  in the graph  $C_k$ .

The above algorithm simply treats each community as a subgraph. The importance (i.e. outlier rank) of each node is computed by PageRank algorithm on the subgraph that the node belongs to. After performing the above algorithm on all communities, each node gets a intra-community outlier rank that is a value in the interval  $[0, 1]$ .

---

**Algorithm 1:** Intra-community outlier rank
 

---

**Input:**  $C_k$ : a set of nodes  
**Output:**  $OV$ : a set of nodes with intra-community outlier ranks

- 1 Construct a subgraph  $G_{C_k}$  based on  $C_k$ ;
- 2 **if** *The edge set in  $G_{C_k}$  is not empty* **then**
- 3     Compute page rank value  $OR_2(v)$  for each node  $v$  in  $G_{C_k}$  based on PageRank algorithm;
- 4     **for**  $v \in C_k$  **do**
- 5         |  $OV = OV \cup \{(v, OR_2(v))\}$ ;
- 6 **return**  $OV$ ;

---

### 2.3 Outliers Weighting

In order to reflect the overall outlier rank of a node, we define the following weighted outlier rank  $OR$ .

$$OR(v) = \begin{cases} OR_1(v), & OR_1(v) > t \\ OR_2(v), & OR_2(v) > t \\ \alpha \cdot OR_1(v) + \beta \cdot OR_2(v), & \text{otherwise.} \end{cases} \quad (5)$$

Here  $t$  is a threshold value, which is set to be 0.95 based on experimental results.  $\alpha$  and  $\beta$  are the weights of the outliers ranks  $OR_1$  and  $OR_2$ , which satisfy that  $0 \leq \alpha, \beta \leq 1$  and  $\alpha + \beta = 1$ . During experiments, we observe that the influence of the  $OR_1$  value on the measurement of the abnormal node is greater than that of the  $OR_2$  value. Thus,  $\alpha$  and  $\beta$  are set to 0.6 and 0.4 in this paper.

Based on the Eq. (4), the weighted outlier rank of each node can be calculated based on its inter-community outlier rank  $OR_1$  and intra-community outlier rank  $OR_2$ . Hence, from the two sets  $Outlierlist_1$  and  $Outlierlist_2$ , we can obtain a set of nodes and weighted outlier ranks pair  $Outlierlist$ .

### 2.4 Node Filtering

In general, the nodes involving in illegal activities such as gambling and money laundering usually have a large amount of transactions. Hence, we can focus on these nodes to improve the efficiency of anomaly detection. So an addition node filtering process can be added before sorting nodes by their outlier rank to filter out nodes, when transaction amount is less than a specific value.

Firstly, in order to reflect the true value of bitcoin, the unit of transaction amount is converted from ‘‘cong’’ into ‘‘US dollar’’ based on the bitcoin exchange rate at the time of transaction. Secondly, the triples in  $Outlierlist$  whose transaction amounts are less than the threshold value  $s$  are filtered out. Thirdly, the remaining triples are sorted by the outlier rank  $OR$  in descending order.

Based on the above properties, the abnormal transaction node detection algorithm is designed as the following Algorithm 2.

---

**Algorithm 2:** Abnormal transaction node detection
 

---

**Input:**  $G$ : a user graph

**Output:**  $OR'$ : a list of abnormal nodes

- 1 Using the Louvain algorithm to identify communities  $C = \{C_1, C_2, \dots, C_k\}$  in the user transaction graph  $G$ ;
  - 2  $OR_1 := \text{IntraR}(C)$ ;
  - 3  $OR_2 := \text{InterR}(C)$ ;
  - 4  $OR := \text{WR}(OR_1, OR_2)$ ;
  - 5  $OR' = \text{Filter}(OR)$ ;
  - 6 **return**  $OR'$ ;
- 

### 3 Experiments and Evaluations

#### 3.1 Experimental Setup

The proposed algorithms are implemented in Python 3 to evaluate their effectiveness. The environment for conducting all experiments is a workstation with Intel(R) Core(TM) i7-8700 CPU @3.20GHz, 32GB memory and Windows 7 64 bit operation system.

In order to evaluate the proposed abnormal detection algorithm, we construct two datasets based on two carefully chosen one-month transaction data of bitcoin blockchain from 2012 and 2013. The first dataset is the BC2012 dataset, which contains all transaction data from September 1 to October 1, 2012 in bitcoin. There are 360,766 nodes (public key addresses) and 1,097,885 edges (transactions) in the BC2012 dataset. The second dataset is the BC2013 dataset, which contains transaction data from May 1 to May 31, 2013 in bitcoin. There are 823,688 nodes and 2,242,622 edges in the BC2013 dataset. In order to make these two dataset suitable for abnormal transaction node detection, we select the two one-month intervals based on whether they contain as many as possible nodes that are known to be involved in illegal activities.

The experiments of the proposed abnormal transaction node detection algorithm is performed on both BC2012 and BC2013 datasets to evaluate its effectiveness.

#### 3.2 Evaluation of Abnormal Transaction Node Detection

Our abnormal transaction node detection algorithm is used to calculate the outliers rank of nodes in the whole transaction graph of BC2012-5 dataset. The outlier ranks and annotations of the top-10 nodes are listed in Table 1. It shows that there are two exchange nodes, one coinbase node, four gambling related nodes, and one money laundering node among the top-10 nodes. Furthermore, we find that the gambling related nodes do not belong to participant of gambling, whereas they belong to the organizers of the gambling websites. The algorithm also detects a known node which belongs to a money laundering site. Additionally, we find two hidden nodes that have yet been annotated as abnormal on the Internet.

**Table 1.** Top-10 abnormal transaction nodes

No.	User ID	Outlier	Amount of transaction	Label
1	162	0.999513	278.75	Exchange
2	1389	0.999513	336.49	
3	123	0.999139	50868.16	Gambling
4	1284	0.999139	320.48	
5	2842	0.999139	7323.62	Gambling
6	6676	0.999139	175.52	Gambling
7	306	0.999134	4415.78	Gambling
8	562	0.999082	40918.57	Coinbase
9	540	0.999082	5959.30	Money laundering
10	341	0.999081	4003.94	Exchange

Especially, the distributions of abnormal transaction nodes identified by the abnormal transaction node detection algorithm varies for different types of communities. In the coinbase community, only one abnormal transaction node is identified. However, there are many abnormal transaction nodes in gambling community and exchange community, which is consistent with the fact that coinbase community is a normal community, but gambling community and money laundering network usually contain a large number of abnormal nodes. This indicates that our algorithm can effectively distinguish nodes in normal communities and abnormal nodes in abnormal communities.

As is known to all, money laundering nodes are the most difficult to detect because its behavior patterns are relatively hard to distinguish with normal transactions'. The results verify that our algorithm can effectively detect money laundering nodes using 10 days transaction data in BC2012 and BC2012 respectively with 5 known addresses that provide money laundering services. The experimental results are listed in Table 2, which indicate that our algorithm identifies 4 money laundering nodes and their outlier rank are particularly high. Although the algorithm does not identify all 5 money laundering nodes, it still demonstrates the capability of the algorithm.

**Table 2.** Detection results of money laundering websites

No.	User ID	Outlier	Amount of Transaction	Year
9	412	0.999982	7987.30	2012
100	624	0.999977	1203.13	2012
24	523	0.999995	1308.92	2013
138	121	0.999983	5469.90	2013

Then we evaluate the abnormal transaction node detection algorithm in a gambling community. The outlier ranks and annotations of nodes in the com-

munity are listed in Table 3. Because of the existence of a value greater than 0.95 of the original two outliers, three of the top-6 nodes with higher outliers ranks are retained ; the nodes of ranking 3-6 are the higher user nodes weighted by the outliers. Table 8 verifies that the node 1078 belongs to a gambling website and the node 2643 is a major player in the gambling community, whose total money transaction is \$20342.453 over 10 days period. Moreover, we detect some abnormal nodes without known annotations, such as node 483, the 5th node.

**Table 3.** Outliers ranked top 6 in a gambling community

No.	ID	Public key address	Outlier	Node type
1	645	1dice8EMZmqKvrGE4Qc9bUFf9PX3xaYDp	0.998	Gambling website
2	648	1dice97ECuByXAvqXpaYzSaQuPVvrtmz6	0.972	Gambling website
3	376	1dice5wwEZT2u6ESAdUGG6MHgCpbQqZiy	0.965	Gambling website
4	1078	1dice6DPtUMBpWgv8i4pG8HMjXv9qDJWN	0.902	Gambling website
5	483	1bankCWEi5gaNPxkw2qPsm6GgF42XaG8K	0.865	-
6	2643	1gKof8dNAoztQQfad1HAHwYup8GTPbMU1	0.604	Gambling participant

## 4 Conclusion

The main contributions of this paper lie in an abnormal transaction node detection algorithm for recognizing the major participants with suspicious transaction communities. The community based ranking are utilized to effectively identify abnormal nodes in financial transactions with incomplete user information and unpredictable abnormal types and features. The abnormal transaction nodes are identified based on outlier detection on graphs, which provides a possible solution for financial crime regulation on blockchain-based crypt currency such as bitcoin. By applying public key addresses merging and community discovery algorithms on the bitcoin blockchain, suspicious communities that are possibly involved illegal activities are clustered and can be used as input for abnormal transaction node detection, which identifies nodes with high outlier ranks in the whole user transaction graph. The experiments on the BC2012 and BC2013 dataset show that the proposed algorithm is effectiveness for detecting core node in communities involving in financial crimes.

## References

1. Akoglu, L., Tong, H., Koutra, D.: Graph based anomaly detection and description: A survey. *Data Mining Knowl. Discov.* **29**(3), 626–688 (2015)
2. Cai, S., Sun, R., Hao, S., Li, S., Yuan, G.: Minimal weighted infrequent itemset mining-based outlier detection approach on uncertain data stream. In: *Neural Computing and Applications*, pp. 1–21 (2018)
3. Chandola, V., Banerjee, A., Kumar, V.: Anomaly detection for discrete sequences: A survey. *IEEE Trans. Knowl. Data Engin.* **24**(5), 823–839 (2012)

4. Christin, N.: Traveling the silk road: A measurement analysis of a large anonymous online marketplace. In: Proceedings of the 22nd International Conference on World Wide Web, pp. 356–362 (2013)
5. Deters, R.: How to detect and contain suspicious transactions in distributed ledgers. In: SmartBlock, pp. 149–158. Springer, Cham (2018)
6. Eshghi, A., Kargari, M.: Introducing a new method for the fusion of fraud evidence in banking transactions with regards to uncertainty. *Expert Syst. Appl.* **121**, 382–392 (2015)
7. Fleder, M., Kester, Michael, S., Pillai, S.: Bitcoin transaction graph analysis. *Comput. Sci.* 102–105 (2015)
8. Gao, S., Xu, D.: Conceptual modeling and development of an intelligent agent-assisted decision support system for anti-money laundering. *Expert Syst. Appl.* **36**(2), 1493–1504 (2009)
9. Hirshman, J., Huang, Y., Macke, S.: Unsupervised approaches to detecting anomalous behavior in the bitcoin transaction network. In: 2016 Information Security for South Africa (ISSA) (2013)
10. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S.: A fistful of bitcoins: Characterizing payments among men with no names. In: Proceedings of the 2013 Conference on Internet Measurement Conference, pp. 127–140. ACM (2013)
11. Möser, M., Böhme, R., Breuker, D.: An inquiry into money laundering tools in the bitcoin ecosystem. In: eCrime Researchers Summit (eCRS), pp. 34–36. San Francisco, CA, USA (2013)
12. Pham, T., Lee, S.: Anomaly detection in bitcoin network using unsupervised learning methods. [arXiv:1611.03941](https://arxiv.org/abs/1611.03941) (2017)
13. Reid, F., Harrigan, M.: An analysis of anonymity in the bitcoin system. In: IEEE Third International Conference on Privacy and Security, pp. 16–20. Amsterdam, Netherlands (2012)
14. Ron, D., Shamir, A.: Quantitative analysis of the full bitcoin transaction graph. In: International Conference on Financial Cryptography and Data Security, vol. 16, pp. 6–24. Springer (2013)
15. Zaharia, M., Chowdhury, M., Franklin, M.J., Shenker, S., Stoica, I.: Spark: Cluster computing with working sets. In: Proceedings of the 2Nd USENIX Conference on Hot Topics in Cloud Computing, HotCloud’10, pp. 10–10. USENIX Association, Berkeley, CA, USA (2010)



# A Review of Visual SLAM Algorithms for Fusion of Point-Line Features

Yong Qing<sup>1,2</sup>(✉) and Haidong Yu<sup>1,2</sup>

<sup>1</sup> College of Automation, Guangxi University of Science and Technology, Guangxi, China  
757255401@qq.com

<sup>2</sup> Department of Artificial Intelligence and Manufacturing, Hechi University, Guangxi, China

**Abstract.** SLAM (hereinafter referred to as SLAM) refers to the autonomous mobile carrier in the unknown environment, through the data information obtained by its own sensor to achieve its own positioning, in addition to the technology can also continuously build and update the map in the process of carrier movement. Visual SLAM is a technology that uses visual sensors as input and uses dense perception of the surrounding environment to achieve SLAM function. Compared with the traditional SLAM method, visual SLAM can retain the semantic information in the environment while ensuring the accuracy, so as to expand the function of the carrier. This paper first introduces the milestone methods in the field of visual SLAM in chronological order, then introduces the standard flow of visual SLAM, and finally introduces the advantages and several typical excellent algorithms of visual SLAM that integrates point-and-line features.

**Keywords:** Visual SLAM · Point-and-line features

## 1 Introduction

As autonomous driving technology continues to evolve, its requirements for positioning accuracy and environmental awareness are also increasing [1, 2]. The traditional global satellite navigation systems have limitations in providing high-precision positioning and cannot offer accurate environmental perception for robots. However, the localization and mapping technique known as SLAM utilizes sensors installed on vehicles to gather data and utilize that data to determine the vehicle's position. SLAM technology holds great potential in the field of autonomous driving as it enables vehicles to achieve high-precision positioning and environmental perception capabilities. In recent years, there has been significant attention given to the research outcomes of SLAM algorithms, indicating a strong interest in the widespread application of SLAM in autonomous driving and other domains [3, 4]. SLAM refers to the process of accurately localizing a mobile device equipped with sensors in an unfamiliar environment while simultaneously creating a comprehensive map of its surroundings. The term originally originated in the robot community, but with the advent of autonomous driving, SLAM technology that can perfectly adapt to it has also received attention from researchers. This is because SLAM can provide more accurate positioning services than traditional GPS, and it can



also build a rich road database for car navigation systems to adapt to the growing trend of autonomous driving. Laser SLAM as a technology was proposed in the early development of SLAM, after years of development and continuous improvement, the research on laser SLAM has reached a high level of maturity. However, due to the limitation of laser SLAM itself, the radar data is distorted when the mobile carrier moves fast, and the accuracy of SLAM is reduced.

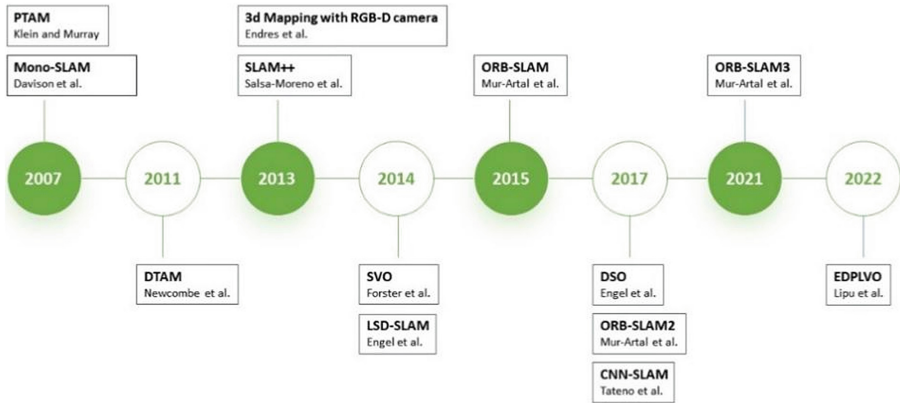
Compared with laser SLAM, which requires active signaling, visual SLAM realizes positioning and map construction through visual dense perception of the environment, which enables visual SLAM to avoid the defects of laser SLAM. In addition, visual SLAM has the advantage of preserving map semantic information. In addition, from the perspective of sensor cost, the cost of camera is generally lower than that of LiDAR, which makes visual SLAM more and more valued by researchers. Most classical visual SLAM algorithms are designed with the assumption of a static environment, but in the actual environment, there will inevitably be dynamic changes. These dynamic changes often have unpredictable characteristics, which makes it difficult to construct effective constraints on them. In addition, these dynamic changes can also cause the static part of the original to be covered. Effectively addressing dynamic changes in the real environment is a pressing challenge in visual SLAM. Additionally, environments with limited texture information or repetitive textures can further complicate visual SLAM matching, leading to unstable optimization calculations.

## 2 History of Visual SLAM Development

In 2007, Davison et al. first proposed a real-time monocular visual SLAM system: Mono-SLAM, which successfully applied the SFM method to SLAM. Mono-SLAM provides solutions for active mapping and measurement, using a universal model for smooth camera motion, and monocular feature initialization and feature orientation estimation. In the same year, Klein et al. proposed the PTAM algorithm, a keyframe-based monocular visual SLAM algorithm, which divides the SLAM system into two parallel threads: tracking and mapping. This mode has been widely recognized by researchers for its effective reduction of computing costs. In 2011, inheriting the dual-threaded parallel mode of PTAM, Newcombe et al. introduced DTAM, a SLAM system that utilizes a single RGB camera for real-time dense positioning and tracking, which maintains a dense mapping of key frames. But like most direct SLAM, DTAM requires high hardware costs to run in real time. In 2013, Endres et al. proposed a visual SLAM method that uses RGB-D cameras to generate high-precision 3D maps. This method has low hardware requirements, but the system and its robustness is limited, making it challenging to handle complex environments. In the same year, Salas-Moreno et al. proposed an object-oriented 3D SLAM framework: SLAM++. By leveraging prior semantic information of 3D objects, the system effectively reduces the amount of data to be processed, resulting in improved processing efficiency.

At present, the research on the overall framework of visual SLAM has been very mature, and the multi-threaded parallel mode is considered to be the optimal solution at present, and researchers primarily focus on enhancing the accuracy and robustness of the system as their main priority. In 2014, Forster et al. proposed a Semi-direct

monocular Visual SLAM algorithm: semi-direct Visual Odometry (SVO for short) Semi-direct method is to obtain camera pose by directly matching feature points in images. In the same year, Engel et al. proposed a monocular camera-based direct visual SLAM algorithm (LSD-SLAM). LSD-SLAM does not use key points, but directly operates on image intensity, and allows the construction of large-scale and consistent environment maps. However, the initialization calculation of LSD-SLAM is complex. In terms of feature point method, Mur-Artal et al. proposed a monocular camera-based visual SLAM algorithm (ORB-SLAM) in 2013 [5]. ORB-SLAM utilizes ORB features and leverages feature matching and relocalization of ORB descriptor points, providing improved view invariance compared to PTAM. Additionally, the algorithm efficiently handles feature matching for newly detected 3D points, enabling timely expansion of the scene. The timeliness of scene expansion plays a crucial role in ensuring stable tracking of subsequent frames. ORB-SLAM also incorporates a closed-loop detection module to eliminate error accumulation. In 2017, Mur-Artal et al. expanded the framework and named it ORB-SLAM2, the biggest change from the previous generation is that the ORB-SLAM2 supports both monocular, stereoscopic and RGB-D cameras. Of course, like most feature point visual SLAM methods, the Mur-Artal et al. 's method can have good performance and accuracy in well-textured environments, but it is still difficult to maintain its performance in the absence of texture or repeated scenes. In addition, the latest version of the method, ORB-SLAM3, has been released in 2021, and ORB-SLAM3 [6] supports the integration of vision and IMU while supporting various cameras, further improving the robustness of the algorithm itself. In 2022, the EDPLVO [7] proposed by Lipu et al., by extending the direct method to line features, significantly reduces the number of variables to speed up optimization (Fig. 1).



**Fig. 1.** Historical milestone in the development of visual SLAM.

### 3 Standard Flow of Visual SLAM System

A complete standard visual SLAM system [8] typically consists of the following five parts:

**Input:** Collect camera images and preprocess the collected image information according to the subsequent work requirements of the system.

**Front-end (visual odometer):** Using camera images captured within a short time-frame, the front end of the SLAM system estimates the camera’s pose (position and attitude) in the mobile robot’s coordinate system. Simultaneously, it constructs a local map. The primary techniques employed in the front end include the feature-based method (indirect method) and the direct method.

**Back end:** In the back end of the SLAM system, the camera poses calculated by the visual odometry, along with the 3D map points and loop detection information, are used for global optimization of both the pose and the 3D map points.

**Loop detection:** By detecting loops and determining if the robot has returned to a previous position, the system can utilize these loop closures as constraints to effectively mitigate accumulated errors in the trajectory estimation.

**Mapping:** Using the estimated trajectory as a foundation, generate a map that aligns with the specific requirements of the mission (Fig. 2).

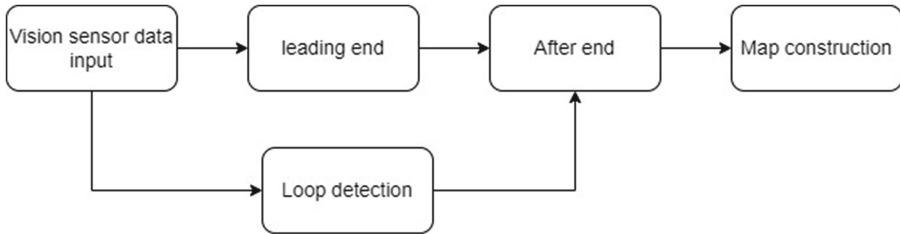


Fig. 2. Visual SLAM standard flow chart.

At present, the application scenarios of visual SLAM mainly fall into three categories: high-precision positioning of autonomous driving, autonomous mobile robots, and three-dimensional reconstruction of indoor scenes. In different scenarios, the requirements for algorithm accuracy, computing resources and computing speed are different. Appropriate algorithms should be selected for different scenarios.

### 4 Visual SLAM Algorithm for Fusion of Point-Line Features

Currently, to ensure high accuracy, mainstream visual SLAM methods predominantly rely on nonlinear optimization techniques. While these methods offer improved precision compared to traditional filter-based approaches, they also demand greater computational resources. As mentioned earlier, visual SLAM can be divided into direct and indirect methods. Point features are one of the most commonly used features in feature-based indirect methods, because they have the advantages of simple structure

and easy establishment of constraints. Therefore, indirect method is also called feature point method. Corner points are the most representative feature points, which have the advantages of simple structure, easy extraction and matching. Nevertheless, feature-point based visual SLAM methods heavily rely on the quality and quantity of point features, which can become a limitation in certain scenarios. In environments with limited texture information or repetitive and similar textures like corridors, windows, and white walls, extracting an adequate number of point features becomes challenging. The challenges in feature extraction significantly impact the accuracy and robustness of the SLAM system, sometimes leading to failure. Factors such as fast camera motion and changes in lighting conditions can cause a significant decrease in the number of accurate point feature matches.

**Table 1.** Several excellent visual SLAM algorithms for fusion of point-line features are introduced.

Presenter	Time	Improvement
Vakhitov et al. [9]	2016	The EPnPL and OPnPL algorithms based on the combination of point and line features are proposed
Zuo et al. [10]	2017	Line features are represented by Prucker coordinates and parameterized line features are represented by minimum orthogonal
Pumarola et al. [11]	2017	A method of system initialization using line features is proposed
Gomez-Ojeda et al. [12]	2019	For the first time open source binocular based point-and-line feature SLAM method
He et al. [13]	2018	Line features are introduced in point feature-based visual inertial system
Wang et al. [14]	2018	The Angle of the line is also added to the construction of the reprojection error of the line feature
Gome-Ojeda et al. [17]	2018	A method based on geometric constraints to construct minimum L1 norm is proposed for line feature matching in binocular image sequences with high dynamic range
Zhou et al. [7]	2022	The line feature is extended to the direct method

Therefore, although point is the most commonly used environment representation method in visual SLAM, representation methods such as line, plane, and even object can provide richer map representation, which is more suitable for the work requirements of dynamic SLAM. Embedding the task of dynamic object detection into SLAM algorithms is crucial and challenging, as it holds significant importance in the context of autonomous driving. The workflow of existing visual SLAM algorithms embedded with dynamic object detection is divided into two stages: First, the dynamic object needs to be segmented, tracked, and its pose estimated, and then this information is used to estimate the state in a probabilistic framework. The detection and segmentation of

dynamic objects has enabled precise solutions in real time. The existing visual SLAM algorithm embedded with dynamic target detection has the problem that its front-end cannot provide reliable attitude information. Therefore, in order to improve the performance of point-feature SLAM, more and more attention has been paid to the use of linear features in SLAM systems. Line features are more abundant in artificial environment and more robust to illumination changes. The integration of point-line features in the SLAM system can enhance feature extraction in environments with weak texture, thereby increasing the overall number of extracted features. Table 1 briefly introduces several kinds of visual SLAM that fuse point and line features.

## 5 Epilogue

An integrated visual SLAM method that incorporates point-line features is proposed, which introduces linear geometric constraints to match line features across different image frames. This method offers several advantages. Firstly, it significantly reduces the computational load involved in feature matching. Secondly, it extracts point features for key frames and utilizes these features to match specific points and edge points within the image region. This approach enhances the accuracy of matching, resulting in a visual SLAM system with improved positioning accuracy. Especially for the scene with uneven light and weak texture, the positioning accuracy and operation speed can be improved, which is an excellent scheme for optimizing visual SLAM system at present, and has a good application prospect and research value. Further investigation and research into visual SLAM systems based on point-and-line features hold great potential and merit.

**Funding Statement:** The authors are highly thankful to the Natural Science Foundation of Guangxi Province (NO. 2023GXNSFAA026025), the National Natural Science Foundation of China (NO. 62063006), to the Innovation Fund of Chinese Universities Industry-University-Research (ID: 2021RYC06005), to the Research Project for Young and Middle-aged Teachers in Guangxi Universities (ID: 2020KY15013), and to the Special research project of Hechi University (ID: 2021GCC028). This research was financially supported by the project of outstanding thousand young teachers' training in higher education institutions of Guangxi, Guangxi Colleges and Universities Key Laboratory of AI and Information Processing (Hechi University), Education Department of Guangxi Zhuang Autonomous Region.

## References

1. Kong, X., Gao, H., Shen, G., et al.: Fedvcp: a federated-learning-based cooperative positioning scheme for social internet of vehicles. *IEEE Trans. Comput. Soc. Syst.* **9**(1), 197–206 (2021)
2. Lu, H., Zhu, Y., Yuan, Y., et al.: Social signal-driven knowledge automation: a focus on social transportation. *IEEE Trans. Comput. Soc. Syst.* **8**(3), 737–753 (2021)
3. Qin, T., Li, P., Shen, S.: Vins-mono: a robust and versatile monocular visual-inertial state estimator. *IEEE Trans. Rob.* **34**(4), 1004–1020 (2018)
4. Shao, W., Vijayarangan, S., Li, C., et al.: Stereo visual inertial lidar simultaneous localization and mapping. In: *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE, pp. 370–377 (2019)
5. Mur-Artal, R., Montiel, J.M.M., Tardos, J.D.: ORB-SLAM: a versatile and accurate monocular SLAM system. *IEEE Trans. Rob.* **31**(5), 1147–1163 (2015)
6. Campos, C., Elvira, R., Rodríguez, J.J.G., et al.: ORB-SLAM3: an accurate open-source library for visual, visual-inertial, and multimap slam. *IEEE Trans. Rob.* **37**(6), 1874–1890 (2021)
7. Zhou, L., Huang, G., Mao, Y., et al.: EDPLVO: efficient direct point-line visual odometry. In: *2022 International Conference on Robotics and Automation (ICRA)*, pp. 7559–7565. IEEE (2022)
8. Li, R., Wang, S., Gu, D.: Ongoing evolution of visual SLAM from geometry to deep learning: challenges and opportunities. *Cogn. Comput.* **10**, 875–889 (2018)
9. Vakhitov, A., Funke, J., Moreno-Noguer, F.: Accurate and linear time pose estimation from points and lines. In: *Computer Vision–ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, October 11–14, 2016, Proceedings, Part VII*, pp. 583–599. Springer International Publishing, Cham (2016)
10. Zuo, X., Xie, X., Liu, Y., et al.: Robust visual SLAM with point and line features. In: *2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pp. 1775–1782. IEEE (2017)
11. Pumarola, A., Vakhitov, A., Agudo, A., et al.: PL-SLAM: Real-time monocular visual SLAM with points and lines. In: *2017 IEEE International Conference on Robotics and Automation (ICRA)*, pp. 4503–4508. IEEE (2017)
12. Gomez-Ojeda, R., Moreno, F.A., Zuniga-Noël, D., et al.: PL-SLAM: a stereo SLAM system through the combination of points and line segments. *IEEE Trans. Rob.* **35**(3), 734–746 (2019)
13. He, Y., Zhao, J., Guo, Y., et al.: Pl-vio: tightly-coupled monocular visual-inertial odometry using point and line features. *Sensors* **18**(4), 1159 (2018)
14. Wang, R., Di, K., Wan, W., et al.: Improved point-line feature based visual SLAM method for indoor scenes. *Sensors* **18**(10), 3559 (2018)
15. Gomez-Ojeda, R., Gonzalez-Jimenez, J.: Geometric-based line segment tracking for HDR stereo sequences. In: *2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pp. 69–74. IEEE (2018)



# Prediction of Self-rated Health of Older Adults by Network Services Based on Agent Simulation and XGBoost Algorithm

Yue Li, Xinyue Hu, Yang Li, Chengmeng Zhang, and Gong Chen<sup>(✉)</sup>

Institute of Population Research, Peking University, Beijing 100871, China  
chengong@pku.edu.cn

**Abstract.** As the aging population grows, health issues have attracted widespread attention, especially among older adults. We explored the effects and simulation prediction of network services based on a multi-dimensional analysis of the health status of older adults, which could help older adults to better manage and evaluate their health. The study was conducted as follows. Based on the China Family Panel Studies (CFPS) data, a chi-square test was used to screen out 16 indicators with significant effects on the self-rated health (SRH) of older adults. To eliminate selection bias between samples, a propensity score matching (PSM) was used to explore the potential impact of network services on SRH of older adults. A multi-agent simulation model was constructed to examine SRH effects and then compare the health both before and after using network services based on the AnyLogic platform. The XGBoost algorithm was used to build a prediction model for assessing SRH of older adults. The experimental results show that network services have a positive effect on SRH of older adults using the multiple PSM methods, improving SRH of older adults by 14.1%. Meanwhile, the multi-agent simulation proves that network services can improve the health status of older adults. It also proves that the XGBoost algorithm has better accuracy, specificity, and running time than the other compared algorithms, and can meet the prediction needs of this paper. This study may enrich and expand the theoretical framework of health influence mechanism and simulation prediction studies.

**Keywords:** Self-rated health · Agent simulation · XGBoost algorithm · Network services

## 1 Introduction

China has entered an aging society, and the degree of aging is continuously deepening. The National Health Commission pointed out that China's aging population presents a situation and characteristics of large quantity, fast speed, and significant differences. According to estimates, around 2035, the proportion of people aged 60 and above in the total population will exceed 30%, entering a stage of severe aging [1]. Aging itself is the result of social development and the health development of residents. It has brought opportunities to our country but also posed significant challenges to elderly care, medical

services, and social services. Among them, the health issues of older adults are one of the most prominent problems [2]. In this context, studying and understanding the health status of older adults, as well as the influencing factors and mechanisms, and conducting scientific simulation and prediction, have practical significance for promoting healthy aging in our country.

Research on measurement indicators of the health status of older adults shows that the self-rated health (SRH) can reflect the subjective and objective aspects of health status [3]. SRH is not only derived from internal physiological factors such as physical condition, and social adaptability, but also depends on the lifestyle and habits of older adults. It has high reliability and robustness in measuring health status [4, 5]. Previous studies have identified multiple influencing factors in health decision-making, including demographic factors, health-related lifestyles, and socioeconomic factors [6]. With the development of smart aging, the use of network services has become a social trend and is widely popular and applied among older adults [7]. Older adults can enjoy the convenience brought by information services, which not only reflects the development of smart aging but also has a certain impact on their health.

The process of influencing the health behavior is complex, resulting from the interaction of many subjects and factors. Even simple behavioral rules can form complex patterns at the macro level. Therefore, it is difficult to accurately describe the influencing process of SRH of older adults using the traditional and static research methods. An agent is a subject that exists in the environment. It can understand and analyze all the information and data obtained from the environment and output corresponding behavioral measures according to its own needs. Agent-based modeling (ABM) system, which consists of multiple agents in the same environment, focuses on studying the individual micro-level behaviors in the system and forms macro-level evolution phenomena [8]. ABM has strong reliability and efficiency in solving practical problems and is widely applied in sociology and economics fields.

On the other hand, the main purpose of predicting SRH of older adults is to identify the potential health level, providing reference for the health intervention. Machine learning typically follows non-linear and non-parametric methods instead of predefining the complexity of the model, enabling tasks such as clustering, classification, and prediction. They can serve as decision support tools for assessing the health status of older adults [9]. Common machine learning classification algorithms include K-nearest neighbor (KNN), decision tree (DT), random forest (RF), support vector machine (SVM), as well as gradient boosting decision tree (GBDT), adaptive boosting (AdaBoost), light gradient boosting machine (LightGBM), eXtreme gradient boosting (XGBoost). They can achieve good accuracy and interpretability when dealing with the complex problems compared to the statistical analysis methods.

This paper focuses on the mechanism and dynamic simulation prediction of the impact of network services on SRH of older adults, aiming to explore methods and pathways to improve the health status of older adults in the context of smart aging in China. The innovations of this paper include: establishing a long-term mechanism for the impact of network services on SRH of older adults, further exploring the dynamic process; selecting suitable algorithms to construct prediction models for identifying the health status of older adults, thus supporting the prediction and early warning of the health-related issues.



## 2 Methods

### 2.1 Data Acquisition and Analysis

The data source for this paper is the latest 2020 database of the China Family Panel Studies (CFPS), a nationwide, comprehensive social tracking survey organized by the China Social Science Research Center of Peking University. This data reflects China's social, economic, demographic, educational, and health changes, and provides a base for academic and policy research [10]. Health is one of the research topics that CFPS focuses on. Older adults aged 60 years and above were selected from the database as the study subjects. After removing the samples with missing values in the dependent and independent variables, the final valid sample of 3409 was obtained. Table 1 is compiled from the CFPS data.

**Table 1.** Variable setting.

Variables	Meanings	Descriptions	Variables	Meanings	Descriptions
Gender	Gender	Male = 1; Female = 2	Health	Health changes	Worse = 1; No change = 2; Better = 3
Age	Age	60 ~ 70 = 1; 70 ~ 80 = 2; 80 and above = 3	Chronic	Is there a chronic disease	Yes = 1; No = 2
Education	Education	Illiteracy = 1; Primary school = 2; Junior high school = 3; High school = 4; Junior college = 5; Bachelor's degree or above = 6	Medical	Where to see a doctor	Comprehensive hospital = 1; Specialized hospital = 2; Community Health Service Center = 3; Community Health Service Station = 4; Clinic = 5; I don't know = 6
Marriage	Marital status	Unmarried = 1; Married = 2; Cohabitation = 3; Divorce = 4; Widow = 5	Medicare	Medical insurance type	Public medical expenses = 1; Urban employee medical insurance = 2; Urban resident medical insurance = 3; Supplementary medical insurance = 4; New rural cooperative medical care = 5; Basic medical insurance = 6; None of the above = 7; I don't know = 8

(continued)

**Table 1.** (continued)

Variables	Meanings	Descriptions	Variables	Meanings	Descriptions
City	Urban and rural	Town = 1; Rural = 2	Exercise	Frequency of physical exercise	Less than once a month = 1; More than once a month, but less than once a week = 2; 1 ~ 2 times per week = 3; 3 ~ 4 times per week = 4; 5 or more times per week = 5; Once a day = 6; 2 or more times a day = 7; Never participate = 8
Soldier	Veterans or not	Yes = 1; No = 2	Smoke	Have you smoked in the past month	Yes = 1; No = 2
Religion	Religious or not	Yes = 1; No = 2	Drink	Have you consumed alcohol three times a week in the past month	Yes = 1; No = 2
Work	Working condition	Working = 1; Unemployment = 2; Exit from the labor market = 3	Read	Reading or not	Yes = 1; No = 2
Retirement	Whether to receive retirement	Yes = 1; No = 2	Network	Mobile internet access or not	Yes = 1; No = 2
Insurance	Whether to receive pension insurance	Yes = 1; No = 2	Computer	Whether computer access	Yes = 1; No = 2
Income	Last year's income	0 ~ 1000 = 1; 1000 ~ 2000 = 2; 2000 ~ 3000 = 3; 3000 ~ 4000 = 4; 4000 ~ 5000 = 5; 5000 and above = 6	SRH	Self-rated health	Unhealthy = 1; General = 2; Relatively healthy = 3; Quite healthy = 4; Very healthy = 5

The dependent variable is SRH, and the CFPS 2020 survey directly asked “How healthy do you think you are? Very healthy, quite healthy, relatively healthy, general, unhealthy”. In this paper, responses are assigned and reverse coded with unhealthy as 1, general as 2, relatively healthy as 3, quite healthy as 4, and very healthy as 5. The explanatory variables are classified into 5 dimensions. Basic personal information, including: gender, age, education, marriage, city, soldier, and religion; work status, including: work, retirement, insurance, and income; disease status, including: health, chronic, medical, and medicare; lifestyle habits, including: exercise, smoke, drink, and read; network services, including: mobile internet and computer access.

Both the dependent and independent variables are categorical variables, so the chi-square analysis test was used to study whether there is significant difference between categorical data (P values less than 0.05). Due to space limitations, only the basic information and network services are shown in Table 2. The chi-square analysis results for other modules are shown in Table 3.

From Tables 2 and 3, a total of 16 factors, are statistically significant and will be used for subsequent analysis of influence and predictive modeling. Gender: significant differences in SRH of older adults of different genders were observed, with male exhibiting

**Table 2.** Effects of different variables on SRH of older adults [n = 3409, percentage (%)].

Items	Features	Unhealthy	General	Relatively healthy	Quite healthy	Very healthy	$\chi^2$ values	P values
Gender	Male	20.7	16.9	38.4	11.9	12.1	51.900	< 0.001
	Female	31.2	16.4	33.3	10.1	9.0		
Age	60 ~ 70	24.8	16.6	36.1	11.3	11.2	13.734	0.089
	70 ~ 80	29.0	15.8	35.2	10.8	9.2		
	80 and above	24.1	22.8	35.4	8.2	9.5		
Education	Illiterate	33.2	18.2	26.8	10.8	11.1	148.878	< 0.001
	Primary school	24.4	17.0	37.6	10.5	10.5		
	Junior high school	20.2	13.2	43.4	12.0	11.3		
	High school	16.8	17.1	47.3	9.8	9.0		
	Junior college	10.8	13.8	56.9	16.9	1.5		
	Bachelor's degree or above	12.5	12.5	54.2	16.7	4.2		
Marriage	Unmarried	35.7	10.7	25.0	17.9	10.7	18.518	0.294
	Married	25.3	16.3	36.3	11.4	10.6		
	Cohabitation	27.3	9.1	54.5	9.1	0.0		
	Divorce	26.1	13.0	34.8	15.2	10.9		
	Widow	29.7	19.0	33.3	7.9	10.1		
City	Town	21.4	19.9	38.9	9.8	10.0	58.294	< 0.001
	Rural	30.3	13.7	33.0	12.0	11.0		
Soldier	Yes	18.2	13.6	50.0	18.2	0.0	5.262	0.261
	No	26.1	16.7	35.7	11.0	10.6		
Religion	Yes	16.0	22.1	39.7	10.7	11.5	8.466	0.076
	No	26.5	16.4	35.6	11.0	10.5		
Network	Yes	19.3	15.7	42.1	11.3	11.6	25.955	< 0.001
	No	27.8	16.9	34.2	10.9	10.2		
Computer	Yes	11.4	14.8	47.7	15.9	10.2	13.271	0.010
	No	26.5	16.7	35.5	10.9	10.5		

a more optimistic attitude towards their SRH than female. Education: significant differences with different educational backgrounds were observed, with those who received higher education exhibiting a more optimistic attitude towards their SRH than those with lower education levels. City: significant differences living in urban and rural areas were observed, with a lower proportion of urban older adults rating themselves as unhealthy compared to their rural counterparts. Network: significant differences with different mobile internet usage were observed, with those who used the internet exhibiting a more optimistic attitude towards their SRH than those who did not. Computer: significant differences with different computer usage were observed, with those who used computers exhibiting a more optimistic attitude towards their SRH than those who did not.

**Table 3.** Chi-square test results of other modules.

Items	$\chi^2$ values	P values	Items	$\chi^2$ values	P values
Work	69.014	< 0.001	Medical	60.967	< 0.001
Retirement	36.356	< 0.001	Medicare	77.141	< 0.001
Insurance	4.505	0.342	Exercise	75.647	< 0.001
Income	122.879	< 0.001	Smoke	30.931	< 0.001
Health	641.349	< 0.001	Drink	32.484	< 0.001
Chronic	362.948	< 0.001	Read	64.976	< 0.001

## 2.2 PSM-Based Impact of Network Services on SRH

To explore the relationship between network services and SRH of older adults, a treatment group (using network services) and a control group (not using network services) were established. This is a set of covariates  $x_i$  that will have an effect on  $y$  and  $x_1$ . To overcome endogeneity of samples due to self-selection bias and bidirectional causality, the propensity score matching (PSM) model was used to assess the impact of network services on SRH of older adults [11]. Assuming that  $y_{1i}$  is the health effect of the  $i$ th individual using the network services ( $D_i=1$ ) and  $y_{0i}$  is the health effect of the  $i$ th individual not using the network services ( $D_i=0$ ), then the health effect of older adults using network services is  $(y_{1i}-y_{0i})$ . Given the observable variable  $x_i$ , the conditional probability that individual  $i$  enters the treatment group is as in Eq. (1). ATT is obtained to measure the average treatment effect for the treated, which represents the difference between the observation results of individual  $i$  and its counterfactual, as in Eq. (2).

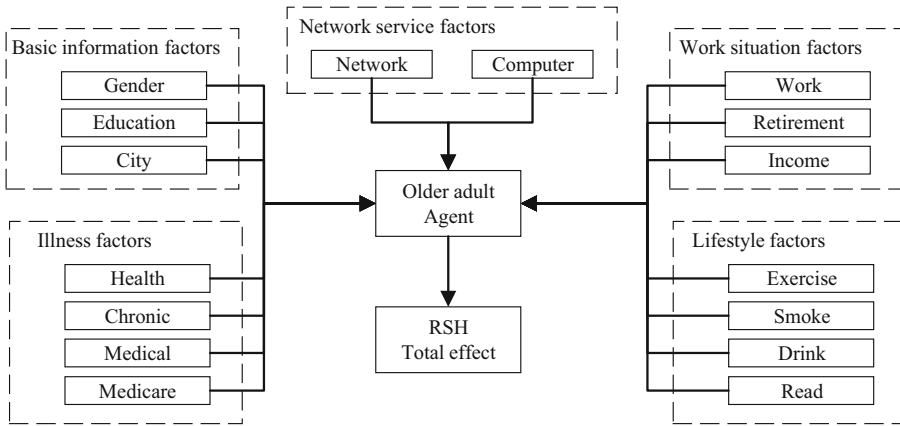
$$p(x_i) = \Pr(D_i = 1|x = x_i) = E(D_i|x_i) \quad (1)$$

$$ATT = E\{y_{1i} - y_{0i}|D_i = 1\} = E[E\{y_{1i} - y_{0i}|D_i = 1, p(x_i)\}] \quad (2)$$

## 2.3 Agent-Based Simulation of Network Services on SRH

The health status of older adults is not only limited by the network services, but also influenced by the external environment and the interactions between users, making the health behavior system of older adults complex. In this paper, the agent-based simulation was applied to analyze the dynamic changes of the impact of network services on the health status of older adults. In the simulation system, each person is an agent with autonomy, mobility, reactivity, and intelligence. Under the influence of network services, the health status of the population has undergone a transformation. The conceptual diagram of the agent-based health simulation is shown in Fig. 1.

According to the analysis results of sample data, the agent behavior rules and simulation process were designed based on the AnyLogic platform. The main steps include the following.



**Fig. 1.** Conceptual diagram of the agent-based health simulation for older adults.

Step 1: Set the agent system environment. The initial number of agents, attributes, and parameters were first set. The environment defines a set of shared properties of agents, and Anylogic will automatically create a certain number of agents within the environment.

Step 2: Set the characteristics and behaviors of agents based on the state diagram. The cross-correlation between the state diagrams were achieved by setting the state transition rate, which is the percentage of potential agents that need to use network services.

Step 3: Create the output chart. Define the functions of potential agents, set the parameters of the time line chart and display data items and formats. Function counting was used to show the number of agents with different health states under the influence of network services.

## 2.4 SRH Prediction for Older Adults Based on SMOTE and XGBoost

Traditional classification methods assume that the samples contained in each category are balanced, but in practical applications, class imbalance often exists. The number of SRH categories is 889, 567, 1220, 375, and 358, respectively. If classification algorithms are directly used for learning, the predicted results often have no practical value [12]. Synthetic minority oversampling technique (SMOTE) is an oversampling technique proposed by Chawla in 2002. The basic idea is to synthesize new samples by interpolating the minority classes with their neighbors, so that each minority class has the same number as the majority class [13]. SMOTE can effectively avoid overfitting and improve the generalization performance of the classifier on the test dataset. The main calculation process is as follows.

For each sample  $x_i$  in the minority class, calculate its Euclidean distance to all samples in the minority class to obtain its K-nearest neighbors.

Set a sampling ratio  $M$  according to the sample imbalance ratio. For each minority class sample  $x_i$ , select several samples at random from its K-nearest neighbors, assuming that the selected nearest neighbor is  $x_{zi}$ .

For the selected sample  $x_{zi}$ , a new sample  $x_m$  is constructed with the original sample  $x_i$  according to Eq. (3), where  $\beta$  is a (0, 1) random number.

$$x_m = x_i + \beta \times (x_{zi} - x_i) \quad (3)$$

The XGBoost algorithm is a tree-based Boosting that can automatically utilize multiple threads for parallelism. A second-order Taylor expansion was used for the loss function, and a regular term was added to the objective function to find the optimal solution, so as to weigh the complexity of the objective function and the model and prevent overfitting. The objective function is Eq. (4).

$$\Psi(y, F(X)) = \sum_{i=1}^N \Psi(y_i, F(x_i)) + \sum_{m=0}^T \Omega(f_m) = \sum_{i=1}^N \Psi(y_i, F(x_i)) + \sum_{m=0}^T (\gamma L_m + \frac{1}{2} \lambda \|\varpi_m\|^2) \quad (4)$$

where  $y_i$  represents the sample label;  $N$  is the number of samples;  $T$  is the number of trees;  $F(x_i)$  represents the first decision trees;  $L_m$  is the number of leaf nodes of the tree  $f_m$ ;  $\varpi_m$  is the output value of each leaf node of  $f_m$ ;  $\gamma$  and  $\lambda$  are the penalty coefficients. XGBoost is to first find the second-order Taylor approximation of the loss function and then minimize the approximate loss function to train the weak learner  $f_m(X)$ , as in Eq. (5).

$$\Psi_m \approx \sum_{i=1}^N [\Psi(y_i, F_{m-1}(x_i)) + g_i f_m(x_i) + \frac{1}{2} h_i f_m^2(x_i)] + \Omega(f_m) \quad (5)$$

where  $F_{m-1}(x_i)$  represents the first ( $m-1$ ) decision trees;  $g_i$  represents the first order partial derivative;  $h_i$  represents the second order partial derivative. The above equation is transformed to Eq. (6), where  $A$  is a constant.

$$\Psi_m = A + \sum_{i=1}^N [g_i f_m(x_i) + \frac{1}{2} h_i f_m^2(x_i)] + \Omega(f_m) \quad (6)$$

## 3 Results

### 3.1 PSM-Based Impact Analysis of Network Services on SRH

Balance test for PSM. Single factor analysis was conducted using chi-square test, and variables that were statistically significant were included in the PSM model to explore the impact of network services on SRH of older adults. The matching methods used in this paper include: Nearest Neighbor Matching (NNM), Caliper Matching (CM), Kernel Matching (KM), and Local Linear Regression Matching (LLRM). To ensure the reliability of the matching results, we tested the balance of the control variables, and the test results are shown in Table 4.

From Table 4, after using the NNM, CM, KM, and LLRM methods, there were no significant systematic differences ( $P > 0.05$ ) between the control and treatment groups, except for the difference in SRH. After sample matching, for mobile internet, the standardized deviation of explanatory variables was reduced from 50% to 7% ~ 4%, and

**Table 4.** Balance test results of the control variables before and after PSM.

Methods	Network services	Pseudo R <sup>2</sup>	LR chi <sup>2</sup>	P > chi <sup>2</sup>	Mean Bias	Med Bias	B	R	%Var
Unmatched	Network	0.217	737.91	0.000	40.2	45.4	119.5*	2.37*	50
	Computer	0.387	316.34	0.000	78.0	78.1	248.1*	0.66	21
NNM	Network	0.009	16.68	0.338	4.5	3.3	22.2	1.40	7
	Computer	0.018	4.51	0.996	6.5	5.6	32.0*	1.09	0
CM	Network	0.008	14.03	0.523	3.6	2.6	20.4	1.47	7
	Computer	0.003	0.67	1.000	2.7	2.6	12.3	1.34	0
KM	Network	0.008	15.98	0.384	3.9	1.9	21.7	1.34	7
	Computer	0.007	1.65	1.000	4.5	4.5	19.3	1.40	0
LLRM	Network	0.014	25.70	0.061	5.7	4.9	27.6*	1.39	14
	Computer	0.023	5.55	0.986	5.6	3.8	35.7*	1.04	14

the total bias was significantly reduced. Pseudo R<sup>2</sup> decreased from 0.217 to 0.008 ~ 0.014 after matching. LR chi<sup>2</sup>, mean bias, and med bias all significantly decreased. Similarly, for computer access, the standardized deviation of explanatory variables was reduced from 21% to 0% ~ 14%, and the total bias was significantly reduced. Pseudo R<sup>2</sup> decreased from 0.387 to 0.003 ~ 0.023 after matching. LR chi<sup>2</sup>, mean bias, and med bias all significantly decreased. Based on the analysis of the above results, it can be seen that PSM can reduce the differences in the distribution of explanatory variables between the control and the treatment groups.

**Measurement of the average treatment effect.** We measured the average treatment effect of network services on SRH of older adults, and the estimated results are shown in Table 5. The measures obtained after matching using the four different methods were generally consistent, indicating good robustness of the sample data. For each matching method, the average treatment effect of network services was positive, indicating that the treatment group (using network services) improved SRH of older adults by 14.1% compared to the control group (not using network services) when controlling for the same confounding variables, i.e., network services had a positive effect on SRH of older adults.

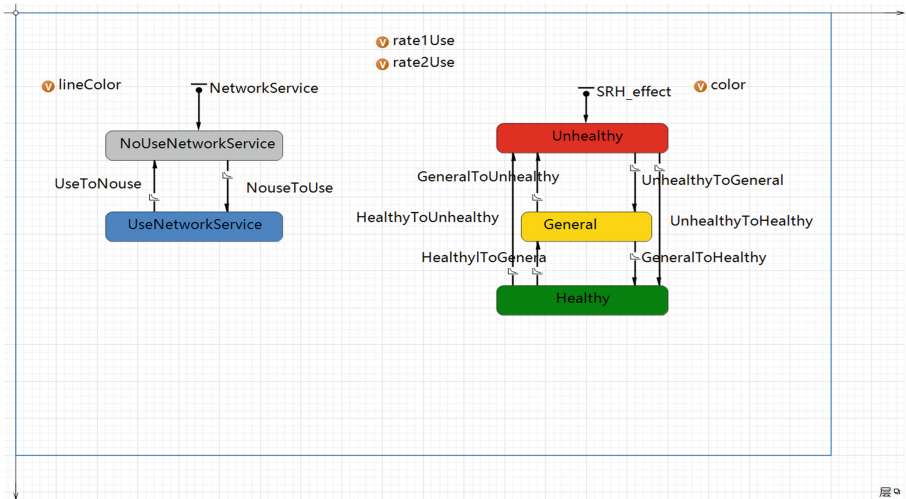
### 3.2 Agent-Based Simulation Analysis of Network Services on SRH

**Experimental environment.** AnyLogic is a simulation tool for modeling discrete, continuous, and hybrid systems by creating the mathematical models, using the experimental results as an approximate solution to the original problem. ABM is an effective method for system analysis and system auditing, which is more convincing and intuitive than other analysis tools. A multi-agent system refers to a collection of individual agents, this system overcomes the shortcomings of incomplete knowledge and information of individual agents.

**Table 5.** Impact of network services on the self-rated health of older adults.

Matching methods	Network services	Treated	Controls	ATT_Difference	S.E	T-stat
NNM	Network	2.802	2.696	0.107	0.074	1.44
	Computer	2.989	2.874	0.114	0.149	0.77
CM	Network	2.798	2.697	0.101	0.070	1.45
	Computer	2.989	2.802	0.186	0.139	1.34
KM	Network	2.802	2.699	0.104	0.071	1.47
	Computer	2.989	2.819	0.169	0.141	1.20
LLRM	Network	2.802	2.691	0.111	0.092	1.21
	Computer	2.989	2.755	0.234	0.191	1.22
Network services	Network	2.801	2.696	0.106	0.077	1.393
	Computer	2.989	2.813	0.176	0.155	1.133
	<b>Average</b>	<b>2.895</b>	<b>2.755</b>	<b>0.141</b>	<b>0.116</b>	<b>1.263</b>

**Simulation results.** The behavior of an agent can be specified in multiple ways. Due to the fact that agents have specific states, and their actions and reactions are state dependent, so the behaviors of agents can be defined through the state diagram. Figure 2 shows the interaction between SRH and network services based on AnyLogic.

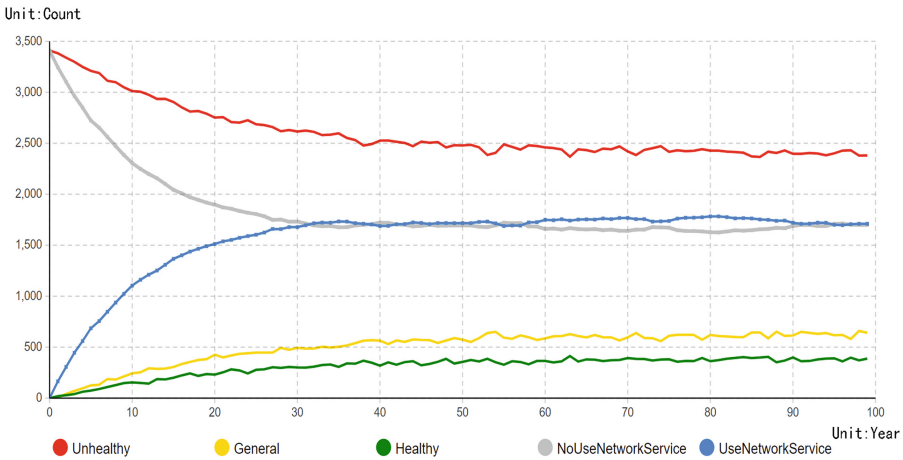


**Fig. 2.** Interface setup diagram in the AnyLogic software.



The colors “gray” and “blue” represent the usage of network services, while the colors “red”, “yellow”, and “green” indicate that the health status of older adults. The three states are “unhealthy”, “general”, and “healthy” respectively. The conversion rate between not using and using network services was calculated by averaging the network services (Table 5). The annual conversion rate for the change from not using network services to using network services was  $0.051 = (2.895 - 2.755) / 2.755$ , and the annual conversion rate for the change from using network services to not using network services was  $0.048 = (2.895 - 2.755) / 2.895$ . Similarly, the annual conversion rate from unhealthy to general to healthy is 0.141, while the annual conversion rate from unhealthy to healthy is 0.282, as shown by the conclusion that “the use of network services improves the health status by 14.1%”.

To simulate the effect of network services on SRH of older adults, a simulation model of the health status of older adults was constructed based on the operation period (in years), and the simulation effect is shown in Fig. 3.



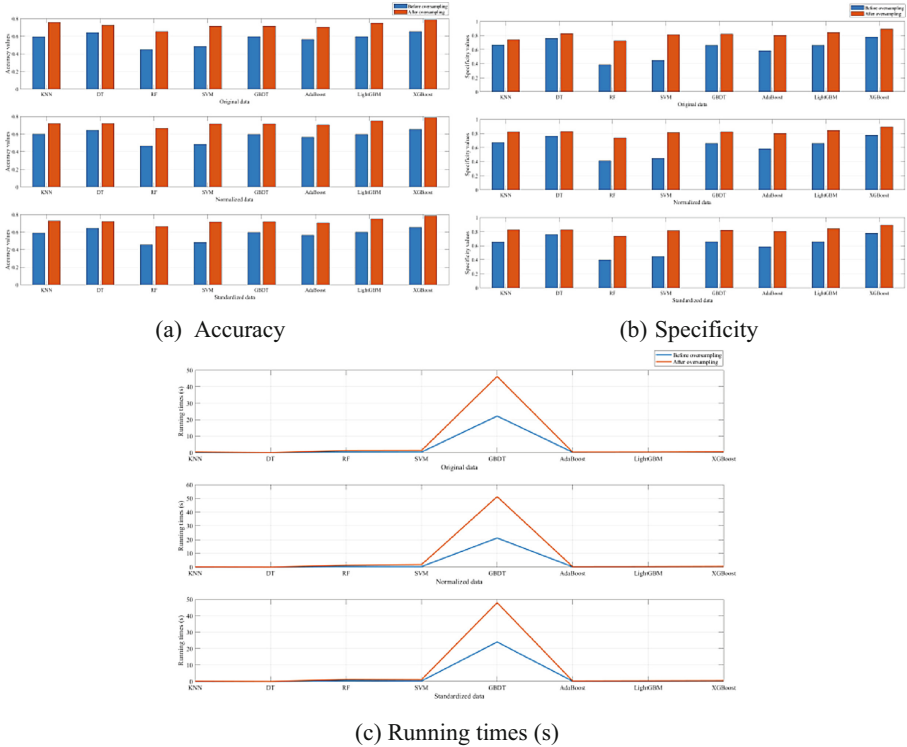
**Fig. 3.** Effect of statistical changes in network services and health status.

Figure 3 shows the change process of the effect of network services on SRH, with the horizontal coordinate indicates the unit of “year” and the vertical coordinate indicates the “count”. It is clear from Fig. 3 that the health status of older adults after using the network services has improved significantly and leveled off over a certain period of time. The fact that the number of people using the network services is increasing and the number of people not using the network services is decreasing and leveling off also shows that the agents are interacting with each other.

### 3.3 Prediction Analysis of SRH Based on SMOTE and XGBoost

Regarding the allocation rule of the dataset used to predict SRH of older adults, we selected 70% of the sample dataset for model construction, and 30% of the sample dataset

for evaluating the prediction performances. The evaluation metrics include accuracy =  $\frac{TP+TN}{TP+TN+FP+FN}$ , specificity =  $\frac{TN}{FP+TN}$ , and running times.  $TP$  represents the number of actual positive samples classified as positive,  $TN$  represents the number of actual negative samples classified as negative,  $FN$  represents the number of actual positive samples classified as negative, and  $FP$  represents the number of actual negative samples classified as positive. To verify the evaluation results of the prediction models, eight classifiers were used for comparison, including KNN, DT, RF, SVM, GBDT, AdaBoost, LightGBM, and XGBoost. The effects are shown in Fig. 4.



**Fig. 4.** Prediction effects based on the different data processing and classifiers.

KNN and SVM belong to the models involving the measurement of sample distance, but the sample missing values can affect the prediction performance. DT is prone to overfitting and has good prediction accuracy on the training dataset, but not obvious effect on the test dataset. RF random sampling makes there is not much correlation between trees, which can lead to the bottleneck of the fitting effect. GBDT has a long training time, usually not applicable to high-dimensional sparse data. AdaBoost uses weak classifiers to cascade and fully considers the weight of each classifier. LightGBM improves the speed while ensuring the accuracy comparable to XGBoost. XGBoost has high computational efficiency, uses second derivatives, and regularizes to reduce overfitting. From Fig. 4, for the three data processing methods, XGBoost has better

performance in terms of both accuracy and specificity compared to the other classifiers. After SMOTE oversampling, accuracy for XGBoost increased from 0.654 to 0.787, and specificity increased from 0.776 to 0.890. Moreover, the running time was acceptable for the case study in this paper.

## 4 Conclusions

Based on the analysis of the health status of older adults in China, a chi-square test was used to analyze the significant factors influencing SRH of older adults. Furthermore, the PSM model was employed to further investigate the potential impact of network services on SRH of older adults, aiming to address the endogeneity issue between the two variables. Using the AnyLogic simulation platform, a multi-agent-based modeling approach for the health behaviors of the older adult population was developed. This study compares the distribution of the number of older adults across health status, providing a dynamic and micro-level exploration of the effects on older adults' health status. By considering the characteristics of the sample data and selecting the significant key factors, the machine learning algorithms were used to construct prediction models.

Descriptive statistics were conducted on a sample of 3409 older adults, revealing a relatively favorable SRH. The results of the chi-square test demonstrate that 16 feature variables, including gender, education, city, network, and computer access, are significantly associated with their SRH. Employing PSM methods to explore the effects of network services on SRH of older adults, the results indicate that the use of network services has a positive impact on SRH, leading to a 14.1% improvement in their SRH level. Utilizing the AnyLogic software, a dynamic multi-agent model was developed to simulate the impact of network services on the health status of older adults. The experimental results confirm that the utilization of network services by older adults contributes to the enhancement of their health status. Based on the significant factors, a comparison of eight classification algorithms, including KNN, DT, RF, SVM, GBDT, AdaBoost, LightGBM, and XGBoost, reveals that the XGBoost algorithm exhibits a noticeable improvement in the accuracy. After applying the SMOTE oversampling technique, XGBoost achieves an accuracy indicator of 0.787, specificity indicator of 0.890, and an evaluation running time of 0.505s, outperforming the other algorithms considered in this study.

**Acknowledgments.** This research was funded by the Strategic Research and Consulting Project of the Chinese Academy of Engineering, grant number 2022-XBZD-30.

## References

1. Bai, C., Lei, X.: New trends in population aging and challenges for China's sustainable development. *China Econ. J.* **13**(1), 3–23 (2020)
2. Alanazi, H., Daim, T.: Health technology diffusion: case of remote patient monitoring (RPM) for the care of senior population. *Technol. Soc.* **66**(4), 1–11 (2021)
3. Pfarr, C., Schmid, A., Schneider, U.: Reporting heterogeneity in self-assessed health among elderly Europeans. *Heal. Econ. Rev.* **2**(1), 1–14 (2012)

4. Zadworna, M.: Pathways to healthy aging - Exploring the determinants of self-rated health in older adults. *Acta Physiol (Oxf.)* **228**, 1–9 (2022)
5. Mcalpine, D.D., Mccreeedy, E., Alang, S.: The meaning and predictive value of self-rated mental health among persons with a mental health problem. *J. Health Soc. Behav.* **59**(2), 200–214 (2018)
6. Kumar, S., Pradhan, M.R.: Self-rated health status and its correlates among the elderly in India. *J. Public Health* **27**(3), 291–299 (2019)
7. Zhang, Y., Wu, B., Chen, P., Guo, Y.: The self-rated health status and key influencing factors in middle-aged and elderly: evidence from the CHARLS. *Medicine* **100**(46), e27772 (2021)
8. Fonoberova, M., Fonoberov, V.A., Mezić, I.: Global sensitivity/uncertainty analysis for agent-based models. *Reliab. Eng. Syst. Saf.* **118**, 8–17 (2013)
9. Li, Y., et al.: A new oversampling method and improved radial basis function classifier for customer consumption behavior prediction. *Expert Syst. Appl.* **199**, 1–28 (2022)
10. Xin, Y., Ren, X.: Predicting depression among rural and urban disabled elderly in China using a random forest classifier. *BMC Psychiatry* **22**(1), 1–11 (2022)
11. Tian, S., Xu, L., Wu, X.: Impacts of social participation on self-rated health of aging women in China: with a mediating role of caring for grandchildren. *Int. J. Environ. Res. Public Health* **18**(11), 1–18 (2021)
12. Gupta, D., Richhariya, B., Borah, P.: A fuzzy twin support vector machine based on information entropy for class imbalance learning. *Neural Comput. Appl.* **31**(11), 7153–7164 (2019)
13. Chawla, N.V., Bowyer, K.W., Hall, L.O., Kegelmeyer, W.P.: SMOTE: synthetic minority over-sampling technique. *J. Artif. Intell. Res.* **16**, 321–357 (2002)



# Research on Telecommuting Security Solution Based on Zero Trust Architecture

Wanli Kou<sup>(✉)</sup>, Huaizhe Zhou, and Jia Du

Test Center, National University of Defense Technology, Xi'an, China  
kouwanli@nudt.edu.cn

**Abstract.** With the continuous deepening of information technology construction and the surge in demand for telecommuting, traditional security protection measures are difficult to cope with complex network environments. Solving security issues such as telecommuting based on Zero Trust architecture become a focus of attention. The core of a Zero Trust architecture is “continuous verification, never trust”, which means that by default, both internal and external personnel, terminals, and businesses are considered untrustworthy, and their access to the network and business resources will be continuously verified and evaluated. The paper first expounds the historical evolution, basic characteristics, and key technologies of Zero Trust, and then proposes a telecommuting security solution based on Zero Trust architecture. The solution can effectively solve problems such as identity trustworthiness discrimination, device trustworthiness discrimination and behavior trustworthiness discrimination, to achieve secure and reliable business access for telecommuting workers and intelligent terminals. The solution has reference significance for further optimization and implementation of Zero Trust framework in relevant application scenarios.

**Keywords:** Zero trust · Telecommuting · Dynamic access control · Software defined perimeter

## 1 Introduction

With the rapid development of technologies such as 5G, cloud computing, the Internet of Things, and mobile internet, various universities and enterprises have vigorously promoted the construction of information technology conditions. Meanwhile, due to the impact of the epidemic in recent years, telecommuting has become increasingly popular in recent years and has become an indispensable work mode. Telecommuting generally involves establishing a temporary virtual secure private tunnel in the public network through VPN and other related technologies, forming a relatively secure and stable connection through the public network. Telecommuting provides us with many conveniences in our work and life, but there are also many security risks, such as telecommuting terminals being stolen, telecommuting workers' account passwords being leaked, and telecommuting workers' own security risks and so on.

The traditional network security architecture takes boundary protection as the principle, constructing layer by layer defense lines to protect sensitive resources in the

network. Telecommuting has made traditional network boundaries increasingly blurred, and traditional boundary security measures are difficult to cope with complex network environments. Borderless network security protection begins to receive attention. In recent years, the concept of “de boundary” has gradually developed and grown, and has now evolved into a systematic and comprehensive concept - Zero Trust. Solving security issues such as remote work based on Zero Trust has become a continuous focus of attention for universities, enterprises, and other units.

## **2 Overview of Zero Trust Architecture.**

As a new security concept at present, The Zero Trust architecture’s core key lies in breaking the default “trust” [1]. It has evolved from a basic concept to a solution framework with certain core technologies, which can ensure identity trust, device trust, application trust, and link trust.

### **2.1 Historical Evolution of Zero Trust**

The coarse security model based on boundary protection has been unable to cope with the increasingly severe network security situation, so the concept of “de-bordering” has been developed and gradually evolved into a systematic and comprehensive conceptual framework—Zero Trust.

At the 2004 Jericho Forum, the concept of “de-bordering” was first proposed. In 2010, the famous research institution Forrester officially proposed the term “Zero Trust”. In 2011, Google began implementing the Beyond Corp Zero Trust implementation project, exploring the use of Zero Trust concepts to build a new network security architecture, enabling employees to securely access internal systems and resources of the company from anywhere. In 2014, the Cloud Security Alliance proposed a Zero Trust solution as SDP (Software Defined Perimeter), which utilizes mechanisms such as identity access control and comprehensive authorization management to build virtual network boundaries and provide stealth protection for micro applications and services. In August 2020, the National Institute of Standards and Technology of the United States released the “Zero Trust Architecture”, which elaborated on the definition, principles, key technologies, and application scenarios of Zero Trust. In April 2020, Qi An Xin Technology Group Inc and Gartner jointly released the “Zero Trust Architecture and Solutions Joint White Paper”, proposing a Zero Trust reference architecture and solutions based on typical application scenarios.

After more than a decade of evolution and development, the Zero Trust security concept has been fully recognized in the security industry. In terms of technological evolution, Zero Trust has gradually evolved from the initial network segment to a new generation of security architecture based on identity and covering multiple scenarios; In terms of development planning, various countries have published white papers, evaluation reports, and scheme architectures, and have also implemented them in typical application scenarios.

### 2.2 Basic Characteristics of Zero Trust Architecture

The Zero Trust security architecture differs from traditional security architectures in terms of protection concept, protection objects, and protection foundation (see Fig. 1). The core of a Zero Trust architecture is “continuous verification, never trust”, which means that all personnel, terminals, and businesses are considered untrustworthy by default, and their access to the network and business resources will be continuously verified and evaluated.

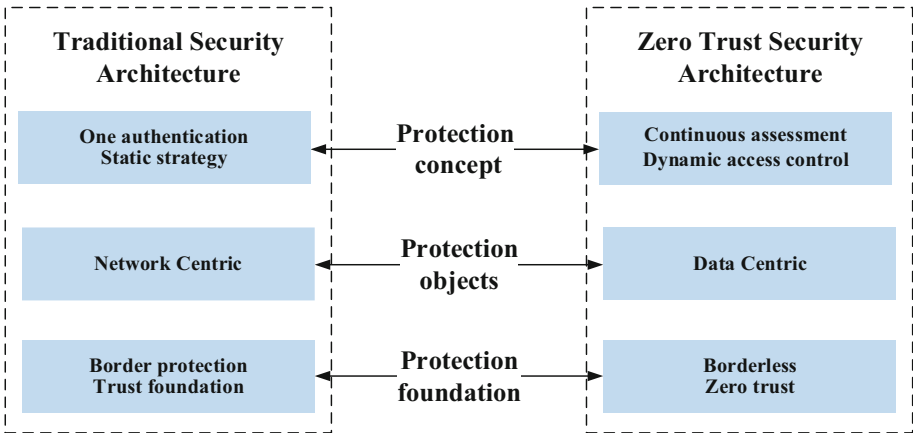


Fig. 1. The difference between zero trust and traditional security institutions.

**Based on Identity.** In a Zero Trust architecture, comprehensive identification of personnel, devices, and businesses in application scenarios is a prerequisite and cornerstone for achieving Zero Trust. The Zero Trust architecture collects multiple identity authentication factors such as passwords, certificates, biosignature, and assigns a unique digital identifier to all legitimate users, devices, applications, services, achieving comprehensive identification of various entities. This is the foundation for forming end-to-end trust relationships.

**Continuous Trust Assessment.** Traditional security protection has one-time certification and has been effective for longer time. In order to ensure the continuous legality and security of identity, Zero Trust is based on continuous trust evaluation for authorization decisions. In trust assessment, multiple factors with higher intensity will be used for authentication, and trust judgment will also be made based on comprehensive evaluation of relevant factors such as risk status and environment.

**Dynamic Access Control.** Zero Trust is different from traditional boundary protection devices based on static access control policies. It is identity centric for dynamic access control. Zero Trust requires mandatory identity recognition, authorization judgment, and fine-grained access control for every access request in all business scenarios. Under the Zero Trust architecture, it is a dynamic and micro decision logic that dynamically authorizes access control through risk assessment through continuous trust assessment.

**Minimum permission control.** Zero Trust emphasizes the on-demand allocation of resource usage, with the minimum degree of resource openness based on comprehensive judgments such as business reality, subject needs, and trust evaluation. At the same time, Zero Trust uses technology such as port hiding and traffic encryption to hide resources outside of the subject's permissions, in order to protect business resources.

### 2.3 Zero Trust Key Technologies

**Software Defined Perimeter (SDP).** The Software Defined Perimeter technology [2], as the security framework of the cloud security alliance, is based on the use of identity access control and comprehensive permission authentication mechanisms to construct virtual boundaries. The SDP puts on "invisibility cloak" for applications and services within the boundaries, so that attackers cannot see the target of the attempted attack at the root, effectively protecting data security. SDP can verify users, devices, data, and other related resources and allow them to access the required services within a specific virtual boundary. It has the characteristics of network stealth, pre authentication and pre authorization.

**Intelligent Identity Management.** Zero Trust intelligent Identity management technology focuses on the intelligent management of key factors such as identity, permissions, environment, activities, to ensure that the right subjects access the right resources based on the right reasons in the right environment. In a Zero Trust architecture, achieving the effects of continuous trust evaluation and dynamic access control will inevitably significantly increase management overhead. To improve the automation level in the Zero Trust architecture, only by introducing intelligent identity analysis can better achieve the implementation of the Zero Trust architecture.

**Micro Isolation Technology.** Micro isolation was first proposed by the VMware technical team as a more fine-grained network isolation technology. For data centers, traditional firewalls typically only provide security protection against north-south traffic while lacking control over internal network east-west traffic. Micro isolation technology can logically divide data centers into different security segments and define security policies for each segment to provide corresponding control services, with a focus on preventing attackers from horizontally moving and spreading within the data center network.

## 3 Telecommuting Security Solution Based on Zero Trust

In the context of large-scale telecommuting applications, due to complex user roles, environments and large network exposure, risk factors will follow such as terminal management and control risk, Man-in-the-middle attack risk, network asset access risk, identity authentication risk, static access control risk and so on. Therefore, there is an urgent need to build a trust system based on the existing security protection architecture. It perceives the comprehensive perception of the environment, continuously evaluates trust, and adapts access control to solve some problem such as security compliance requirements, terminal access requirements, and network security requirements.



### 3.1 Architecture Design

The essence of Zero Trust security is to dynamically control business access based on identity authentication, mainly consisting of identity security infrastructure, Zero Trust proxy, control analysis platform and so on. Through these components, a security access framework that links control and data plane is established. It ensures the credibility of the access subject’s access to object applications, data and so on (see as Fig. 2).

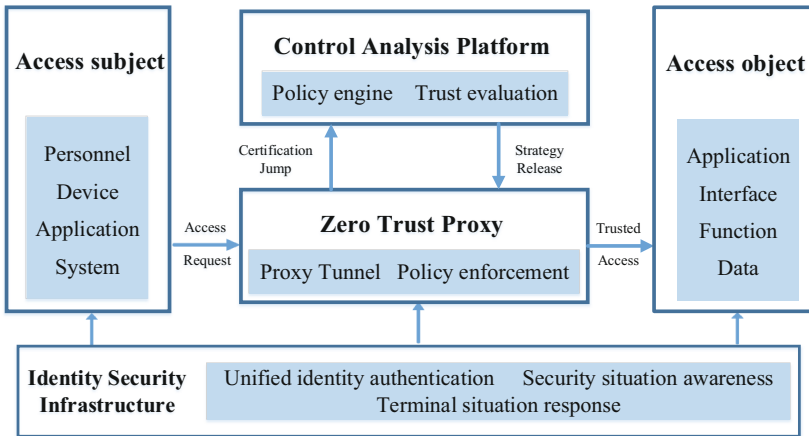
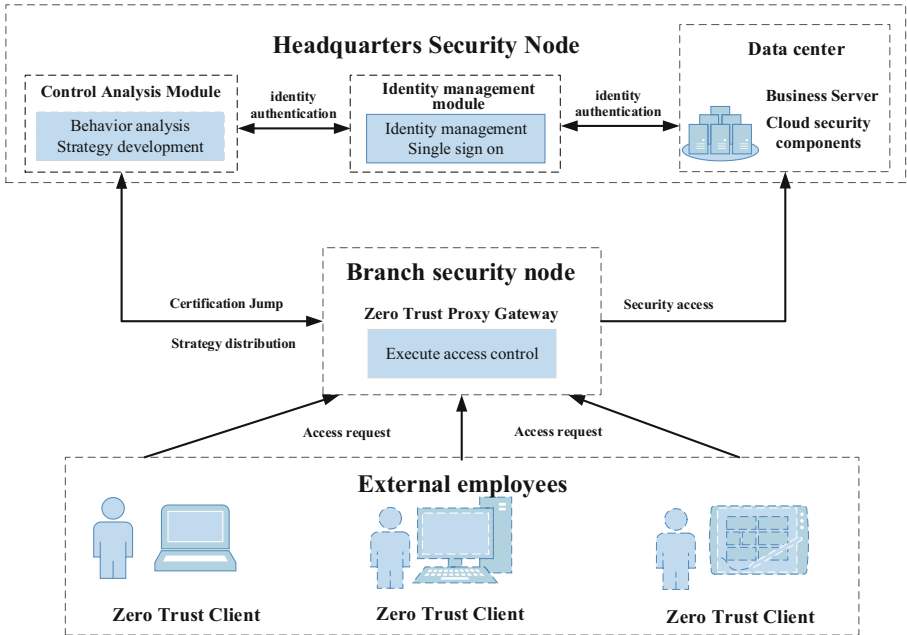


Fig. 2. Zero trust basic architecture.

Identity security infrastructure [3, 4] mainly includes unified identity authentication, security situation awareness, terminal situation response and other components, providing Identity management, authority management, situation presentation, terminal protection and other functions. It provides Zero Trust agents with identity, authority and other security baseline data. Zero Trust proxy mainly includes functions such as proxy tunneling and policy execution, and it is a policy execution point for dynamic access control. The control analysis platform mainly includes control engine, trust evaluation and other components, which conduct continuous analysis on access behavior and continuous evaluation. Based on the dynamic Principle of least privilege, all access requests are authenticated and authorized, and are delivered to the Zero Trust proxy module for execution.

### 3.2 Deployment Design

According to the demand analysis and architecture design of telecommuting, a trusted access system for various personnel and devices can be established based on a Zero Trust system [5]. It can achieve trusted detection and discrimination of personnel identity, device access to the business system, and personnel behavior, solving the problem of secure and trustworthy business access for employees and intelligent terminals working outside (see as Fig. 3).



**Fig. 3.** Basic architecture of zero trust system deployment.

This solution is designed according to the application scenarios of three-level security nodes for headquarters, branches, and external personnel. Based on retaining the original security means, the company headquarters deployed a Zero Trust control analysis system and a unified Identity management system, the headquarters data center deployed business servers and related cloud security components, each branch only needed to deploy a Zero Trust proxy gateway, and the employees outside needed to deploy a Zero Trust client to build a terminal trusted access system.

The PC, Pad, mobile phone and other smart terminals used by external workers need to install Zero Trust client. When they initiate remote office and other access requests, the Zero Trust client will start immediately, mainly to ensure that the security compliant terminal is allowed to access business. It prevents attacks on business and data through vulnerable or lost terminals as a springboard, and strengthen the security detection and evaluation of device side applications. It discovers and block untrusted applications from accessing business systems, effectively preventing untrusted applications from accessing the system. After checking compliance with the terminal baseline, it accesses the Zero Trust proxy gateway in an encrypted manner.

The Zero Trust proxy gateway [6] deployed by the branch security node supports the protection function of user accounts throughout their entire lifecycle, application control policy lifecycle management, and control policy exception analysis function. After linking with the Zero Trust platform of the unit headquarters, it can jump to the Zero Trust analysis control module for identity authentication. Authorized users can access the corresponding resources, otherwise access will be denied.

The Zero Trust control analysis module and the unified Identity management module deployed by the headquarters are mainly responsible for the authentication, policy management and distribution of various access business system behaviors, and for the overall scheduling and management. They are responsible for the trust evaluation of the accessed identity, terminal, environment and behavior. Based on the results of the behavioral risks judged by various algorithm models, they decide to allow or reject sessions and let the trusted gateway open or block them.

Before and after the entire external personnel access process, the Zero Trust platform will continuously evaluate the identity, terminal, and behavior of personnel, and can interact with traditional security protection methods. Once risks are discovered, corresponding dynamic access control actions will be executed.

### 3.3 Capability Design

**Establish a trusted Identity management system.** The solution integrates and controls personnel, identities, accounts, permissions, data, and communication methods comprehensively for various business systems in the company headquarters data center and various external access employees. The solution achieves identity unification and provides multiple identity authentication methods. It enhances identity authentication methods in abnormal environments, and verifies the effectiveness and authenticity of access behavior, and prepares for subsequent association analysis and refined dynamic access control.

**Possess the ability to identify abnormal behavior risks.** Through the behavior analysis component provided by the Zero Trust Control Center, the solution learns and models the access behavior of personnel. After a period of learning, the solution summarizes various characteristics of personnel accessing the business system, such as time baseline, access object baseline, access behavior baseline, etc. And the system compares and learns the baseline situation of these elements during each visit process, timely identifying potential risk situations.

**Building a continuous analysis and evaluation system.** This solution has the ability of abnormal behaviors analyzing and distinguishing in situations where the security of personnel outside the unit is uncontrollable, such as the theft of personnel identities or terminals. Zero Trust system continuously evaluates the trust of access subject, terminal and behavior based on multiple data sources, and comprehensively evaluates whether each access can be based on trusted Environment and Behavior.

**Establish a trusted business usage environment.** For different business usage forms and environments of remote office, it is necessary to ensure that the terminal itself can access the corresponding business system in a safe and trustworthy manner. During the process of accessing the business system, other unrelated processes cannot be executed. The Zero Trust system has the ability of network stealth and application stealth. It adapts “authentication before connection” approach, greatly reducing network exposure and effectively alleviating various network attacks.

## 4 Conclusion

The Zero Trust architecture aims to protect data security, aiming to solve the inherent problem of establishing trust based on traditional boundary static access control, and reflects the latest concept achievements of security architecture. The Zero Trust architecture has become an important option for cloud computing, big data, and mobile to realize de boundary network security. However, Zero Trust is still in its early stages, and institutions such as universities and companies should take the optimization and iteration of the network security system as an opportunity to integrate the concept of Zero Trust, and use typical scenarios as a starting point to promote the transformation of Zero Trust capabilities. In addition to telecommuting, application exploration can be carried out in multiple fields such as edge computing environment [7, 8] and 5G security, promoting further optimization and implementation of Zero Trust frameworks and related technologies.

## References

1. Shaw, K.: What is zero trust network architecture (ZTNA)?. *Network World (Online)* (2022)
2. Singh, J., Refaey, A., Koilpillai, J.: Adoption of the software-defined perimeter (SDP) architecture for infrastructure as a service. *Can. J. Electr. Comput. Eng.* **43**(4), 357–363 (2020)
3. Hao, P.: He Yuanwen. Research and application of network security architecture based on zero trust Guangdong communication technology **02**, 63–67 (2022)
4. Minlu, T., Meng, R.: Research on zero trust security system. *Inf. Secur. Commun. Confidential.* **10**, 124–132 (2022)
5. Xiaohai, C., Xiaohua, Y., Yanling, L.: Design of remote office security solutions in the context of the epidemic. *Guangdong Commun. Technol.* **43**(01), 20–23+31 (2023)
6. Tao, Z., Jian, G., Zhen, L., Xuan, Z.: Design of a security gateway based on zero trust architecture. *Netw. Secur. Technol. Appl.* (06), 2–4 (2023)
7. Dawei, L., Enzhun, Z., Ming, L., Chunxiao, S.: Zero Trust in edge computing environment: a blockchain based practical scheme. *Math. Biosci. Engin.: MBE* **19**(4), 4196–4216 (2022)
8. Haiqing, L., Ming, A., Rong, H., Rixuan, Q., Yuancheng, L.: Identity authentication for edge devices based on zero-trust architecture. *Concurrency Comput.: Practic. Experi.* **34**(23) (2022)



# RLOP: A Framework Design for Offset Prefetching Combined with Reinforcement Learning

Yan Huang and Zhanyang Wang<sup>(✉)</sup>

College of Software, Zhengzhou University of Light Industry, Zhengzhou 450001, China  
spocki@163.com

**Abstract.** Previous prefetching schemes have been found to be very effective at enhancing the performance of computers. However, speculative prefetching requests can have negative effects on computers, such as increased memory bandwidth consumption and cache pollution. To address the deficiencies of previous prefetching schemes, we propose the Reinforcement Learning Based Offset Prefetching Scheme (RLOP), an offset prefetching scheme based on reinforcement learning. As with previous offset prefetching schemes, RLOP evaluates multiple offsets and enables offsets that qualify to issue prefetching requests. RLOP, however, selects appropriate prefetch offsets through reinforcement learning, and the reinforcement learning reward scheme determines the goal of the prefetcher; we divide the rewards into four different rewards—accurate and timely prefetch, accurate but delayed prefetch, inaccurate prefetch, and no prefetch operation—and by increasing or decreasing the reward value, we facilitate or inhibit RLOP from future environments to collect such rewards, which enables or inhibits RLOP from collecting such rewards, which enables We evaluated and contrasted RLOP with various advanced data prefetchers and demonstrated that our scheme resulted in a 25.26% increase in system performance over systems without data prefetchers and a 3.8% increase over the previous best performing data prefetcher.

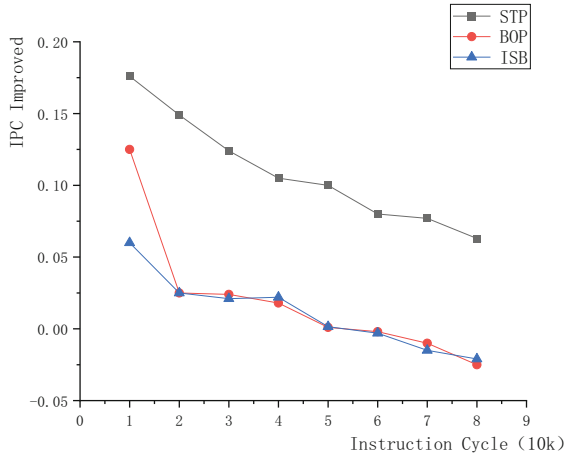
**Keywords:** Cache optimization · Data prefetching · Offset prefetching · Machine learning · Reinforcement learning

## 1 Introduction

Prefetching is a current technique that has been explored to effectively reduce cache miss rates, and early processors could realize substantial performance gains by employing simple stride or stream prefetchers. Various varieties of prefetchers have been proposed in prior research [1–5]. They have implemented prefetch requests using various programme features (programme counter, cache line address, page offset of a cache line, or simply combining these features with simple operations) in order to continuously improve prefetch accuracy (Accuracy and cache coverage), thereby enhancing computer performance. For instance, program counter-based inter-step prefetchers learn a constant step size between two consecutive memory accesses induced by the same

program counter by utilizing the program counter as a feature. Kumar and Wilkerson predicted the spatial memory access footprint of the entire memory region using the program counter and the address of the first memory region accessed. According to the SMS study, the program counter and the offset of the first memory region accessed were superior predictors of the memory access footprint. Bingo merged Bingo incorporates the capabilities of Spatial Footprints and SMS, and its features are program counter & cache line address and program counter & page offset of a cache line.

As shown in Fig. 1, excessive conjecture prefetching does not improve computer performance over time and can be detrimental. After conducting research, it was determined that the design of prefetchers in the past was primarily plagued by the following issues: (1) untimely and inaccurate prefetching; (2) lack of system awareness, speculative prefetch requests can have negative effects on the computer, such as increased memory bandwidth consumption, cache-polluted memory access interference, and system energy consumption, which can offset the performance gains from hiding long memory latencies; and (3) some prefetches were inefficient and inefficiently implemented. A effective prefetcher should maximize prefetching coverage and precision while minimizing the prefetcher’s negative impact on the system.



**Fig. 1.** The cumulative effect of prefetchers on computer performance.

We propose the Reinforcement Learning Based Offset Prefetching Scheme (RLOP), a reinforcement learning-based offset prefetching mechanism, to overcome the shortcomings of prior prefetching schemes. Recent research has shown that reinforcement learning frameworks can solve complex problems, such as mastering human-like control in Atari and Go [6, 7]. In this paper, we propose an offset prefetching framework incorporating reinforcement (RLOP) learning to accomplish improved prefetching coverage and accuracy by selecting accurate and timely prefetching offsets using the reward mechanism of reinforcement learning. The reward scheme determines the prefetcher’s

objective, and the incentive is divided into four categories: accurate and timely prefetching, accurate but delayed prefetching, inaccurate prefetching, and no prefetching operation. By iteratively learning the Q-value of the state-action pair, the reinforcement agent continuously optimizes its policy to perform increasingly optimal actions over time. By increasing or decreasing the reward's value, we enable or disable the RLOP to collect such rewards from the environment in the future, thereby guiding the RLOP to generate more precise and timely prefetching requests.

## 2 Related Work

### 2.1 Offset Prefetching

Offset prefetching [8, 9] is a modification of stride length prefetching in which the prefetcher does not seek to identify stride streams. The offset prefetchers do not associate the accessed addresses with any specific stream; rather, they process them individually and issue a prefetch request for each accessed address based on the prefetch offset.

Offset prefetchers that have reached maturity have an offset selection mechanism that dynamically determines the offset based on application behavior. Sandbox prefetcher was the first mature offset prefetcher proposed by Pugsley et al. Pierre Michaud's optimal offset prefetcher (BOP) [9] takes prefetching timeliness into consideration. While BOP is able to generate prefetch requests in a timely manner, it misses out on many opportunities to cover cache failures by relying on a single best offset and discarding many other suitable offsets. Previous offset prefetching schemes, according to Mehran et al., either disregarded timeliness or sacrificed cache coverage area to achieve timeliness when selecting prefetching offsets. Mehran et al. proposed a new offset prefetching mechanism, Multi-Lookahead offset Prefetcher (MLOP), which incorporates cache misses and timeliness when issuing prefetch requests, to overcome the shortcomings of previous offset prefetching algorithms.

### 2.2 Exploration of Prefetching with Machine Learning

Several researchers have attempted to incorporate machine learning into the development of prefetchers. In 2015, Rahman et al. proposed using machine learning algorithms to select the optimal prefetcher for various stages of program execution, whereas Gutman et al. investigated how software and hardware prefetches can be used more effectively together. The Long Short-Term Memory (LSTM) algorithm employs continuous incremental history within a page for training and prediction. Bhatia et al. posited Perceptron-based Prefetch Filtering in 2019 (PPF). Yuan Liang et al. 2019 proposed enhancing prefetchers with the reinforcement learning algorithm Sarsa. They utilized the contextual information accessed by the CPU as the state set of the Sarsa algorithm and the address values to be prefetched as the action set. The Pythia prefetcher, proposed by Rahul Bera et al., customizes prefetchers as reinforcement learning agents. For each demand request, Pythia considers multiple categories of program context data before making a prefetching determination. For each prefetch decision, Pythia [10] is rewarded numerically for evaluating the quality of the prefetch relative to the current memory

bandwidth consumption. Pythia uses this reward to strengthen the correlation between program context data and prefetch decisions in order to generate future prefetch requests that are highly accurate, expeditious, and system-aware.

We believe that the primary reason why the RL framework is appropriate for an offset prefetcher is that it can perform adaptive learning in complex state spaces. A decent prefetcher should maximize its advantages while minimizing its disadvantages, such as memory bandwidth consumption. The prefetcher should be able to adaptively trade-off between coverage and higher accuracy, based on its impact on the system as a whole, in order to provide robust performance enhancements in the face of fluctuating workloads and system configurations. Similarly, offset prefetchers do not associate access addresses with any particular stream; rather, they process each access address independently and issue a prefetch request based on the prefetch offset. RL is well-suited to modelling offset prefetchers as autonomous agents that learn prefetching through interaction with the system due to the nature of adaptive learning in a complex state space.

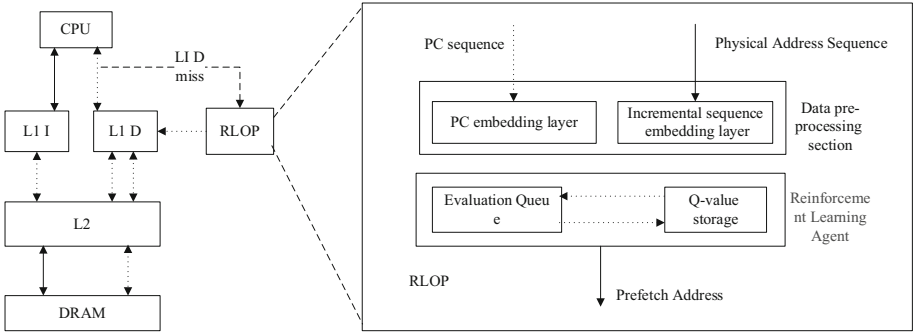
### 3 A Reinforcement Learning-Based Framework for Offset Prefetching

In this study, prefetching is viewed as a reinforcement learning problem and the reinforcement learning-based offset prefetcher RLOP is modified to act as a reinforcement learning agent. By interacting with the computer system, it learns to choose the correct offset and make precise and expeditious prefetching decisions. RLOP observes the state of the computer system and performs a prefetch action for each new demand request. RLOP receives a numerical incentive for each prefetch action that evaluates the precision and timeliness of the prefetch action. The objective of RLOP is to identify the optimal prefetch strategy in order to maximize the number of accurate and punctual prefetch requests, thereby enhancing computer performance.

#### 3.1 Framework Overview

Figure 2 depicts the cache prefetching framework based on the RLOP prefetcher proposed in this paper. The RLOP prefetcher learns the access miss information of the L1 D Cache, including the access miss physical address sequence and PC value sequence, to determine the processor's access mode and then issues a prefetch instruction to prefetch the data. The RLOP prefetcher is founded on an implementation of reinforcement learning. The RLOP prefetcher is composed of two major components: the data preprocessing component and the model prediction component. From the time the dataset is obtained until it is input into the prediction model, the data must be preprocessed. The PC value sequences and physical address sequences are converted into multidimensional vectors and fed into the reinforcement learning model so that the agent can learn. The prediction portion of the model consists of a QVStore and an evaluation queue, with the QVStore serving to store the Q values of the RLOP-observed iterative learning state-action pairs. The evaluation queue's purpose is to maintain a first-in-first-out inventory of the most recent RLOP actions. After the model prediction phase, the state vectors obtained from the data preprocessing phase are learned to extract the corresponding prefetch addresses.





**Fig. 2.** A framework design for offset prefetching combined with reinforcement learning.

### 3.2 Prefetcher Design

State space, actions, and reward schemes are formally defined as the three pillars of reinforcement learning-based prefetchers.

**State Space.** The state space is defined as a  $k$ -dimensional vector of program characteristics.

$$S \equiv \{ \phi_s^1, \phi_s^2 \dots \phi_s^k \} \tag{1}$$

A feature of the program comprises primarily of a program control flow component and a program data flow component. The control flow component includes basic information such as load-PC (i.e., the PC of the load instruction) or branch-PC (i.e., the PC of the branch instruction immediately preceding the load instruction) as well as a history indicating whether this information is extracted from only the current demand request or from a series of past demand requests. Similarly, the dataflow component is comprised of fundamental information such as cache line addresses, physical page numbers, page offsets, cache line increments, and their respective histories.

**Action.** Whenever a cache block (e.g.,  $A$ ) is requested, a cache block  $k$  cache blocks (e.g.,  $A + k$ ) away is prefetched, where  $k$  is the prefetch offset. The action of the RL agent is defined as selecting a prefetch offset from a set of candidate prefetch offsets. (possible increments between the predicted cache line address and the requested cache line address). For systems with legacy-sized 4 KB pages and 64B cache lines, previous prefetchers generated prefetch requests within physical pages with a prefetch offset list comprising only the physical page’s address  $(-63, 63)$ . Using offset prefetching as an operation (instead of the complete cache line address) reduces the size of the operation space significantly.

**Reward Program.** The reward scheme determines the prefetcher’s objective, and the rewards are divided into four categories: accurate and punctual prefetching, accurate but delayed prefetching, inaccurate prefetching, and no prefetching operation. Accurate and expeditious prefetching entails selecting the correct offset in time to complete the prefetching operation when required. Accurate but delayed prefetching indicates that the

correct offset is not chosen in time to finish the prefetching operation when it is required. Incorrect prefetching in which the incorrect offset is chosen when a prefetch operation is required. When a prefetch operation is required, neither prefetch nor an offset is selected for the prefetch operation. The reward scheme determines the prefetcher’s objective, and by increasing or decreasing the reward value, we enable or disable RLOP to collect such rewards from the environment in the future, thereby guiding RLOP to generate more accurate and punctual prefetch requests.

### 3.3 Hardware Architecture

The interaction process between an agent and its environment can be depicted by a Markov decision process, which serves as reinforcement learning’s fundamental framework. And in a Markov decision process, a state’s action is determined by its policy. The policy of an agent requires it to perform a specific action in a specific environment. The agent’s objective is to discover the optimal strategy that maximizes the reward received from the environment over time. The desired reward value for performing an action in a specific state is represented by the Q-value of the state-action pair (abbreviated Q(S, A)). At each time step, the agent iteratively optimizes its policy in two steps: (1) the agent updates the Q-value of the state-action pair using the rewards accumulated in the current time step, and (2) the agent optimizes its current policy using the most recent updated Q-value. Q-values are therefore the foundation of reinforcement learning. Q-values can be derived from the Q-function, also known as the action-value function, which specifies an expectation of the possible reward for performing a specific action in a particular state [11].

$$Q\pi(s, a) = E\pi[Gt|st = s, at = a] \tag{2}$$

Given that this expectation is also based on the strategy function, we must conduct a summation of the strategy function to determine its value. The value function is obtained by summing the actions in the Q function [12].

$$V\pi(s) = \sum_{a \in A} \pi(a|s)Q\pi(s, a) \tag{3}$$

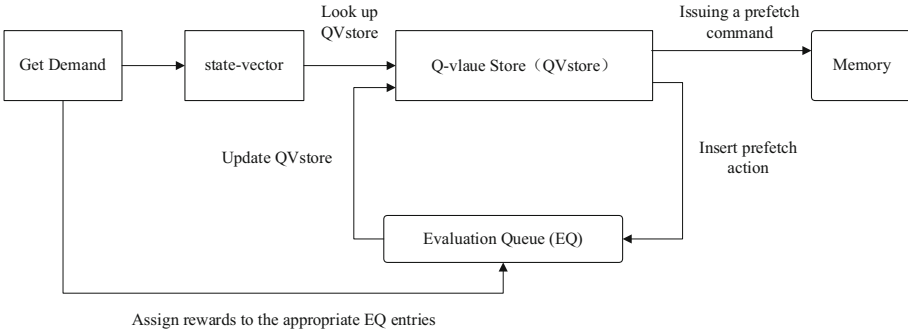
By iteratively learning the Q-value of the state-action pair, the reinforcement agent continuously optimizes its policy to take actions that approach the optimal one over time.

In a given time step  $t$ , the agent observes a state  $S_t$ , takes an action  $A_t$ , while the environment transitions to a new state  $S_{t+1}$  and issues a reward  $R_{t+1}$ , and the agent takes an action  $A_{t+1}$  in the new state, the SARSA algorithm iteratively optimizes the Q-value of the previous state-action pair  $Q(S_t, A_t)$ .

$$Q(S_t, A_t) \leftarrow Q(S_t, A_t) + \alpha[R_{t+1} + \gamma Q(S_{t+1}, A_{t+1}) - Q(S_t, A_t)] \tag{4}$$

$\alpha$  is a learning rate parameter that determines the convergence rate of Q.  $\gamma$  is a discount factor used to give greater weight to the instantaneous rewards received by the agent

at any given time step as opposed to the delayed future rewards. A value of  $\gamma$  close to 1 confers “farsighted” planning capabilities on the agent, i.e., the agent can obtain a greater future reward from a smaller immediate reward. Figure 3 depicts the RLOP hardware structure. The agent is able to determine the long-term effects of its actions in order to optimize its strategy, which approaches optimality over time.



**Fig. 3.** RLOP hardware structure.

## 4 Evaluation

### 4.1 Methodology

We evaluated the RLOP prefetcher using the Gem5 [13, 14] simulator and compared it to three previous prefetching scenarios. We simulated a multicore processor with up to twelve cores. The most important system parameters are listed in Table 1. We evaluate the performance of the RLOP prefetcher using *bizp2*, *gromacs*, *deall*, *hmm*, *libquantum*, and *h264ref*, which are benchmark programs from the SPEC CPU2006 [15] test suite. The Best Offset Prefetcher (BOP), the Irregular Stream Buffer Prefetcher (ISB) [16] and the ST predict prefetcher (STP) [17] based on an LSTM neural network were chosen for comparison with RLOP. Based on Sandbox Prefetcher, bop The ISB prefetcher learns how addresses are accessed by combining the spatial proximity of PCs and the correlation of access stream addresses. ST. Predict proposes a novel cache prefetching strategy based on deep LSTM neural networks.

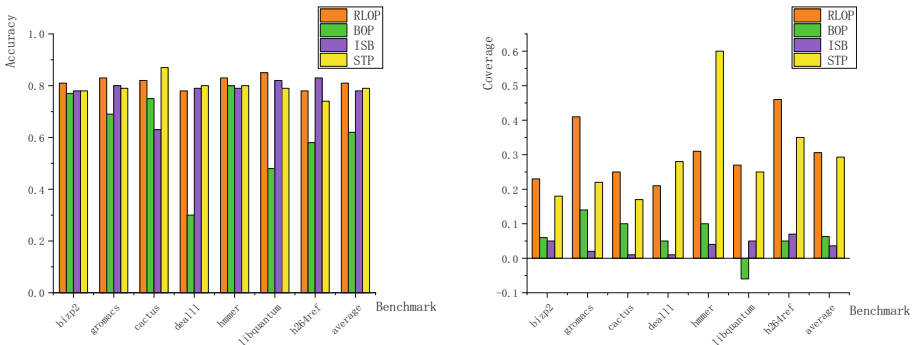
### 4.2 Evaluation

The efficacy of RLOP was evaluated based on the evaluation methodology described previously. Figure 4 (left) depicts the prediction accuracies of various prefetchers across multiple SPEC2006 test sets. As shown in the graph, the overall prediction accuracy of the RLOP prefetcher is comparatively high, exceeding 0.8, and is the highest of all prefetchers. In the *h264ref* and *deall* test sets, the prefetchers were marginally less precise than 0.8 and marginally inferior to the ISB and STP prefetchers. The average

**Table 1.** Simulated system parameters.

Suite	Parameters
Core	1–12 cores, 4-wide OoO, 128-entry ROB, 32/36-entry LQ/SQ
Branch predictor	Tournament
L1/L2 caches	Private, 32KB/1MB, 64B line, 8 way, LRU, 4/20 MSHRs
Main memory	4096 MB

prediction accuracy of the RLOP prefetcher was 23.5% higher than the average prediction accuracy of the BO prefetcher, and in some test sets, the prediction accuracy was also considerably higher than that of the ISB and SPP prefetchers. This suggests that the RLOP prefetcher has a high rate of right address prediction. Accuracy only indicates the probability that the prefetcher predicts correctly and does not indicate the improvement in program performance by the prefetcher; coverage is also required for an accurate representation of the improvement in program runtime performance by the prefetcher. Figure 4 (right) demonstrates the prefetch coverage area of multiple prefetchers under various SPEC2006 test sets. The minimum coverage area of the RLOP prefetcher is 0.216 and the maximum coverage area is 0.462. Under the hummer test set, the RLOP prefetcher has a lower coverage area than the STP prefetcher, but the RLOP prefetcher has a higher coverage area overall. The coverage area of the RLOP prefetcher is 35.16% greater than that of the BO prefetcher and 32.67% greater than that of the ISB prefetcher on average. The coverage area of the RLOP prefetcher was 32.67% greater than that of the ISB prefetcher and 4.37% greater than that of the STP prefetcher.



**Fig. 4.** Comparison of the prediction accuracy (left)/coverage (right) of different prefetchers.

The prediction accuracy parameter and the coverage area parameter of the prefetcher are reflected in the combined performance of the program in terms of the improvement in the number of instructions per cycle. The larger the improvement in the number of instructions per cycle, the more the prefetcher enhances the running speed of the program. Figure 5 (left) illustrates the IPC improvement of RLOP for multiple SPEC2006 test sets compared to when the prefetcher is not added, and it can be concluded that the system

performance is significantly improved by adding the RLOP prefetcher. Figure 5 (right) demonstrates the IPC improvement of different prefetchers for multiple SPEC2006 test sets. The minimum performance improvement for the RLOP prefetcher is 5.17%, the maximum performance improvement is 21.23% and the average performance improvement is 12.42%. This shows that the RLOP prefetcher can indeed improve the performance of the program, and that reinforcement learning combined with offset prefetching can be used in prefetcher design to improve the speed of the program.

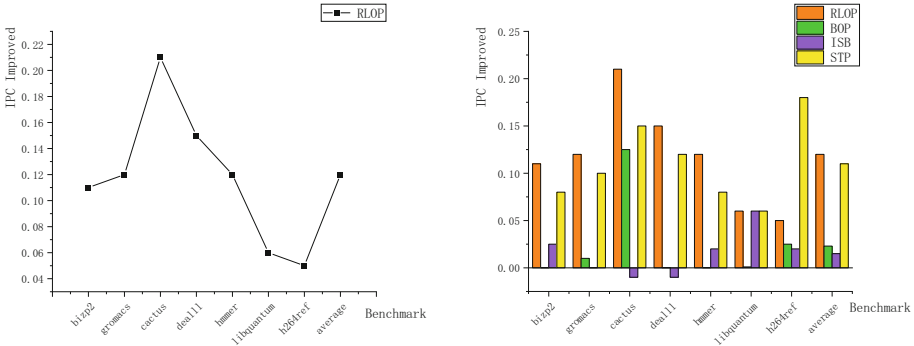


Fig. 5. Comparison of IPC boost with different prefetchers.

### 4.3 Result

RLOP demonstrates improved performance robustness by decreasing the cache failure rate while delivering a relatively significant performance boost. This indicates that the Agent finds superior prefetch offsets during execution, and we can assist the Agent in selecting the optimal prefetch offset by defining a reward scheme. RLOP outperforms STP, ISB, and BOP on average, indicating that the Agent is learning to take purposeful action. The primary disadvantage of RLOP is that the libquantum and h264ref test sets did not achieve relatively significant performance gains, indicating that RLOP did not fully exploit certain program features, possibly because we restricted the action space for better training and the Agent did not learn some better actions.

## 5 Conclusion

By formulating prefetching as a reinforcement learning (RL) problem, we present RLOP, a prefetching framework that integrates offset prefetching and reinforcement learning. RLOP establishes objectives through reward schemes, utilizing multiple program features and system-level feedback information for the Agent to learn to predict memory accesses through prefetching. Our evaluation demonstrates that RLOP not only outperforms three state-of-the-art prefetchers, but also provides significant performance benefits across a broad spectrum of instruction sets and system configurations, with RLOP’s performance advantages stemming from a lightweight hardware architecture. We expect

that RLOP will provide experience for the development of prefetcher designs that combine machine learning with prefetchers that continuously learn by interacting with the system to produce more visionary prefetching strategies. Not only will these prefetchers improve performance and efficiency across a broad spectrum of workloads and system configurations, but they will also relieve system architects of the responsibility of designing complex prefetching mechanisms.

## References

1. Aguilar-Armijo, J., Timmerer, C., Hellwagner, H.: Segment prefetching at the edge for adaptive video streaming, C, vol. 2022-October, pp. 339–344. Thessaloniki, Greece (2022)
2. Laith, M.A., Gratz, P.V., Jimenez, D.A: Slap-cc: Set-level adaptive prefetching for compressed caches, C, vol. 2022-October, pp. 50–58. Olympic Valley, CA, United States (2022)
3. Buyuktanir, T., Aktas, M.S.: A deep learning-based prefetching approach to enable scalability for data-intensive applications, C, pp. 2716 – 2721. Osaka, Japan (2022)
4. Buyuktanir, T., Aktas, M.S.: Mobile prefetching and web prefetching: a systematic literature review. LNCS, C, vol. 13379, pp. 75 – 89, Malaga, Spain (2022)
5. Chacon, G., Garza, E., Jimborean, A., Ros, A., Gratz, P.V., Jimenez, D.A., Mirbagher-Ajorpaz, S.: Composite instruction prefetching, C, vol. 2022-October, pp. 471–478. Olympic Valley, CA, United States (2022)
6. Silver, D., Huang, A., Maddison, C.J., Guez, A., Sifre, L., Van Den Driessche, G., et al.: Mastering the game of Go with deep neural networks and tree search. *Nat. J.* (2016)
7. Silver, D., Hubert, T., Schrittwieser, J., Antonoglou, I., Lai, M., Guez, A., et al.: A general reinforcement learning algorithm that masters chess, J. shogi, and Go through self-play. *Science* (2018)
8. Pugsley, S.H. et al.: Sandbox Prefetching: Safe Run-Time Evaluation of Aggressive Prefetchers, C. HPCA (2014)
9. Michaud, P.: Best-Offset Hardware Prefetching, C. HPCA (2016)
10. Bera, R., Kanellopoulos, K., Nori, A.V., Shahroodi, T., Subramoney, S., Mutlu, O.: Pythia: customizable hardware prefetching framework using online reinforcement learning, C. In: 54th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO). IEEE/ACM (2021)
11. Zouzias, A., Kalaitzidis, K., Grot, B.: Branch prediction as a reinforcement learning problem: why, how and case studies. *J. arXiv:abs/2106.13429* (2021)
12. Sutton, R.S., Barto, A.G.: Reinforcement Learning: An Introduction (Second Edition), C. MIT Press (2018). Chapter 1–3
13. Binkert, N., Beckmann, B., Black, G., et al.: The gem5 simulator. *J. ACM SIGARCH Comput. Architect. News* **39**(2), 1–7 (2011)
14. Butko, A., Garibotti, R., Ost, L., et al.: Accuracy evaluation of gem5 simulator system, C. In: 7th International Workshop on Reconfigurable and Communication-Centric Systems-on-Chip (ReCoSoC), pp. 1–7. IEEE (2012)
15. Henning, J.L.: SPEC CPU2006 benchmark descriptions. *J. ACM SIGARCH Comput. Architect. News* **34**(4), 1–17 (2006)
16. Jain, A., Lin, C.: Linearizing irregular memory accesses for improved correlated prefetching, C. In: Proceedings of the 46th Annual IEEE/ACM International Symposium on Microarchitecture, pp. 247–259 (2013)
17. Liu, X.: Machine Learning Based Cache Prefetcher Design, D. Southeast University, Nanjing (2021)



# A Compliance-Enhancing Approach to Separated Continuous Auditing of Intelligent Endpoints Security in War Potential Network Based on Location-Sensitive Hashing

Hanrui Zhang<sup>1,2(✉)</sup>, Chenrong Huang<sup>3</sup>, and Andrew Lyu<sup>4</sup>

<sup>1</sup> School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210000, China

m15335196643@163.com

<sup>2</sup> School of Information and Communication Engineering, Nanjing Institute of Technology, Nanjing 210000, China

<sup>3</sup> School of Computer Engineering, Nanjing Institute of Technology, Nanjing 210000, China

<sup>4</sup> University of York, Heslington, UK

z12665@york.ac.uk

**Abstract.** The War Potential Network (WPN) is critical infrastructure determining national security. With the recent trend of increasingly tense international situation, frequent occurrences of cyber-attacks, and the proliferation of new intelligent endpoint devices in WPN, the importance of Continuous Auditing (CA) for intelligent endpoints in WPN has become increasingly significant. Several researches have focused on the accuracy of CA. However, the information in WPN intelligent endpoint devices might have sensitive information. Some laws require computer systems to not disclose data containing national secrets, while certain legal regulations demand the protection of personal privacy. In order to meet compliance requirements, specific technologies have to be implemented in CA, while there are existing research gaps in this field. To fill the gap, this research proposed a compliance-enhancing approach based on Locality-Sensitive Hashing (LSH) and clustering method to enhance compliance in CA. In this approach, auditing nodes gathers encoded data which cannot be read by human, while can be analyzed by algorithms to conduct CA. To quantitatively evaluate this approach, this research also introduced an inference attacking method in WPN scenario as threat model. The research also evaluated the influence of the capability of the auditing object and the correctness of the auditing result, to prove our compliance-enhancing approach can achieve relatively good performance in different evaluation dimensions.

**Keywords:** War potential network · LSH · Machine learning · Cybersecurity · Separated continuous auditing

## 1 Introduction

In recent years, multiple incidents of Advanced Persistent Threat (APT) attacks have demonstrated that network attacks occurring within the war potential network are at the forefront of the cybersecurity industry, both in terms of sophisticated exploitation

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2024

Y. Zhang et al. (Eds.): CENet 2023, LNEE 1127, pp. 100–119, 2024.

[https://doi.org/10.1007/978-981-99-9247-8\\_11](https://doi.org/10.1007/978-981-99-9247-8_11)

techniques and well-designed attack chains [1]. In the current landscape where various types of intelligent endpoints are widely utilized in the operations of the war potential network, these intelligent endpoints have become an attack surface that cannot be ignored [2]. Therefore, conducting continuous audits of the security of intelligent endpoints within the war potential network is an essential task in ensuring its resilience against APT attacks. With the increasing focus on network security, the need for privacy protection has also gained significant attention from various sectors [3, 4]. In light of these concerns, China has enacted laws such as the Personal Information Protection Law and the Data Security Law, bringing data security and privacy protection directly into the scope of enforcement [5, 6]. Given the current legal framework for privacy protection, it is necessary to have an in-depth understanding of potential privacy risks associated with continuous auditing of intelligent endpoint security in the war potential network [7]. Technical measures should be employed to mitigate these privacy risks [8, 9]. However, research on privacy protection in the context of continuous auditing for intelligent endpoint security in the war potential network is still relatively limited. In the process of conducting separated continuous audits on the security of intelligent endpoints in the war potential network, certain privacy protection techniques require additional cryptographic means. These computations can introduce significant additional overhead to the devices, affecting their availability. Some privacy protection techniques may also impact the probability distribution of auditing data, thereby affecting the accuracy of security risk detection in continuous auditing. In conclusion, while maintaining the other two characteristic indicators and ensuring that accuracy and availability are not significantly affected, it is meaningful to prioritize data security and privacy protection in the separated continuous auditing of intelligent endpoint security in the war potential network. This should be a significant direction for research on separated continuous auditing technologies for intelligent endpoint security in the war potential network.

This paper presents a technical solution for separated continuous auditing of intelligent endpoints in the war potential network, utilizing a combination of Locality Sensitive Hashing (LSH) and clustering. The solution employs LSH to encrypt the collected auditing data on the client-side, ensuring that most of the plaintext sensitive data remains on the terminal and meeting the requirements of privacy protection at the technical level. Upon receiving the encrypted auditing data on the server-side, preliminary analysis is conducted to filter out data representing the normal operational state of the devices. Subsequently, a semi-supervised learning approach is employed to accomplish the continuous auditing process.

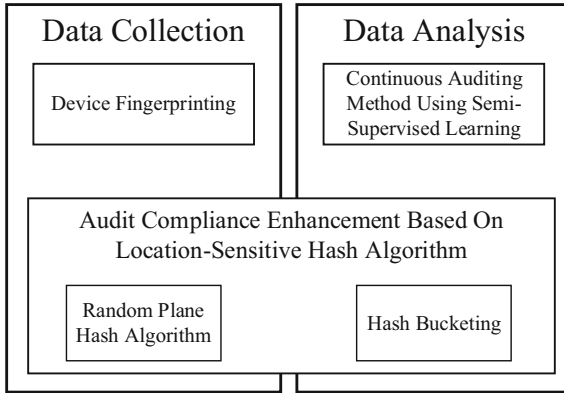
## 2 System Model and Problem Description

### 2.1 System Model

As shown in Fig. 1, the LSH-based audit compliance enhancement scheme permeates the data collection and data analysis stages of the separated continuous auditing for cyber security of the war potential network.

The significance of using LSH for privacy protection lies in:





**Fig. 1.** Architecture diagram for audit process compliance enhancement based on LSH.

- (1) The majority of samples that can form large-scale clusters do not need to transmit plaintext data to the auditing server, thereby protecting the privacy information within this data.
- (2) Although the use of LSH adds a certain amount of additional burden to intelligent endpoints, compared to other privacy protection techniques based on cryptography, LSH still demonstrates significant advantages in balancing smart terminal availability and continuous auditing accuracy.

In this part, we will examine the phenomenon of requiring the use of plaintext data for analyzing suspected abnormal sample data in this proposed approach: Network attacks targeting war potential networks often utilize novel attack pathways and payloads that have not been encountered before. Therefore, for suspected malicious payloads, a comprehensive security analysis is required to determine their security risk level. Additionally, the war potential network is crucial for national security and social stability. Hence, detailed analysis of potential malicious payloads is necessary to continuously safeguard the network's security and enhance its resilience against security risks. If a suspicious payload is indeed identified as malicious, further threat intelligence and hunting are needed to expand threat intelligence. If the payload is not malicious, optimization of existing threat assessment engines is necessary to prevent false positives triggered by such novel payloads. In summary, the analysis of a large number of unknown malicious payloads that may occur in the war potential network still requires the expertise of experienced cybersecurity professionals for analysis and judgment. Therefore, collecting plaintext data for the assessment of unknown risks is a necessary step in conducting intelligent endpoint-separated security continuous auditing for the war potential network. In relevant laws and regulations, similar scenarios in normal business operations, such as regular inspections of critical infrastructure or audits of users or devices accessing critical network assets, can collect plaintext data following the principle of minimization, which means collecting only the minimum necessary data required for business purposes after obtaining authorization. The application of LSH enables the separated continuous auditing for intelligent endpoints security to only collect a small amount of plaintext data from suspicious payloads instead of collecting the entire plaintext data. This ensures that

continuous auditing work can follow the principle of minimization to meet privacy protection requirements. It adequately satisfies the practical and compliance needs for data security.

## 2.2 Problem Description

Although there have been few studies specifically focused on data security and privacy protection in the context of continuous auditing for war potential network intelligent endpoints, some relevant research has addressed the security and privacy risks in continuous auditing data. Wang et al. [10] proposed a technical solution using aggregatable signature-based broadcast encryption method to achieve data security in continuous auditing of cloud storage. However, the study did not explicitly specify the specific data security risks involved in cloud storage auditing. Yan et al. [11] proposed a novel certificateless PDP protocol that effectively audits the integrity of shared data within a working group while ensuring user privacy. However, this study only focuses on anonymizing user identities during communication and does not consider the presence of sensitive information in communication payloads. Anbuchelian et al. [12] proposed a scheme to audit the integrity of encrypted data in cloud storage using a new secure cryptographic hash algorithm. However, this research's auditing objective only focuses on the integrity of ciphertext data and does not possess the capability to detect more complex network attacks. Wang et al. [13] proposed a ciphertext-based public auditing method for data protection, utilizing an innovative cryptographic technique to secure communication between the cloud client and auditing node. However, this study primarily focuses on the integrity of storage and data. Hussien et al. [14] proposed a public auditing method for securing cloud storage data, enabling auditing nodes to conduct integrity audits on cloud storage using a homomorphic linear authenticator (HLA) method. However, on one hand, HLA imposes high computational resource requirements, making it difficult to run on some intelligent endpoints. On the other hand, their approach allows auditing nodes to access the full plaintext data of the auditing target during HLA processing, making the security guarantee of this approach for intelligent endpoint data unclear.

In summary, the deficiencies in existing research related to secure continuous auditing for war potential network intelligent endpoints can be categorized into the following six points:

1. Lack of specific descriptions regarding data security risks in auditing tasks, resulting in insufficient clarity in demonstrating the effectiveness of data security guarantees.
2. Lack of specific experimental or case validations of the data security and privacy protection effectiveness of the proposed technical solutions, relying only on theoretical proofs.
3. Narrow coverage of data security and privacy protection, such as focusing solely on anonymizing user identities in communication protocols while ignoring plaintext data in communication payloads.
4. Limited auditing capabilities, restricted to checking file integrity, lacking the ability to detect complex network attacks targeting modern war potential network intelligent endpoints.
5. High computational resource requirements of the proposed solutions, making them impractical to run on intelligent endpoints.

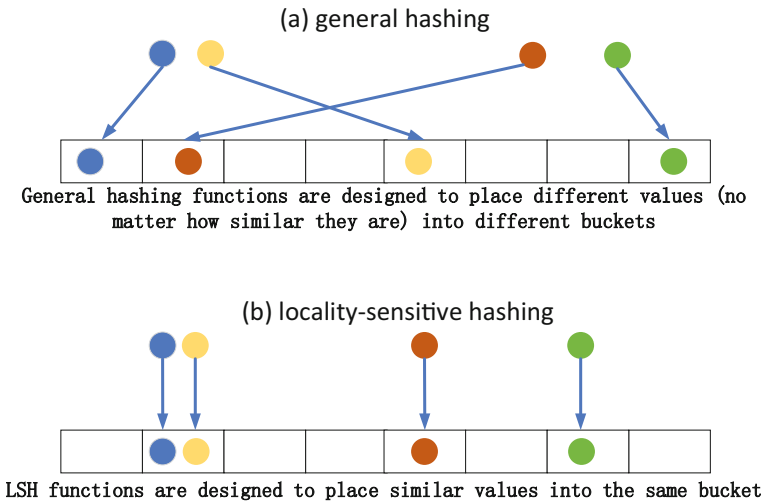
6. Ambiguous trust systems and a lack of attack models. For example, some studies, even when transmitting ciphertext to auditing nodes as part of the encryption process, still allow auditing nodes to access the full plaintext data.

In view of this, this paper will improve upon the six points to advance the research on data security and privacy protection in the separated continuous auditing of intelligent endpoints security in the war potential network. It aims to address certain issues pertaining to this topic and promote their resolution.

### 3 Data Security and Privacy Protection Scheme Based on LSH

#### 3.1 Locality Sensitive Hashing

LSH is a technique used for efficient approximate nearest neighbor search. It is widely applied to similarity search problems in large-scale datasets, such as image recognition, recommendation systems, and text clustering, among others [15]. As shown in Fig. 2, unlike the typical hash algorithm where the position distribution of plaintext is unrelated to its position distribution in the hash space, LSH is almost the opposite. The basic idea of the LSH is to map data points to the hash space in a way that similar data points have a higher probability of falling into the same bucket in the hash space. By doing so, the similarity search problem can be transformed into a bucket search problem in the hash space, significantly reducing the time complexity of the search.



**Fig. 2.** **a** The plaintext and hash space mapping for a typical hash algorithm. **b** The plaintext and hash space for the LSH algorithm.

The key steps of the LSH include the design of hash functions and the construction strategy of buckets. Hash functions should satisfy certain properties to ensure that similar data points are mapped to nearby locations in the hash space, while dissimilar data points

are mapped to distant locations. Commonly used LSH hash functions include random projection hashing and hashing signatures.

Random Projection Hashing is a commonly used type of hash function in LSH. Its main idea is to map data points to a lower-dimensional space through random projection, thereby achieving an approximate preservation of similarity. The process of Random Projection Hashing is as follows:

- (1) Randomly generate a hyperplane of dimension  $d$ , which is represented by a normal vector (a vector of length  $d$ ).
- (2) For a given data point  $x$ , calculate its projection onto the hyperplane, which results in a one-dimensional value.
- (3) Use the projection result as the hash value and assign the data point to different buckets based on the hash value.

The characteristic of Random Projection Hashing is that it maps similar data points in high-dimensional space to nearby locations in a lower-dimensional space, while dissimilar data points are mapped to distant locations. By appropriately selecting the number and dimension of hyperplanes, one can adjust the sensitivity of the hash function and the storage space consumption. In LSH, multiple random projection hash functions are typically used to construct hash tables or hash buckets. By performing projections and hashing operations on different hash functions, the probability of data points falling into the same bucket can be increased, thereby improving the accuracy and efficiency of similarity search. However, using the plane hashing technique to handle data results in dimensionality reduction, which leads to a loss of information and may affect the final data analysis results. Hashing Signatures is another commonly used type of hash function in LSH. It generates a fixed-length binary signature by applying hash operations to data points, representing the features of the data points. The process of Hashing Signatures is as follows:

- (1) Select a set of hash functions. Each hash function maps a data point to a binary bit (0 or 1).
- (2) For a given data point  $x$ , apply the mapping of each hash function to obtain a binary bit string.
- (3) Concatenate the binary bit string to form a fixed-length binary signature.

The characteristics of hash signatures include small storage space and efficient computation speed. By appropriately selecting the quantity and nature of hash functions, the sensitivity and collision probability of hash signatures can be adjusted. In LSH, multiple hash signatures are typically used to construct hash tables or hash buckets. By applying hash operations on different hash functions, the probability of data points falling into the same bucket can be increased, thereby improving the accuracy and efficiency of similarity search.

The construction of buckets is achieved by assigning data points to different buckets based on the mapping results of hash functions. During the search, only the hash result of the query point needs to be matched to find the bucket with the same hash result as the query point. Further search and comparison are performed within the bucket to find approximate nearest neighbor data points. The size and quantity of buckets need to be set reasonably. If the buckets are too small, it may lead to a large number of data

points being mapped to the same bucket, increasing the possibility of collisions and errors. If the buckets are too large, it may reduce the distinguishability of similarities. Therefore, it is necessary to adjust the size and quantity of buckets appropriately based on the scale and characteristics of the dataset, as well as the sensitivity of the hash functions. In addition, since the mapping results of hash functions are finite, different data points may be mapped to the same hash value or similar hash values, causing conflicts within the buckets. To handle conflicts, open addressing, linked lists, or other conflict resolution methods can be used. These methods ensure that similar data points are placed in the same bucket and support fast searching within the bucket. Lastly, LSH is sensitive to the distribution of data. If the data points are unevenly distributed in space, some buckets may become overcrowded while others remain relatively empty. This situation can affect search efficiency and accuracy. To address this issue, adjusting the hash functions, redistributing the buckets, or using methods that dynamically adjust bucket sizes can be considered to achieve a balanced data distribution. In summary, LSH has the advantage of efficiently performing approximate nearest neighbor search on large-scale datasets, with good time and space complexity. However, the performance of LSH is greatly influenced by the design of hash functions and the process of bucket partitioning. Its effectiveness is affected by factors such as parameter selection and data distribution, requiring optimization based on specific application scenarios.

The data sampling scheme used in the study includes the type and duration of executing processes. We have listed the names of 176 common Android device applications and processes, and assigned a unique number to each process name. For example, the process “com.android.mms” is assigned the number 1, “com.android.providers.calendar” is assigned the number 2, and so on. Any other processes not included in the list are assigned the number 177. If process 1 runs for  $l$  seconds, process 2 runs for  $m$  seconds, and the unlisted process runs for  $n$  seconds, we represent it as a tensor of size  $1 \times 177$ , denoted as  $[l, m, \dots, n]$ . During normalization, we adjust the upper and lower boundaries based on the actual values in order to distribute the values as evenly as possible between 0–1. Therefore, the data collected using this fingerprinting scheme belongs to a high-dimensional dense dataset. As the dimensionality of the features increases, the data samples tend to exhibit increased sparsity in high-dimensional space, known as the “curse of dimensionality”. In dense data, the samples are distributed more densely in high-dimensional space, resulting in a lower curse of dimensionality problem. Since random projection hashing maps high-dimensional data to low-dimensional space, the tight distribution of dense datasets makes it more likely for similar samples to maintain a closer distance in low-dimensional space, thereby improving the effectiveness of random projection hashing.

Furthermore, in high-dimensional space, the correlation between features can cause data samples to become similar across different dimensions, making them difficult to distinguish. Random projection hashing reduces the correlation between features to some extent through random projection operations, thus improving the discriminability of samples. In dense data, due to relatively low inter-feature correlations, random projection hashing is more likely to produce better discriminative effects through random projection. Lastly, random projection hashing can map high-dimensional data to low-dimensional space, but the resulting dimensionality may still be high. In dense

datasets, the mapping results of samples in low-dimensional space may be more dispersed, reducing conflicts between similar samples. Additionally, while using multiple hash algorithms in LSH may improve the accuracy of LSH bucketing, it also significantly increases computational resources and storage costs. Therefore, for the data collected using this scheme, applying the random projection hashing algorithm for LSH is more suitable. Considering that the part of processing data using LSH is performed on smart terminal devices (otherwise, the auditing node could obtain the full plaintext data), and smart terminal devices are highly sensitive to computational resources and storage costs, deploying a solution that uses multiple hash algorithms for LSH on the device terminal is challenging. For the implementation of LSH on smart terminal devices, this study utilizes the Annoy library. Annoy [16] is a fast and lightweight approximate nearest neighbor library that supports LSH. It provides C++ and Python interfaces and can be used on Android and iOS platforms. The application of LSH in this solution aims to process plaintext data and achieve data anonymization. This enables the auditing nodes that handle the data processing to avoid directly dealing with plaintext data, thereby mitigating privacy risks from a technical perspective. Besides LSH, there are other techniques that can achieve similar goals, such as differential privacy [17], secure multiparty computation, and homomorphic encryption [18–20].

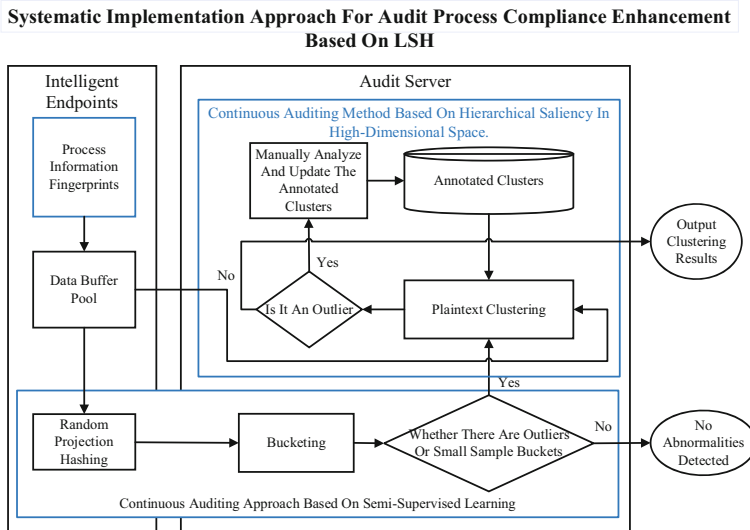
### 3.2 Enhancing Audit Process Compliance Based on LSH

By analyzing the number of hash values in LSH buckets, it can be observed that some buckets contain only a few samples corresponding to hash values. Based on the principles of LSH, it can be inferred that these hash values correspond to samples with significant differences in their plaintext fingerprints' feature space compared to other samples. Since LSH utilizes random plane hashing, the distance between buckets that contain hash values is lower than the distance between non-adjacent buckets in subsequent bucketing strategies. Correspondingly, the plaintext fingerprints corresponding to hash values in these discrete buckets exhibit significant differences in the feature space compared to the plaintext fingerprints corresponding to hash values in other buckets that are more densely distributed within a certain region. Therefore, in the context of secure continuous auditing, if a few hash values exist in these discrete buckets, the corresponding plaintext fingerprints may represent infrequently occurring operational states.

Now, let's discuss the viewpoint that discrete samples represent highly likely abnormal operating states: If the majority of smart terminals related to the War Potential Network's business are in abnormal operating states, it would be noticeably indicative of a severe security situation from a business perspective. In such cases, the emergency response process should be immediately initiated to conduct a more comprehensive and thorough security audit and threat detection, without the need to maintain continuous auditing. Therefore, under the premise of normal ongoing continuous auditing, most smart terminal devices should be in a normal operating state. Similarly, for similar devices connected to the same War Potential Network, the fingerprints collected under normal operating conditions should be close to each other, and these fingerprints should exhibit a relatively concentrated distribution in the feature space. On the other hand, the

operating states represented by discrete samples with a large distance from the majority of samples in the feature space demonstrate significant differences from the normal operating state, indicating a high probability of corresponding to an abnormal state.

After the initial screening of input data using LSH bucketing, if there are discrete buckets or buckets that only contain a small number of samples, and these buckets have a significant distance from other buckets, it is necessary to perform in-depth analysis on the plaintext data using clustering algorithms. At this point, the plaintext data is extracted from the audit node to the data cache pool of the terminal. In this paper, we employ the high-dimensional clustering algorithm based on hierarchical activity proposed in chapter “Current Challenges in Federated Learning: A Review” to analyze the plaintext data, ensuring the accuracy of the audit results.



**Fig. 3.** Systematic implementation approach for audit process compliance enhancement based on LSH.

Therefore, this paper combines the LSH-based audit process compliance enhancement method with process information fingerprints and a continuous audit scheme based on semi-supervised learning, thus proposing a systematic implementation plan for enhancing audit process compliance based on LSH. The technical process of the implementation plan is illustrated in Fig. 3. Firstly, the high-performance non-intrusive asynchronous monitoring data processing module in the smart terminal devices periodically collects and generates fingerprints from the plaintext data. These fingerprints are then stored temporarily in the data buffer pool of the terminal device. Once the data buffer pool accumulates fingerprints from multiple sampling periods, LSH is applied to these fingerprints, resulting in an LSH hash table that stores the hash values of the data nodes in buckets. The encrypted LSH hash table is then transmitted to the audit server for analysis. The audit server performs the initial clustering by using the hash-based bucketing. If no outliers or small clusters are detected, it notifies that no anomalies have

been found. However, if outliers or small clusters are identified, the audit server retrieves the plaintext data corresponding to that record from the intelligent terminal data buffer pool. The retrieved data is then audited according to the continuous audit scheme based on semi-supervised learning.

## 4 Experimental Analysis

The effectiveness of the systematic implementation approach for enhancing the compliance of the audit process based on LSH can be evaluated from three dimensions: audit process compliance, audit object availability, and audit result accuracy, with audit process compliance being the primary objective of using LSH. However, on one hand, LSH can generate significant resource overhead on smart terminal devices, thereby reducing device availability and stability. On the other hand, applying LSH for hashing plaintext data can lead to information loss, affecting the accuracy of audit results. Therefore, there is a trade-off among audit process compliance, audit object availability, and audit result accuracy. A comprehensive evaluation of the systematic implementation approach using LSH-based enhancements can assess the performance in terms of device resource overhead and audit result accuracy, providing a measure of whether the technical solution can achieve a balance among audit process compliance, device availability, and continuous audit accuracy.

### 4.1 Compliance Verification of the Auditing Process

#### 4.1.1 Experimental Design

To verify the compliance of the audit process, it is necessary to simulate an attack scenario targeting sensitive data in the audit process. The effectiveness of the proposed method in defending against attacks in this scenario will be evaluated to measure its protective effect on audit process compliance. In this experiment, it is assumed that the audit node itself is completely untrusted, meaning the audit node can employ various techniques and make full use of the information it possesses to carry out inference attacks.

Experimental Evaluation Criteria:

The process fingerprint scheme employed in this paper is a device fingerprinting scheme aimed at smart terminals. For the fingerprint constructed by the process fingerprinting scheme, each sample is a 194-dimensional array. Below is an example of a fingerprint data, selecting 50 plaintext data about process information:

[0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0.2, 0.45, 0.67, 0.22, 0.64, 0.52, 0.28, 0.89, 0.32, 0.83, 0.02, 1, 0.63].

Each element of the fingerprint data represents the specific process's runtime status during the fingerprint construction. For example:

- The 1st element represents the “com.spotify.music” process.
- The 2nd element represents the “com.netflix.mediaclient” process.
- ...
- The 19th element represents the “com.google.android.gms” process.
- The 20th element represents the “com.google.android.apps.photos” process.





This reverse operation scheme attempts to infer a plaintext corresponding to a ciphertext by combining known plaintext-ciphertext mappings using the same algorithm. Under the specific privacy model associated with this research, it can be used to attempt to derive the plaintext corresponding to a random plane hash algorithm ciphertext. In the experiment, 100 ciphertext records were selected and an attempt was made to reverse infer their corresponding plaintexts. By measuring the success rate of the inference attacks, the effectiveness of the proposed LSH-based audit process compliance enhancement method in enhancing audit process compliance can be evaluated in reverse.

The experimental comparison is as follows:

This experiment evaluates the effectiveness of the proposed approach in defending against specific inference attack scenarios. Due to the lack of similar studies, only a longitudinal comparison is conducted to validate the effectiveness of the proposed method in ensuring audit process compliance.

The controlled variables for the experiment are as follows:

Number of ciphertext data for inference attacks: 100.

Experimental dataset:

The dataset consists of 20,000 process fingerprints from this study, which have been scattered using random plane hashing and their plaintext-ciphertext mappings are known as prior knowledge. Additionally, 100 ciphertext data generated by scattering process fingerprint using random plane hashing are used as the test data.

The experimental control group is designed as follows:

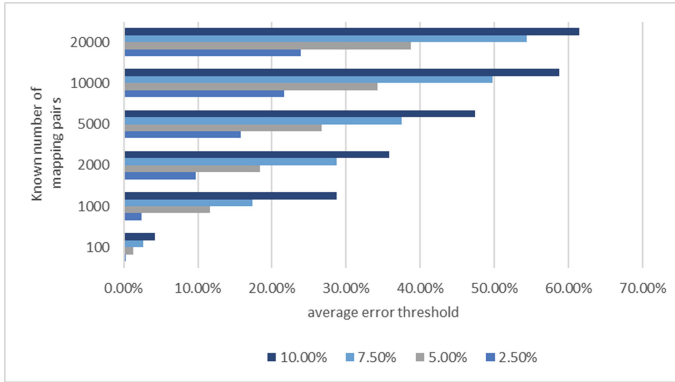
In this experiment, we consider two dimensions that can affect the effectiveness of inference attacks: the number of known mappings held by the audit system and the allowable error threshold for inference accuracy. Therefore, we set up control groups based on these two dimensions. The number of known mappings includes six values: 100, 1000, 2000, 5000, 10000, and 20000. It was observed in the experiment that the success rate of inference attacks slows down as the number of known mappings exceeds 10000, so we do not include values greater than 20000. The average error threshold includes four values: 2.5%, 5.0%, 7.5%, and 10.0%. It was found that when the difference between the inferred plaintext and the original plaintext exceeds 10%, there is already a significant discrepancy between the inferred plaintext and the true data, so we do not investigate success rates of inference attacks with error thresholds above 10%.

#### **4.1.2 The Experimental Results**

The experimental results are shown in and Fig. 4. Due to the low dimensionality of the ciphertext, there is no curse of dimensionality issue when calculating distances, allowing for accurate assessment of the similarity between ciphertexts. Therefore, when an adequate number of known mappings is available, the search for similar ciphertext mappings yields favorable results and can provide some inference capabilities for the plaintext.

#### **4.1.3 Experimental Analysis**

The experimental results intuitively reflect the success rate of inference attacks with changes in the number of known mappings and the average allowable error. As the



**Fig. 4.** Attempting to infer the accuracy of plaintext based on the information possessed by audit nodes.

number of known mappings increases, the success rate of inference attacks rises rapidly. However, as the number of known mappings continues to increase, the growth rate of the success rate slows down, and the increase becomes less significant in the range of 10,000 to 20,000 mappings. When the average allowable error rate increases, the number of recognized successful inference attacks also increases. Even with an average allowable error rate of 2.5%, when the auditing node possesses the specific implementation of the hash scattering algorithm and a large number of plaintext-ciphertext mappings, there is still close to a 25% probability of inferring the plaintext data.

If restrictions are placed on the number of known mappings, the LSH-based compliance-enhancement method for continuous auditing of the war potential network of intelligent endpoints can provide effective privacy protection. Therefore, the auditing node should periodically delete fingerprint records of retrieved plaintext data to ensure the effectiveness of privacy protection at the technical level. For example, by limiting the number of stored plaintext-ciphertext mappings to below 100, it becomes nearly impossible to accurately reverse-engineer the plaintext data, even with the knowledge of plaintext data and encryption algorithm information at the auditing node.

## 4.2 Compliance Verification of the Auditing Process

This experiment aims to quantitatively evaluate the device resource overhead caused by the technical solution introduced in this paper. It is conducted to measure the dual-objective optimization effect of process fingerprinting and the compliance enhancement method based on LSH in addressing the conflict between audit target availability and audit process compliance in the separated continuous auditing for intelligent endpoints security in the war potential network.

### 4.2.1 Experimental Design

Evaluation Criteria for the Experiment:

The experiment assesses the device resource overhead caused by data security and privacy protection techniques, aiming to measure the impact of the corresponding techniques on the audit object's availability. Since audit nodes are typically deployed on high-performance servers and are not likely to become performance bottlenecks, the evaluation of resource overhead primarily focuses on the execution of Locality Sensitive Hashing (LSH) on smart terminal devices. For power-sensitive smart terminals, the evaluation should include additional metrics beyond commonly used indicators such as CPU usage and memory usage, such as power consumption, to capture the impact on resources caused by the algorithm.

Comparison of Experimental Approaches:

As a comparison, this experiment will evaluate three different approaches: Multi-Party Secure Computation based on MP-SPDZ Mobile [21], Homomorphic Encryption based on HELib [22], and Differential Privacy based on Google Privacy Sandbox [23]. MP-SPDZ Mobile is a library designed for secure multi-party computation, known for its high performance and strong security. It is a version specifically designed for mobile devices and can run on smartphones, offering various secure multi-party computation protocols and optimizations suitable for diverse application scenarios. HELib is a powerful homomorphic encryption library that supports fully homomorphic encryption. It enables homomorphic encryption computations on mobile devices and supports a wide range of homomorphic operations. The HELib library is implemented in C++ and can be compiled and deployed on the Android platform. Google Privacy Sandbox is a collection of privacy protection technologies and APIs introduced by Google. It aims to protect user privacy while providing personalized services. It includes various differential privacy techniques and corresponding APIs that can be used on the Android platform. Both multi-party secure computation and homomorphic encryption involve operations on devices that generate ciphertext conforming to the corresponding computation protocols. Differential privacy, on the other hand, involves adding sufficient random noise to the data to protect privacy while maintaining statistical accuracy.

Control variables for the experiment are as follows:

1. SmoothPrint fingerprints: 100 identical fingerprint records.
2. Device types: 3 different models.

The experimental dataset is as follows:

This experiment only focuses on validating the performance overhead caused by privacy-enhancing computations and the compliance-enhancing method based on LSH described in this chapter. It does not involve the dataset.

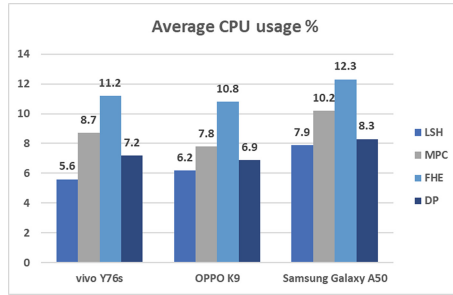
The experimental control group is designed as follows:

Based on the devices used to run each evaluated method, three control groups have been constructed.

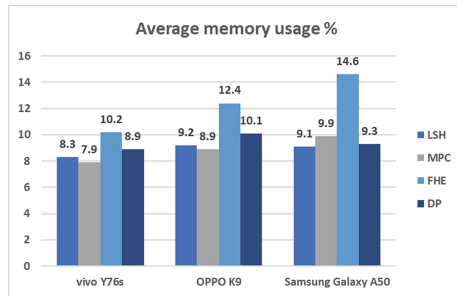
### 4.2.2 Experimental Results

In the experimental results, the multi-party secure computation scheme is denoted as MPC, fully homomorphic encryption scheme is denoted as FHE, differential privacy

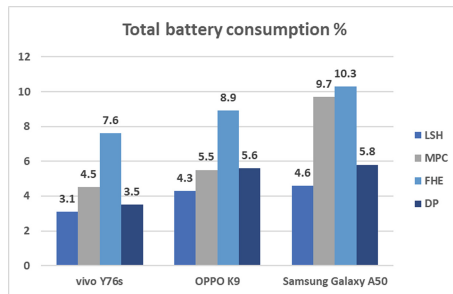
scheme is denoted as DP. The comparison of resource overhead caused by LSH is shown in Figs. 5, 6, 7 and 8.



**Fig. 5.** Average CPU usage caused by using privacy protection methods on different device models.



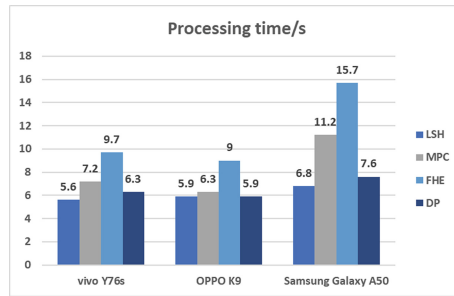
**Fig. 6.** Average memory usage caused by using privacy protection methods on different device models.



**Fig. 7.** Total battery consumption caused by using privacy protection methods on different device models.

### 4.2.3 Experimental Analysis

In a horizontal comparison, the system-level implementation of compliance enhancement in the audit process based on LSH incurs relatively lower additional resource



**Fig. 8.** Processing time caused by using privacy protection methods on different device models.

overhead on devices compared to the differential privacy-based approach. On the other hand, secure multi-party computation and homomorphic encryption schemes impose significant additional resource overhead on devices. In comparison to differential privacy, LSH achieves better performance due to its relatively lower algorithm complexity. However, LSH is generally limited to approximate nearest neighbor search scenarios, whereas data processed with differential privacy can be flexibly used with other clustering or classification algorithms. Thus, LSH may not be as flexible in its application scenarios as differential privacy. However, in terms of the additional resource overhead dimension in this specific research context and task, LSH performs better.

In a vertical comparison, on a resource-constrained device like the Samsung Galaxy A50, the time required to run the computationally intensive homomorphic encryption scheme is much higher compared to the running time of other schemes. Therefore, for devices with more severe resource constraints, the significant resource overhead of homomorphic encryption has a greater impact on device availability, while LSH does not exhibit this phenomenon. It is speculated that the system overhead caused by LSH has not reached the threshold where it significantly affects device availability.

In summary, the system-level implementation of compliance enhancement in the audit process based on LSH can effectively ensure the availability of audit targets in the separated continuous auditing for intelligent endpoints security in the war potential network. The system-level implementation of compliance enhancement based on LSH demonstrates good performance in both audit target availability and audit process compliance.

### 4.3 Sample Verification of Audit Result Accuracy

This experiment aims to evaluate the accuracy of audit results in the systematic implementation of the audit process enhancement based on Locality Sensitive Hashing (LSH).

#### 4.3.1 Experimental Design

The experimental evaluation criteria are as follows:

This paper classifies the following operating states: normal operation, launching DDoS attacks, running mining programs, running non-system root processes, background downloading of malicious applications, deceived phone charges, stolen GPS information, frequent pop-up ads, and other malicious behaviors. The accuracy of the trained system's evaluation on the classification test samples is evaluated using recall rate, precision rate, and accuracy-related metrics.

The experimental comparative scheme is as follows:

Since no research targeting anomalous operating states in terms of network security dimensions has been found, this experiment does not involve comparative schemes. It only evaluates the performance that the proposed technical solution can achieve in the task.

The controlled variables for the experiment are as follows:

Number of devices participating in the experiment: 129 (including virtual machines).

Data sampling frequency: 5 min per sample.

Data collection duration: 96 h.

Simulation of device operation method: Monkey tool.

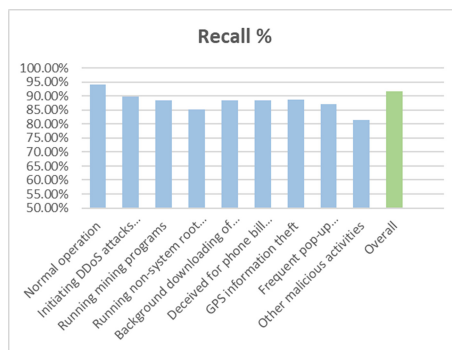
PCA dimension reduction: 20 dimensions.

The experimental datasets are as follows:

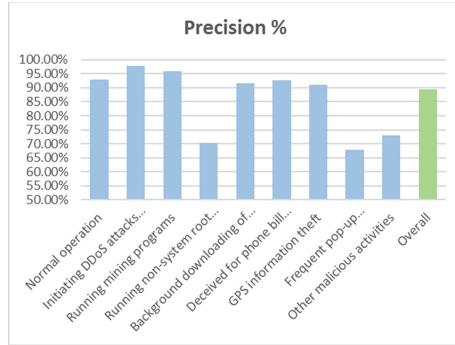
Training dataset: 5560 malicious software samples from the Drebin [24] project. The Drebin dataset is widely used for Android malware detection and analysis. It was developed by researchers at the University of Duisburg-Essen in Germany and aims to provide a comprehensive and diverse dataset for the study of Android malware. The Drebin dataset contains approximately 5,560 Android application samples, including both malware and benign software.

Prediction dataset: 2780 malicious software samples released after 2022 from Koodous [25].

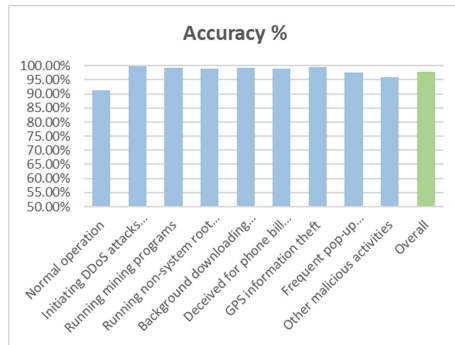
The experimental results are shown in Table 4.3, and the corresponding outcomes are illustrated in Figs. 9, 10, 11 and 12.



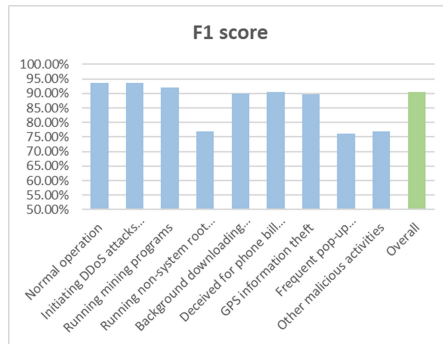
**Fig. 9.** Recall of anomaly detection in the systematic implementation approach for audit process compliance enhancement based on LSH.



**Fig. 10.** Accuracy of anomaly detection in the systematic implementation approach for audit process compliance enhancement based on LSH.



**Fig. 11.** Precision of anomaly detection in the systematic implementation approach for audit process compliance enhancement based on LSH.



**Fig. 12.** F1 score of anomaly detection in the systematic implementation approach for audit process compliance enhancement based on LSH.



## References

1. Run, W., Yuhang, J.: A brief discussion on the new trends in network security under the background of cyber warfare. *Netw. Secur. Technol. Appl.* **269**(05), 162–164 (2023)
2. Xin'an, Z.: The Russo-Ukrainian conflict rings the alarm bell for safeguarding network security. *China Inf. Secur.* **151**(06), 5 (2022)
3. Dengguo, F., Min, Z., Hao, L.: Big data security and privacy protection. *Chinese J. Comput.* **37**(01), 246–258 (2014)
4. Xiuxia, T., Xiaoling, W., Ming, G., et al.: Database services: security and privacy protection. *J. Softw.* **21**(05), 991–1006 (2010)
5. Zhenfu, C., Xiaolei, D., Jun, Z., et al.: Research progress on big data security and privacy protection. *J. Comput. Res. Develop.* **53**(10), 2137–2151 (2016)
6. Handong, W.: Institutional arrangements and legal regulations in the era of artificial intelligence. *Legal Sci. (J. Northwest Univ. Polit. Sci. Law)* **35**(05), 128–136 (2017)
7. Yanping, X., Zhaofeng, M., Zhonghua, W., et al.: Overview of security for android smart terminals. *J. Commun.* **37**(06), 169–184 (2016)
8. Guang, Y., Geng Guining, D., Jing, et al.: Security threats and measures in the internet of things. *J. Tsinghua Univ. (Sci. Technol.)* **51**(10), 1335–1340 (2011)
9. Junzhou, L., Ming, Y., Zhen, L., et al.: Cyber security system and key technologies in cyberspace. *Sci. Sin. Inf.* **46**(08), 939–968 (2016)
10. Wang, S., Chen, D., Wang, Z., et al.: A new solution of privacy-preserving public auditing scheme for cloud storage security. *Telecommun. Sci.* **28**(9), 15–21 (2012)
11. Yan, H., Liu, Y., Zhang, Z., et al.: Efficient privacy-preserving certificateless public auditing of data in cloud storage. *Secur. Commun. Netw.* **2021**, 1–11 (2021)
12. Anbuchelian, S., Sowmya, C.M., Ramesh, C.: Efficient and secure auditing scheme for privacy preserving data storage in cloud. *Clust. Comput.* **22**, 9767–9775 (2019)
13. Wang, B., Li, B., Li, H.: Panda: Public auditing for shared data with efficient user revocation in the cloud. *IEEE Trans. Serv. Comput.* **8**(1), 92–106 (2013)
14. Hussien, Z.A., Jin, H., Abduljabbar, Z.A., et al.: Public auditing for secure data storage in cloud through a third party auditor using modern ciphertext. In: 2015 11th International Conference on Information Assurance and Security (IAS), pp. 73–78. IEEE (2015)
15. Datar, M., Immorlica, N., Indyk, P., et al.: Locality-sensitive hashing scheme based on p-stable distributions. In: Proceedings of the Twentieth Annual Symposium on Computational Geometry, pp. 253–262 (2004)
16. Annoy. <https://github.com/spotify/annoy>, Accessed: 2023-05-01
17. Dwork, C.: Differential privacy: a survey of results. In: Agrawal, M., Du, D., Duan, Z., Li, A. (eds.) TAMC 2008. LNCS, vol. 4978, pp. 1–19. Springer, Heidelberg (2008). [https://doi.org/10.1007/978-3-540-79228-4\\_1](https://doi.org/10.1007/978-3-540-79228-4_1)
18. Yao A C. Protocols for secure computations. In: 23rd annual symposium on foundations of computer science (sfcs 1982), pp. 160–164. IEEE (1982)
19. Yao A C C. How to generate and exchange secrets. In: 27th Annual Symposium on Foundations of Computer Science (Sfcs 1986), pp. 162–167. IEEE (1986)
20. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, pp. 169–178 (2009)
21. Araki, T., Furukawa, J., Lindell, Y., et al.: High-throughput semi-honest secure three-party computation with an honest majority. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 805–817 (2016)
22. Halevi S, Shoup V. Algorithms in helib. In: Advances in Cryptology—CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17–21, 2014, Proceedings, Part I, vol. 34, pp. 554–571. Springer, Berlin (2014)

23. The Privacy Sandbox. <https://privacysandbox.com/>. Accessed: 2023-05-01
24. Drebin Dataset. <https://www.sec.cs.tu-bs.de/~danarp/drebin/index.html>. Accessed: 2023-05-01
25. Koodous. <https://koodous.com/>. Accessed: 2023-05-01



# Design and Implementation of an Embedded Streaming Terminal

Yan Shen<sup>(✉)</sup>, Tai Qin, and Min Chen

Wuhan Digital Engineering Institute, Hubei 430074, China  
359046703@qq.com

**Abstract.** Expensive and relatively rigid specialized processing devices are used to perform audio and video processing functions in traditional audio and video systems. These devices not only have limited configurability but also lack openness to the users. In this paper, an embedded streaming terminal is implemented by embedded chips, combining software and hardware. It integrates audio and video capture, encoding/decoding, transmission, and image processing functions. The encoding/decoding, transmission, and fusion processing functions are standardized and quantifiable, forming a versatile processing terminal. It is constructed through quantity stacking and Ethernet switch cascading, enabling functions such as video switching, video splicing, video overlay, PIP (Picture-in-Picture), PBP (Picture-by-Picture), and seamless zooming. The terminal exhibits excellent performance in terms of encoding/decoding latency, bitrate control, and overlay channels, ensuring the flexibility and scalability of audio and video business systems.

**Keywords:** Embedded · Audio and video business · Streaming · Terminal

## 1 Introduction

In recent years, with the rapid development of audio and video processing technology and network communication technology, the application of video business processing are increasing, and the functionality has become complex. Traditional audio and video systems typically rely on expensive and relatively fixed-function dedicated processing equipment. These types of devices not only have limited configurability but also lack openness to users, resulting in limited flexibility, scalability, and compatibility with various functions in the later applications of such systems.

To address the issues aforementioned, current audio and video transmission and processing technologies have gradually adopted a distributed and digital approach. This has resulted in audio and video systems based on embedded business processing terminals. These terminals employ a combination of software and hardware to standardize the design of video encoding and decoding, video transmission, and video fusion processing capabilities. The aim is to create quantifiable and versatile processing terminals. They are constructed through quantity stacking and Ethernet switch cascading, and their management and configuration are achieved through network control interfaces. This approach enhances the flexibility, scalability, and ability to customize deeply tailored applications in audio and video business systems.

## 2 Research Status at Home and Abroad

In terms of video business processing, scholars both domestically and internationally have conducted extensive research. Ping [1] studied a system based on streaming video conferencing mobile terminals, Weilun [2] and others studied a vehicle embedded streaming terminal based on FFMPEG, and Heng [3] studied a mobile streaming live streaming system based on multiple terminals. All three implemented video decoding using software libraries, with strong compatibility but limited performance. Lize [4] studied streaming media terminals based on the improved TFRC protocol, focusing on solving data transmission in network environments with severe latency jitter. Yao [5] studied audio and video synchronization technology for airborne entertainment systems, with a focus on synchronization control between multiple decoding terminals.

In this article, the streaming media terminal adopts a combination of software and hardware to achieve a minimum unit for audio and video business processing. As shown in Fig. 1, both the input and output ends of the audio and video are connected to the terminal. The terminal completes tasks such as audio and video encoding, decoding, and fusion processing. These functions are uniformly configured online by a centralized operations and maintenance management platform for each basic unit.

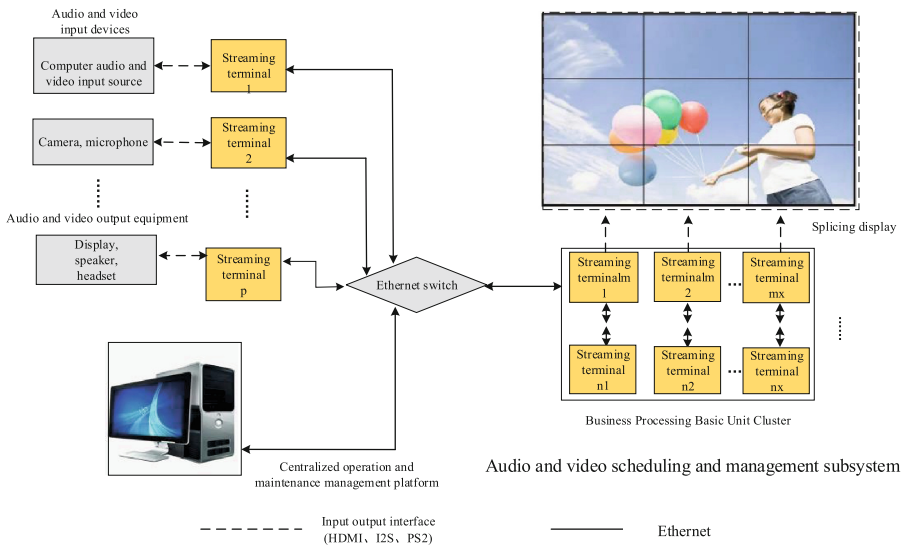


Fig. 1. Diagram indicating the application of streaming terminals.

## 3 Detailed Design and Implementation

### 3.1 Detailed Design

This paper proposes an embedded streaming terminal, which integrates audio and video capture, encoding and decoding, transmission, and image processing. The hardware module is shown in Fig. 2, with built-in modules such as encoding and decoding, power

supply, status display, and debugging. The encoding and decoding module uses a domestic HiSilicon chip Hi35XX, which supports HDMI input and output. The module uses a conversion chip to convert HDMI to BT1120 for inputting into the HiSilicon chip and also supports converting the BT1120 signal to HDMI output. It provides a 10M/100M/1000M adaptive Ethernet interface and audio and video input and output interfaces. It supports a maximum resolution of no less than 3840X2160, a maximum frame rate of no less than 60fps, and supports H264/H265/AAC/G711 encoding. It also supports remote network configuration.

The software is implemented by using the media processing software platform provided by HiSilicon, which supports rapid development of application software and implementation of video encoding and decoding, video input and output display, video image preprocessing, encoding stream OSD overlay, video frame rate analysis, audio capture and output, audio encoding and decoding functions.



Fig. 2. Terminal appearance diagram.

### 3.2 Specific Implementation

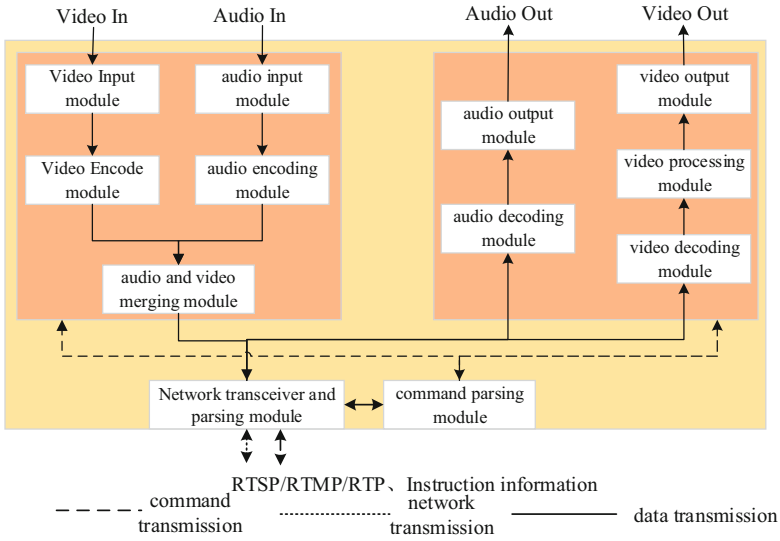
The audio and video service processing terminal adopts modular processing, and the internal firmware module structure diagram is shown in Fig. 3. It is divided into video input module VI (Video Input), video encoding module VENC (Video Encode), audio input module AI (Audio Input), audio encoding module AENC (Audio Encode), audio and video merging module AVM (Audio video merging), audio decoding module ADEC (Audio Decode), audio output module AO (Audio Output), video decoding module VDEC (Video Decode), video processing module VPSS (Video Process), video output module VO (Video Output), command parsing module NCP (Net cmd Parse) and network transceiver and parsing module NTA (Network transceiver analysis).

The detailed module functionalities are shown in Table 1.

In Fig. 1, the visual application interface runs on the centralized operations and maintenance management platform, including login and permission management, audio-video capture and encoding management, decoding and display management, layout scenario management, and operations and maintenance management. The software enables online configuration of the functionality of each basic unit through network commands.

Network commands are divided into audio-video encoding commands, audio-video decoding commands, etc.

- a. Each command includes a message header, checksum, padding data, flag bits, and message footer. The padding data and flag bits are temporarily filled with 0x0/0xff, and these bytes can be used to expand the command content.



**Fig. 3.** Internal firmware module diagram of the audio and video service processing terminal.

- b. The audio-video decoding command includes chip selection, command word, mode, output resolution frame rate, switch, decoding format, decoding channels (supporting a total of 9 channels), and decoding information for each channel including display priority, decoding source address, port address, resolution frame rate, display top-left coordinates, display width and height, sampling rate, sampling depth, audio mode, etc.
- c. The audio-video encoding command includes chip selection, command word, mode, audio-video working type, audio-video encoding format, output network protocol, main and secondary stream bit rate, etc.

### 3.3 Key Technology Solutions

In this paper, the streaming media terminal is used to realize the audio and video system based on the embedded business processing basic terminal, which has complete functions and excellent performance. The key technologies are as follows:

- a. Standardize the design of video encoding and decoding, video transmission, and video fusion processing capabilities to form quantifiable and universal processing terminals. Build the system through quantity stacking and Ethernet switching cascading, with excellent performance and strong scalability
- b. Implement management configuration through network control interfaces to enhance the flexibility of the audio and video business system.
- c. Breaking through the design of the HiSilicon chip SDK, it can achieve multi-channel video stacking, splicing, and scaling.

**Table 1.** Module functionality table.

NO	Module	function
1	Network transceiver and parsing module	The network transmitting and parsing module is responsible for receiving, sending, and parsing various types of information such as audio and video streams, network commands, and heartbeats
2	Command parsing module	Complete audio and video encoding and decoding instruction parsing, obtain configuration parameters, picture overlay, translation parameters, and pass parameter information to the corresponding module
3	Video input module	Complete video signal capture and input conversion
4	Audio input module,	Completing the collection and input conversion of audio signals
5	Video encoding module	Encode videos according to the command parameter requirements
6	Audio encoding module	Encode audio files according to the command parameter requirements
7	Audio-Video merging module	Merge audio and video encoded data to achieve audio and video synchronization
8	Audio decoding module	Decode audio based on command parameter requirements
9	Audio output module	Complete audio output
10	Video decoding module	Complete video decoding according to command parameter requirements
11	Video processing module	Complete functions such as multi-screen splicing, scaling, and translation according to command parameter requirements
12	Video output module	Complete video output

## 4 Functional Performance Testing

### 4.1 Testing Environment

The testing environment for streaming terminals is shown in Fig. 4, consisting of several service processing terminals, a centralized operation and maintenance management platform (PC), audio-video output devices, network cameras, speakers, splicing screens and ethernet switches.

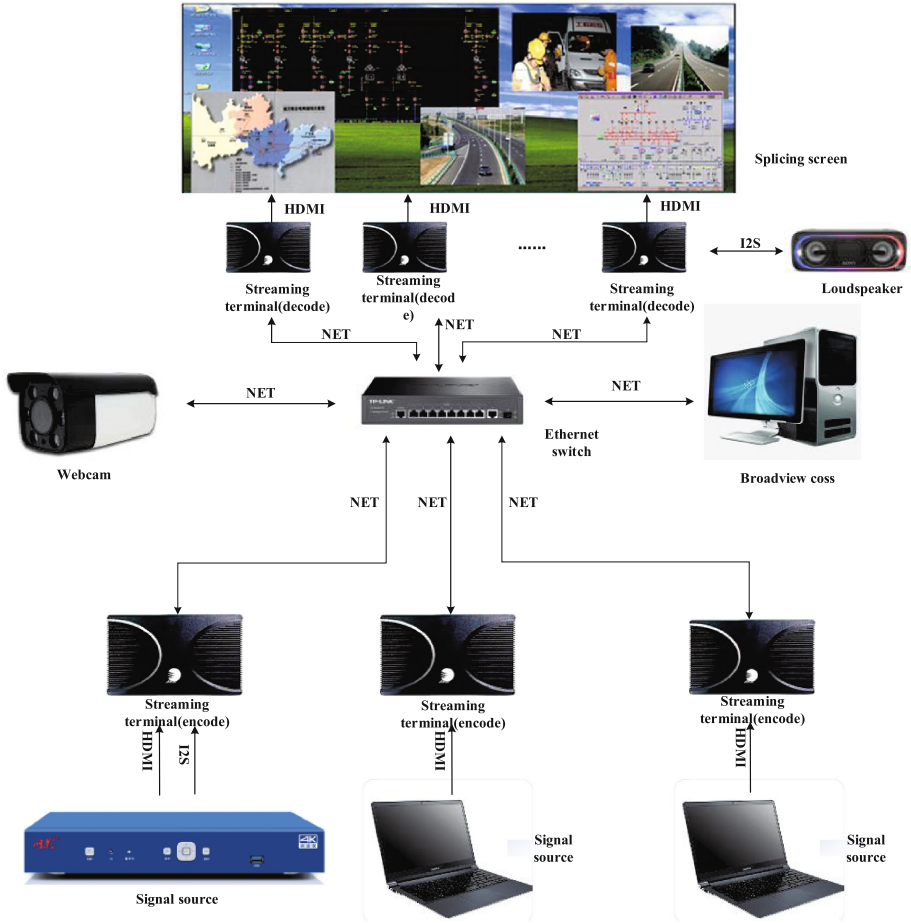


Fig. 4. Testing environment for streaming terminals.

## 4.2 Function Testing

Function testing includes video switching, video splicing, video overlay, PIP (Picture-in-Picture), PBP (Picture-by-Picture), seamless zoom, etc., with videos of different resolutions and frame rates. It also includes testing the RTSP network protocol. The test results are shown in the following Table 2.

## 4.3 Performance Testing

Performance testing includes tests for encoding and decoding channels, encoding and decoding latency, and output bit rate. The test results are shown in the Table 3.



**Table 2.** Multi-function testing.

NO	Testing items	Testing methods	Test results
1	Encoding function	Encode terminal accessing audio and video sources, control encoding parameters and bitrate information through centralized operation and maintenance management software, use commercial tool VLC to pull the stream, and view the streaming screen and parameters	The RTSP stream is successfully pulled and displayed in VLC. The encoding parameters are consistent with the settings
2	Decoding function	Control a decoding terminal to pull a specific RTSP stream through centralized operation and maintenance management software, and view the corresponding display screen and speaker sound output through the HDMI output of the decoding device	VLC successfully displays the video, and the sound is playing correctly
3	Decoded screen splicing	Control multiple decoding terminals to pull a specific RTSP stream through centralized operation and maintenance management software, and display the images according to the decoding splicing instruction requirements, and view the display of multiple spliced screens	Multiple displays with mosaic screen configuration are functioning properly and showing a consistent output
4	Decoded screen overlay	Control decoding terminals to pull multiple RTSP streams through centralized operation and maintenance management software, and control the position of each decoding image to overlay the images, and view the status of the overlay display	Multiple decoded images overlay display normally

*(continued)*

**Table 2.** (continued)

NO	Testing items	Testing methods	Test results
5	Decoded screen translation	Control the decoding terminal to pull a specific RTSP stream through centralized operation and maintenance management software, and control the display position. Send multiple instructions for different positions, and view the screen's display translation status	The image panning is normal
6	Decoded screen scaling	Control the decoding terminal to pull a specific RTSP stream through centralized operation and maintenance management software, and control the display position. Send multiple instructions for different decoding output sizes to observe the output status of the screen	The image scaling is normal

**Fig. 5.** Test process screen.

**Table 3.** Multiple performance testing.

NO	Test performance metrics	Testing methods	Test results
1	Encoding output bit rate testing	Control the output bit rate (VBR) of the decoding terminal through network commands, and observe the decoding effect. At the same time, test the bit rate of the terminal's output bitstream using Wireshark software tool	The output bitrate is consistent with the settings. The bitrate for 1080P ranges from 1Mb/s to 10Mb/s
2	Encoding/decoding concurrency testing	By using network commands, adjust the Variable Bit Rate (VBR) of the decoding terminal's output. Monitor and evaluate the decoding effect. Concurrently, employ Wireshark software tool to measure the bit rate of the output bitstream from the terminal	When the coding resolution and frame rate are set at 1080p@60fps, it can achieve 9-channel decoding
3	Latency testing	Run a stopwatch software on the video source connected to the encoding terminal, with accuracy up to milliseconds. Control the decoding terminal to stream and decode the content using network commands. Capture the frames of both the encoding and decoding terminals simultaneously using a high-speed camera. Calculate the time difference between the two sides to determine the encoding and decoding latency	<ul style="list-style-type: none"> <li>a. The screen delay is 245 ms for 4 k@30fps</li> <li>b. The screen delay is 80 ms for 1080p@60fps</li> </ul>

## 5 Conclusion

This design implements an embedded audio and video processing terminal on a self-developed embedded Hisilicon module. Compared to existing technologies, it provides an embedded audio and video processing basic terminal that standardizes the capabilities of audio and video codec, transmission, and video fusion processing, forming a quantifiable and universal processing terminal. The functional performance test results

are good, achieving functions such as video switching, video splicing, video overlay, PIP, PBP, and seamless zoom with good latency performance and controllable bitrate, realizing multi-channel overlay. This processing terminal fully taps into the scalable, expandable, quantifiable, and customizable capabilities of audio and video systems.

## References

1. Ping, H.: System Research Based on Streaming Media Video Conferencing Mobile Terminal. Beijing Jiaotong University, Beijing (2014)
2. Wei-lun, C., Heng-Fei, T.: Research and implementation of mobile embedded streaming media terminal based on FFMPEG. *Agricult. Equip. Veh. Engin.* **59**(8), 120–122 (2021)
3. Heng, S.: Design and implementation of multicxs-terminal mobile streaming media broadcasting system. *Res. Explorat. Labor.* **37**(8), 315–320 (2018)
4. Li-ce, P.: Design and Implementation of Streaming Media Terminal Based on the Improved TFRC. Zhejiang University of Technology, Zhejiang (2015)
5. Yao, M.: Research and Application of Audio and Video Synchronization Technology in In-Flight Entertainment System. University of Electronic Science and Technology, Chengdu (2022)



# Digital Copyright Transaction Scheme Based on Blockchain Technology

Yuan Gao<sup>1</sup>, Jin Wen<sup>2</sup>, Peidong Miao<sup>1</sup>, and Zhiqiang Wang<sup>2</sup>(✉)

<sup>1</sup> Department of Electronics and Communications Engineering, Beijing Electronic Science and Technology Institute, Beijing 10070, China

<sup>2</sup> Department of Cyberspace Security, Beijing Electronic Science and Technology Institute, Beijing 10070, China  
wangzq@besti.edu.cn

**Abstract.** In the current digital and networked era, the demand for digital copyright transactions is growing, and the traditional centralized registration method has problems such as high costs and long time limits for copyright registration, and difficulties in copyright protection. The technical features of blockchain technology, such as decentralization, immutability of information, openness and anonymity, offer new opportunities for digital copyright protection. We design a digital copyright transaction scheme based on blockchain technology. Firstly, we use Java to build an underlying platform that simulates the operation of the blockchain data layer, consensus layer and contract layer, on top of which we design a distributed underlying blockchain platform that can securely generate blocks, generate transactions, validate transactions, add transactions into blocks, broadcast blocks, validate blocks and add blocks into the blockchain, and use an interface to manipulate the database for the trading functions to be implemented by the platform, and a visual interface is provided to facilitate users' transactions of digital copyright content. The results show that our platform can effectively address trust, intermediary and execution problems in digital copyright transactions and help reduce copyright infringement.

**Keywords:** Blockchain · Digital copyright · Copyright transactions

## 1 Introduction

With the advancement of global informatization, the development of economic globalization has become more and more profound, accompanied by the vigorous development of the globalization of knowledge [1], and the knowledge economy has gradually become an important area of national development [2]. Individual countries and regions wishing to enhance their competitiveness in the international market must vigorously develop intellectual property rights and enhance the strategic position of intellectual property rights in national economic development [3, 4].

However, due to the convenience of digital content dissemination brought by informatization, the relatively large openness of the network, the limited awareness

of intellectual property rights among citizens, and the regulatory system at the national level to be improved [5], the phenomenon of online infringement is more serious in China, while infringements are also naturally hidden and difficult to trace, and these infringements are flexible and changeable [6, 7], and the dissemination channels are quite extensive [8].

Blockchain is a distributed open ledger with node participation [9, 10], and blockchain technology can produce the smart contract by pre-determining copyright rules for the characteristics of copyright, so as to realize automated and intelligent transactions of digital copyright, giving full play to the advantages of decentralization, non-falsification, non-tampering and smart contracts of blockchain [11, 12].

Therefore, this paper, against this research background, by reviewing relevant literature and drawing on relevant research results at home and abroad, proposes to build a distributed digital copyright transaction platform capable of trading the digital copyright content stored in the database from the data layer of the blockchain. The main contributions of the platform are as follows:

1. The platform makes full use of the decentralized features of blockchain technology to effectively solve the trust problem in digital copyright protection, and the transaction parties do not go through a centralized institution, and any user is directly involved in the transaction, which is conducive to an in-depth understanding between the transaction parties.
2. The use of distributed nodes to jointly store the unspent transaction output list of transactions solves the intermediary problem in digital copyright protection, and each transaction can be verified by network-wide transaction return, jointly realizing that each transaction is traceable and each transaction is safe and reliable.
3. The smart contract is used to solve the execution problem in digital copyright protection, when both parties meet the set conditions, the transaction will automatically trigger, and at the same time, both parties will be forced to execute, solving the execution problem in the transaction.
4. Providing a simple visual interface, users can log in to the client for digital copyright trading operations.

## 2 Related Works

The rapid development of digital technology has created a vast amount of digital copyright content. As digital technology enters millions of homes, our lives are becoming more and more connected to digital copyright. The short videos you watch every day on your mobile phone, the music you like to listen to, the electronic academic articles you read, the information technology products you use, the office software you operate at work, etc., all these digital products make full use of digital copyright behind the scenes. However, due to the inherent problem of easy copying and borrowing of digital works [13], incidents of disrespecting digital copyright and infringing on the intellectual achievements of others now occur repeatedly on the Internet, causing damage to the legitimate rights and interests of the originators and seriously dampening motivation, which can have a huge impact on the digital industry [14–16]. Therefore, how to trade digital copyrights in a safe, efficient and low-cost manner and protect the legitimate rights

and interests of copyright owners has become a topic of research for many scholars and experts at home and abroad [17–19].

Wu et al. [20] proposed a research and design scheme for DCI-based copyright protection of digital works, establishing a complete DCI system, issuing DCI codes to digital copyright owners through code issuance centers, and using the four characteristics of DCI codes themselves, namely uniqueness, permanence, compatibility, and scalability, to perform DCI code embedding and fetching operations on digital copyright information such as digital software, audiovisual video, and digital text, realizing the identification of digital copyright.

Xiao et al. [21] proposed a digital copyright protection system based on feature images. A new digital rights management (DRM) technology system was established using the traversal encryption method, which utilizes the triple encryption mechanism technique, thus enabling the encryption of the content of the digital copyright, the encryption key of the digital copyright, and the coordinates of the image pixel points of the digital copyright [22].

And Li [23] proposed an advanced practical byzantine fault tolerance algorithm (APBFT) and designed a digital copyright registration data interaction and storage model based on blockchain technology, which changed the problem of low throughput and resource waste in the traditional digital copyright transaction process, and implemented a digital copyright registration system based on blockchain technology according to the proposed improved algorithm and model, thus protecting the security of digital copyright.

In 2023, Ciriello et al. [24] proposed design principles for blockchain-based centralized DRM systems, using the music industry as an example, the design principles provide an integrated and flexible solution by enabling transparent music licensing structures, consistent and complete copyright metadata, and efficient and transparent royalty payments.

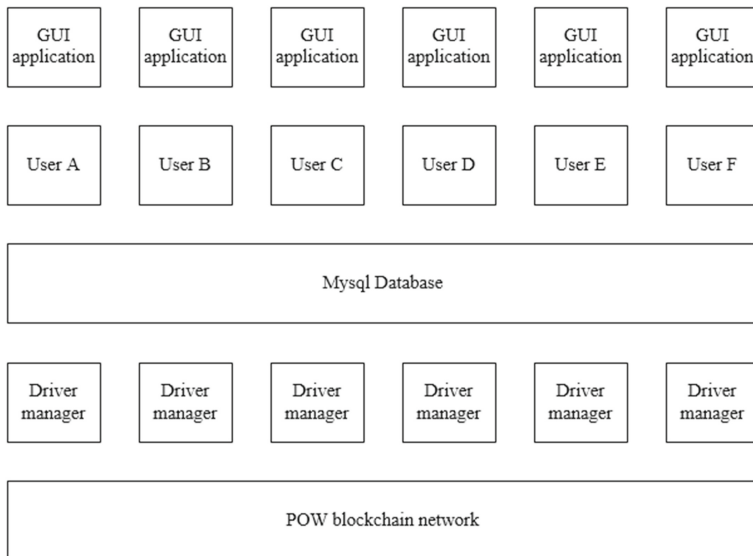
In general, from the overall picture of the research on digital copyright transaction schemes at home and abroad, the traditional centralized registration method suffers from high costs and long time limits for copyright registration, and difficulties in copyright protection. The use of blockchain technology to encrypt the transaction process of digital copyrights can make full use of the decentralization, time-series data, multi-node maintenance, smart contracts, key encryption and other features of the current blockchain technology [25, 26], which is undoubtedly a very secure, efficient and operable digital copyright transaction scheme, so this paper conducts a study on the digital copyright transaction scheme based on blockchain technology.

### **3 Blockchain-Based Digital Copyright Transaction Platform Design**

The transaction platform uses the blockchain underlying technology, which can store all the user's transaction information in the blockchain and realize tamper-proof and traceable transactions. As the transaction information is stored in a non-centralized consortium blockchain, any user of the system can use the system to query the current account information and past transaction records, ensuring the authenticity and validity of the data when querying.

### 3.1 Transaction Platform Network Design

To achieve the functions of the entire transaction platform, the construction of the entire transaction platform network is the foundation, a complete and excellent platform network can maximize the operating efficiency and security of the transaction platform. This platform is a blockchain-based transaction platform. First of all, it needs to run each blockchain node in the underlying blockchain, while providing users with cloud database services. Therefore, it needs to design a dedicated database for each user. In addition, the consensus algorithm we use is proof of work (POW). The overall architecture of the platform is shown in Fig. 1, and the overall flow of the platform is shown in Fig. 2.



**Fig. 1.** General architecture of the transaction platform.

### 3.2 Blockchain Interface Design

In the blockchain, data writing is achieved through transaction writing, and the transaction information can be written into the blockchain while the transaction occurs. During the data interaction process of POW, the data will not be encrypted. Therefore, in this design, transaction information will be encrypted using algorithms such as sha256, base64 and elliptic curve cryptography. In each transaction, the initiator of the transaction is the user who needs to purchase the right to use the copyright, and the recipient of the transaction is the owner of the copyright. In this way, personal information is made public, but without the corresponding decryption algorithm, the specific transaction information is not available and security is ensured.



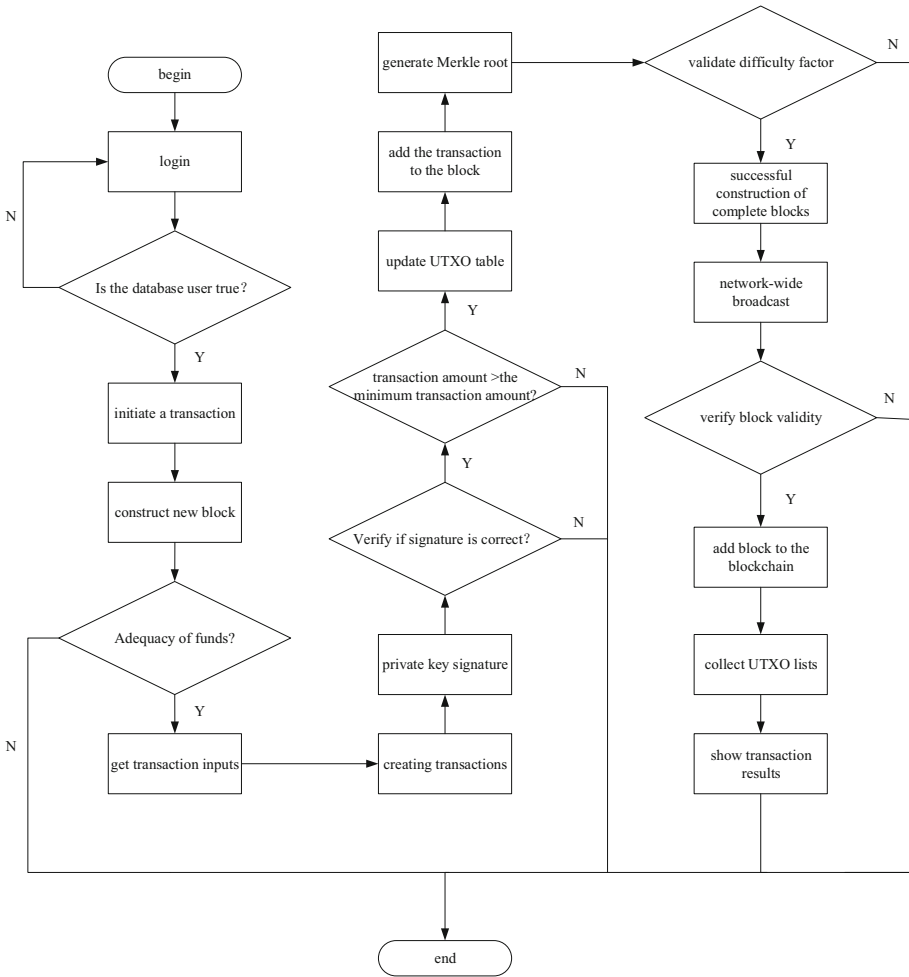
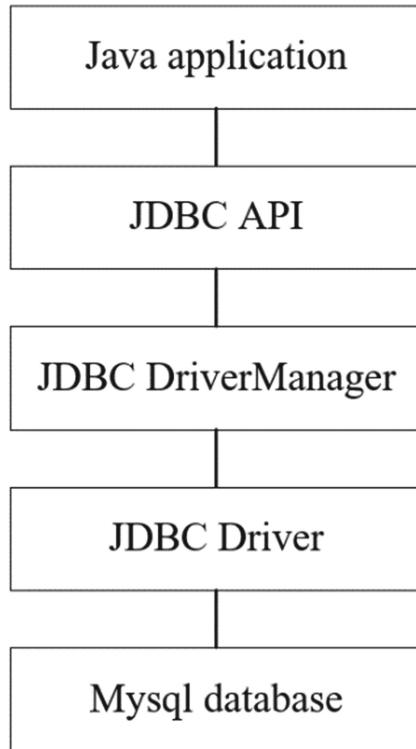


Fig. 2. General flow of the transaction platform.

Java provides a JDBC driver as an interface to connect to MySQL databases, providing 5 classes and interfaces. The Collection interface represents the connection to the Mysql database and is responsible for executing SQL statements through Java and returning the results. The Statement interface is used to send SQL statements to the database after establishing the connection between the two. The PreparedStatement interface is used to pre-compile the SQL statements and save the compilation in the instance. The DriverManager class is used to manage all drivers in the database and to establish connections between individual drivers. The ResultSet interface is a table for temporarily storing the results of database query operations. The design of the blockchain interface architecture is shown in Fig. 3.



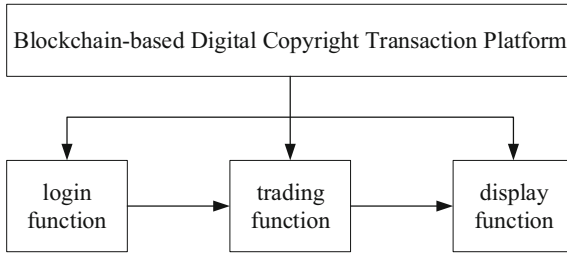
**Fig. 3.** Blockchain interface architecture.

In summary, the functions of the interface of this blockchain mainly focus on collecting database information, establishing connections, executing SQL statements, and returning results.

### **3.3 Transaction Platform Upper Layer Application Design**

This design will provide users with a system that allows direct digital copyright transactions. Not all databases are suitable for storage in the blockchain, for example, digital copyright information can only be called temporarily and is not suitable for storage in the database. The blockchain only stores the user's address, which doesn't contain any other information about the user's identity, thus ensuring the anonymity of the user. I will therefore provide the database to store the user's bid information and digital copyright content, and the interface is responsible for linking the application to the database.

The front-end interface will provide the following functions: login function, transaction function and display function. The architecture is shown in Fig. 4.



**Fig. 4.** Transaction platform upper layer application architecture.

## 4 Implementation and Evaluation of the Scheme

The scheme consists of the following components in the design process: editing the underlying blockchain using Java language, developing Java programs using the MyEclipse development environment, debugging and running, and designing the graphical user interface (GUI) interface using Java language as the user's operation interface; editing the MySQL database using SQL language as a cloud platform for storing copyright arrays; using JDBC driver as the interface to connect Java blockchain and MySQL database.

In addition, we have divided the functional modules of the blockchain into block class, wallet class, transaction class, transaction input class, transaction output class, and method class, with the specific functions of each class shown in Table 1.

Some of the interfaces of the transaction platform are shown in Fig. 5, where Fig. 5 shows the digital copyright transaction interface.

After a series of tests, the whole platform, whether it is the interface or database or the underlying blockchain, can function normally and realize the login, transaction and display functions as expected, and can provide all-round protection for digital copyright transactions between users through the blockchain, preventing theft and malicious use of digital copyright in the process of users' digital copyright transactions.

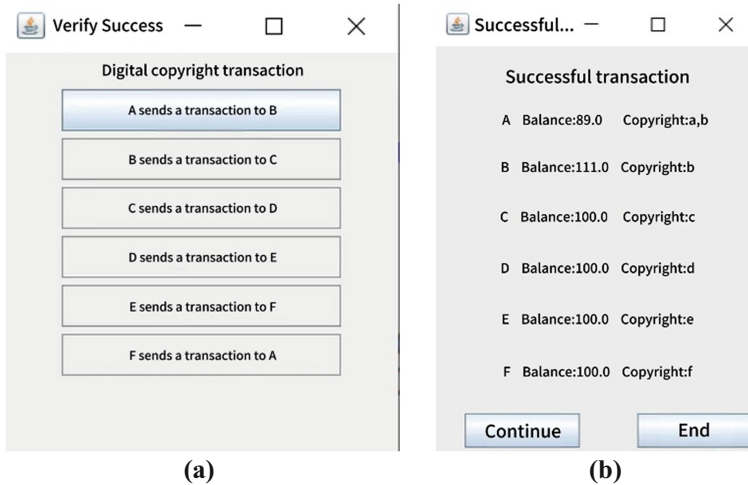
## 5 Conclusions

Currently, most of the digital copyright protection methods are centralized registration type, which is essentially a copyright management mechanism based on centralization authorized by authoritative management agencies, but there are problems such as high costs and long time limits of copyright registration, and difficulties in copyright protection. Therefore, we design a digital copyright transaction scheme based on blockchain technology and implement a blockchain-based digital copyright transaction platform. The platform's visual interface is user-friendly, and the platform can safely generate blocks, generate transactions, verify transactions, add transactions to blocks, broadcast blocks, verify blocks and add blocks to the blockchain. Based on the distributed ledger, decentralization of blockchain and the application of the smart contract, it can effectively solve the trust problem, intermediary problem and execution problem in digital copyright transactions, greatly improve the efficiency of the successful execution of transactions

**Table 1.** Functional modules of the blockchain.

Module name	Function
Block class	Perform some of the functions of the data and consensus layers in the blockchain, and act as the miner node for constructing blocks and giving bookkeeping power to the generated blocks
Wallet class	The wallet class acts as the transaction user node and contains information such as the public and private keys, a list of transactions, and transfer fees. The public key is used to represent the user's address, the private key is used to encrypt the transaction information, and the wallet class also includes the ability for the user to initiate a transaction, thus creating a new transaction
Transaction class	The transaction class contains seven functions: constructing a transaction, calculating the hash represented by this transaction, signing, verifying, processing the transaction, calculating the sum of the inputs and the sum of the outputs
Transaction input class	The transaction input class constructs the transaction input list, and uses the class construction method to obtain a transaction input method with the same name as the transaction input class. The unused transaction output is used as the input information for the next input transaction
Transaction output class	The transaction output class is mainly used to construct transaction output information and verify whether the hash value of the next block is correct
Method class	The method class provides computational tools and auxiliary methods for the individual methods in the previous classes

and increase the motivation of creators. Blockchain's immutable and traceable characteristics provide natural credibility for infringement accountability and protection, becoming effective evidence that can be adopted by law enforcement agencies, simplifying the process of defending rights, reducing the cost of defending rights, and fully protecting the rights and interests of creators.



**Fig. 5.** Digital copyright transaction **a** Transaction selection **b** A sends a transaction to B and the transaction is successful.

**Acknowledgement.** This research was supported by the Fundamental Research Funds for the Central Universities (Grant No. 328202203, 20230045Z0114, 3282023013), China Postdoctoral Science Foundation funded project (Grant No. 2019M650606), First-class Discipline Construction Project of Beijing Electronic Science and Technology Institute (Grant No. 3201012).

## References

1. Halmai, P.: Globalisation versus deglobalisation. *Financ. Econ. Rev.* **22**(2), 5–24 (2023)
2. Parcero, O.J., Ryan, J.C.: Becoming a knowledge economy: the case of Qatar, UAE, and 17 benchmark countries. *J. Knowl. Econ.* **8**, 1146–1173 (2017)
3. Sun, Y., Li, M., Zhang, M., Khan, H.S.U.D., Li, J., Li, Z., et al.: A study on China's economic growth, green energy technology, and carbon emissions based on the Kuznets curve (EKC). *Environ. Sci. Pollut. Res.* **28**, 7200–7211 (2021)
4. Tomizawa, A., Zhao, L., Bassellier, G., Ahlstrom, D.: Economic growth, innovation, institutions, and the great enrichment. *Asia Pacific J. Manag.* **37**, 7–31 (2020)
5. Bican, P.M., Guderian, C.C., Ringbeck, A.: Managing knowledge in open innovation processes: an intellectual property perspective. *J. Knowl. Manag.* **21**(6), 1384–1405 (2017)
6. Liu, J., Wang, X., Wang, Y.: Research on Internet copyright protection mechanism: based on the perspective of the comparison of Chinese and American legislation. In: 2022 7th International Conference on Social Sciences and Economic Development, pp. 1592–1600. Atlantis Press, Paris (2022)
7. Lee, J.A., Li, Y.: The Pathway Towards Digital Superpower: Copyright Reform in China. *GRUR International* **70**(9), 861–870 (2021)
8. Liu, Y., Zhang, J., Wu, S., Pathan, M.S.: Research on digital copyright protection based on the hyperledger fabric blockchain network technology. *PeerJ. Comput. Sci.* **7**, e709 (2021)
9. Lemieux, V.L.: Blockchain and recordkeeping. *Computers* **10**(11), 135 (2021)

10. Ma, Z., Wang, Z., Wu, H., Guo, X., Wang, X.: Research on monitoring technology of industrial cannabis based on blockchain and SM series cryptographic algorithm. *Int. J. Netw. Secur.* **24**(1), 36–48 (2022)
11. Yuan, Y., Wang, F.: Blockchain: the state of the art and future trends. *ACTA Autom. Sin.* **42**(4), 481–494 (2016)
12. Wang, H., Li, X., Xuan, J., Guo, Q., Zhao, L., Yang, K.: Research and system architecture design of dispatching data chain technology for load regulation and control. In: 2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications, pp. 594–598. IEEE, Piscataway (2023)
13. Meurer, M.J.: Price discrimination, personal use and piracy: copyright protection of digital works. *Buff. L. Rev.* **45**, 845 (1997)
14. Lemley, M.A., Reese, R.A.: Reducing digital copyright infringement without restricting innovation. *Stan. L. Rev.* **56**, 1345 (2003)
15. VaridaAriani, N.: Enforcement of law of copyright infringement and forgery with the rise of the digital music industry. *Jurnal Penelitian Hukum De Jure* **21**(2) (2021)
16. Mezei, P., Harkai, I.: End-user flexibilities in digital copyright law—an empirical analysis of end-user license agreements. *Interact. Entertain. Law Rev.* **5**(1), 2–21 (2022)
17. Tuo, X.: Research and design of a blockchain-based encrypted information backup system. Master's thesis, Southwest Petroleum University, Chengdu, China (2017)
18. Gao, J., Yu, H., Zhu, X., Li, X.: Blockchain-based digital rights management scheme via multiauthority ciphertext-policy attribute-based encryption and proxy re-encryption. *IEEE Syst. J.* **15**(4), 5233–5244 (2021)
19. Zheng, X., Zhu, Y.: Blockchain based architecture for digital-right management in scientific data sharing. In: IOP Conference Series: Earth and Environmental Science, p. 012004. IOP Publishing, the United Kingdom (2020)
20. Wu, J., Wang, S.: Research and design of copyright protection of digital products based on DCI. *Comput. Engin. Sci.* **37**(08), 1486–1491 (2015)
21. Xiao, Y., Xiao, M.: Digital rights management system based on characteristic images. *Comput. Eng. Appl.* **50**(11), 105–109 (2014)
22. He, Y., Gong, G.: A summary of research on block chain technology in the security field of IoT. *Telecom Engin. Tech. Standard.* **30**(05), 12–16 (2017)
23. Li, L.: Research and application of block chain technology in digital rights. Master's thesis, North China University of Technology, Beijing, China, 2018
24. Ciriello, R.F., Torbensen, A.C.G., Hansen, M.R.P., Müller-Bloch, C.: Blockchain-based digital rights management systems: design principles for the music industry. *Electron. Mark.* **33**(1), 1–21 (2023)
25. Xu, Y., Ma, X.: Research and implementation of a comprehensive evaluation system for student behaviour based on blockchain. *Inf. Tech. Inf.* **12**, 131–133 (2016)
26. Wang, Z., Wang, Z., Ni, A.: Research on blockchain anomaly transaction detection technology based on stacking ensemble learning. *J. Inf. Secur. Res.* **9**(02), 98–108 (2023)



# Research on Network Security Situation Assessment Method

Yuan Gao<sup>1</sup>, Jin Wen<sup>2</sup>, Pu Chen<sup>1</sup>, and Zhiqiang Wang<sup>2</sup>(✉)

<sup>1</sup> Department of Electronics and Communications Engineering, Beijing Electronic Science and Technology Institute, Beijing 10070, China

<sup>2</sup> Department of Cyberspace Security, Beijing Electronic Science and Technology Institute, Beijing 10070, China  
wangzq@besti.edu.cn

**Abstract.** The Internet has penetrated into various fields of human production and life. While enjoying Internet technology, people have to face various problems brought about by the Internet, among which network security issues are particularly prominent. The network security situation assessment summarizes, filters and analyzes security events generated by devices, builds suitable mathematical models based on security indicators and assesses the level of security threats to the entire network system, thereby analyzing and capturing the overall security status of the network. This paper analyzes the relevant research at home and abroad, and selects Elman neural network model, intuitionistic fuzzy set model and hidden Markov model for network security situation assessment. The result is compared with the expert assessment, and the advantages and disadvantages of the different models are analyzed in conjunction with relevant model theory. It is found that the network security situation assessment model more suitable for the current network environment is the intuitionistic fuzzy set model.

**Keywords:** Network security situation assessment · Elman neural network · Intuitionistic fuzzy set · Hidden Marko

## 1 Introduction

With the rapid development of computer network technology and communication technology, the sharing of resources in computer networks has been further enhanced, and the Internet has penetrated into many aspects of human production and life [1, 2], becoming one of the main tools for social change today, influencing the development of social economy and people's way of life [3]. According to the Internet Information Center, as of December 2022, the number of Internet users in China had reached 1.067 billion, with an Internet penetration rate of 75.6% [4]. The popularity of the Internet has brought convenience to people, but the increase in Internet-connected devices has also led to an increase in the attack surface, raising the risk of attacks on networks [5, 6]. And with the development of Internet technology, the means of attackers are becoming more and more advanced [7, 8], and there are endless ways to attack. In recent years, the number of various network damage incidents is increasing and the degree of damage is gradually

increasing [9], which has caused great economic losses to the individual, the enterprise, and even the country, and the security of the network is facing great challenges [10–13], and both the country and the people attach great importance to the security of the Internet.

Therefore, in this research context, this paper analyzes various cyber attacks by building hidden Markov model, intuitionistic fuzzy set model and Elman neural network model based on the dataset CIC-IDS2017, studies the attack situation in the network, makes the network security situation assessment and compares it with the expert assessment. The specific contributions of this paper are as follows:

1. Based on the model's network security posture assessment values and theoretical knowledge, we study and analyze the advantages or disadvantages of the hidden Markov model, intuitionistic fuzzy set model and Elman neural network model to provide suggestions for reducing the security situation assessment value errors and improving the model.
2. Using the expert assessment as the reference value, the mean error values of hidden Markov model, intuitionistic fuzzy set model and Elman neural network model are compared and analyzed, and the results show that the situation values obtained from the intuitionistic fuzzy set model are closest to the actual situation values and can more accurately assess the current situation of the network.
3. By studying network security situation assessment methods, this paper provides useful references for the future formation of good situational awareness systems, so as to improve the security and stability of the network, better prevent network security incidents, and play a positive role in promoting the progress of network security situational awareness research.

## 2 Related Works

Bass [14] proposed cyberspace situational awareness in 2000, the first appearance of situational awareness in the field of cyberspace. Blyth [15] pointed out that the hackers' attack paths could be traced to further qualitatively assess the security threats to the network, but their research was limited to theory and was not applied in practice. In addition to this, a large number of other scholars conducted related research, such as DeMontigny-Leboeuvf [16] and Yurcik [17]. Later, based on research on traffic networks, the CERT/NetSa team used the traffic monitoring tool NetFlow [18] to monitor large networks in real-time, achieving early warning of network attacks and avoiding network paralysis caused by network attacks. In 2020, Liao et al. [19] designed a network security situation assessment system based on an extended hidden Markov model, which extends the model tuple and adds two parameters, network defense efficiency and risk loss vector, so that the model can describe the network security situation more completely.

Compared with the current situation of foreign research on network security, China's research on network security situation assessment is relatively late and is still in the development stage. Chen et al. [20] divided the network into layers, from the system layer related to software, to the host layer and service layer related to servers and hosts, to the attack layer and vulnerability layer related to cyber attacks, and used a rich variety of



methods, such as top-down and part first and then whole, etc. This situational assessment method is very conducive to practical applications. However, it is too practically oriented, resulting in too much reliance on subjective opinions in the allocation of weights, and therefore the assessment results may be biased. Subsequently, Gu et al. [21], after researching and analyzing the theories, combined game theory and other theories with them and eventually improved the hierarchical analysis method, especially its problem of assigning weights to different indicators. Finally, when calculating the value of the network security situation, a fuzzy comprehensive evaluation method was also proposed to be used for the calculation, which resulted in a more accurate assessment value. 2021, Shi et al. [22] optimize the parameters of neural networks and classify the attacks on industrial control systems and thus quantify the situation results. The security situation assessment method applying neural networks reduces the reliance on expert opinions in traditional assessment methods, focuses on the representation of raw data information, and the results are more consistent with the real network situation.

In this paper, based on the review and study of relevant research results at home and abroad, three different network security situation assessment methods are selected, which are hidden Markov model, intuitionistic fuzzy set model and Elman neural network model. In the dataset CIC-IDS2017, which is more in line with the current network environment, the network security situation is analyzed through the simulation experiments of the three models. By comparing expert assessment differences and delving into relevant model theories to analyze the advantages and disadvantages of each model, the model that finally gets suitable for the current network environment is the intuitionistic fuzzy set model.

### 3 Network Security Situation Assessment Models

This paper selects three different models: hidden Markov model, intuitionistic fuzzy set model and Elman neural network model to assess the network security situation. The models were selected because they are three basic models that can extend or supplement network security situation assessment, enabling them to conduct network security situation assessment in more complex and ever-changing network environments.

#### 3.1 Hidden Marko Model

##### 3.1.1 Introduction of Hidden Markov Model

The hidden Markov model is the process of extending the Markov model to express the hidden Markov chain with implicit unknown parameters, which is explained as follows: the state  $x_t$  in the system is hidden and cannot be viewed by the observer, but the system will simultaneously generate the observation symbol  $y_t$  with a certain functional relationship with  $x_t$ , so the observer views and dissects the observation sequence  $Y = \{y_1, y_2, \dots, y_t\}$ , thus obtaining the implied state sequence  $X = \{x_1, x_2, \dots, x_t\}$ , whose specific state transfer process is shown in Fig. 1.

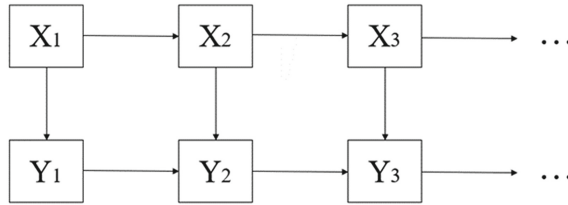


Fig. 1. Hidden Markov state transition

**3.1.2 Model Representation**

The hidden Markov model is expressed using the five-tuple  $\{S, O, \pi, A, B\}$ , each of these factors is described in detail below:

1. Implied state space  $S$ .

$S = \{S_1, S_2, \dots, S_n\}$ , where  $n$  is the size of the state space. The different factors in  $S$  represent different hidden states in the system, and all different hidden states must comply with Markov properties.

2. Observable state space  $O$ .

$O = \{O_1, O_2, \dots, O_m\}$ , where  $m$  is the size of the observation space. Different factors in  $O$  can serve as observation symbols that can be directly observed by observers.

3. Initial state probability matrix  $\pi$ .

$\pi = \{\pi_1, \pi_2, \dots, \pi_n\}$ , where  $\pi$  is the probability of different states in different moments.

4. Implied state transition probability matrix  $A$ .

$A = [a_{ij}]_{N \times N}$ , where  $a_{ij} = p(x_{t+1} = S_j | x_t = S_i)$ ,  $1 \leq i, j \leq N$ ,  $A$  is the probability of change of the model from state  $i$  to state  $j$  at moment  $t + 1$ .

5. Observed state transition probability matrix  $B$ .

$B = [b_{jk}]_{M \times N}$ , where  $b_{jk} = p(y_t = o_k | x_t = S_j)$ ,  $1 \leq j \leq N$ ,  $1 \leq k \leq M$ , where the probability that the observer observes the observed symbol when the system is in state  $S_j$  is  $o_k$ .

In the general case, instead of using the implied state space  $S$  and the observable state space  $O$ , the Hidden Markov Model is expressed as a three-tuple with  $\lambda = (A, B, \pi)$ .

**3.2 Intuitionistic Fuzzy Set Model**

**3.2.1 Introduction of Intuitionistic Fuzzy Set Model**

**Definition 1** Let  $X$  be a defined domain of discourse, then the intuitionistic fuzzy set  $A$  in the domain  $X$  is  $A = \{ \langle x, \mu_A(x), \gamma_A(x) \rangle | x \in X \}$  And  $\mu_A(x) : X \rightarrow [0, 1]$  and  $\gamma_A(x) : X \rightarrow [0, 1]$  are membership function  $\mu_A(x)$  and non-membership function  $\gamma_A(x)$  on  $X$ , and  $0 \leq \mu_A(x) + \gamma_A(x) \leq 1$  holds for all  $x \in X$  on  $A$ .

When  $X$  is a continuous space,  $A = \int_A \frac{\langle \mu_A(x), \gamma_A(x) \rangle}{x}$ ,  $x \in X$ ; when  $X = \{x_1, x_2, \dots, x_n\}$  is a discrete space,  $A = \sum_{i=1}^n \frac{\langle \mu_A(x_i), \gamma_A(x_i) \rangle}{x_i}$ ,  $x_i \in X$ ,  $i = 1, 2, \dots, n$ . Intuitionistic fuzzy set  $A$  can be abbreviated as  $A = \langle x, \mu_A, \gamma_A \rangle$  or  $A = \frac{\langle \mu_A, \gamma_A \rangle}{x}$ .

In intuitionistic fuzzy set  $A$ , it is called  $\pi_A(x) = 1 - \mu_A(x) - \gamma_A(x)$  is the intuitive index of  $x$  in  $A$ , which represents the degree of hesitation of  $x$  towards  $A$ .

**Definition 2** Let  $A = \{\langle x, \mu_A(x), \gamma_A(x) \rangle | x \in X\}$  And  $B = \{\langle x, \mu_B(x), \gamma_B(x) \rangle | x \in X\}$  be intuitionistic fuzzy subsets on a given domain of discourse  $X$ . Then the operations between intuitionistic fuzzy sets is:

$$A \subseteq B \Leftrightarrow \forall x \in X, [\mu_A(x) \leq \mu_B(x) \wedge \gamma_A(x) \geq \gamma_B(x)] \quad (1)$$

$$A \subset B \Leftrightarrow \forall x \in X, [\mu_A(x) < \mu_B(x) \wedge \gamma_A(x) > \gamma_B(x)] \quad (2)$$

$$A = B \Leftrightarrow \forall x \in X, [\mu_A(x) = \mu_B(x) \wedge \gamma_A(x) = \gamma_B(x)] \quad (3)$$

$$A^c = \{\langle x, \mu_A(x), \gamma_A(x) \rangle | x \in X\} \quad (4)$$

$$A \cap B = \{\langle x, \mu_A(x) \wedge \mu_B(x), \gamma_A(x) \vee \gamma_B(x) \rangle | \forall x \in X\} \quad (5)$$

$$A \cup B = \{\langle x, \mu_A(x) \vee \mu_B(x), \gamma_A(x) \wedge \gamma_B(x) \rangle | \forall x \in X\} \quad (6)$$

$$A + B = \{\langle x, \mu_A(x) + \mu_B(x) - \mu_A(x) \cdot \mu_B(x), \gamma_A(x) \gamma_B(x) \rangle | \forall x \in X\} \quad (7)$$

$$A \cdot B = \{\langle x, \mu_A(x) \cdot \mu_B(x), \gamma_A(x) + \gamma_B(x) - \gamma_A(x) \cdot \gamma_B(x) \rangle | \forall x \in X\} \quad (8)$$

where:  $A \cdot B$  is the inner product;  $\vee$  is used to get maximum value;  $\wedge$  is used to get minimum value.

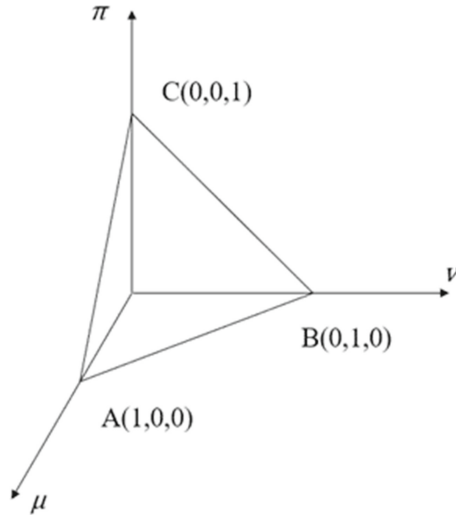
### 3.2.2 Geometric Representation

Each intuitionistic fuzzy subset is composed of the three-tuple  $\langle x, \mu_i(x), \gamma_i(x) \rangle$ , and  $\pi_i(x) = 1 - \mu_i(x) - \gamma_i(x)$ , so a geometric representation method with  $x, \mu_i(x), \gamma_i(x)$  as coordinates can be used. As in Fig. 2, each coordinate point in  $\triangle ABC$  corresponds to an intuitionistic fuzzy subset.

## 3.3 Elman Neural Network Model

### 3.3.1 Introduction of Elman Neural Network Model

The Elman neural network has been around for nearly 30 years now, and its inventor is Elman [23]. It is a modified feedforward neural network, and its main improvement is that the feedforward network is transmitted without delay, whereas in the feedback network there is delay, and the output signal of a neuron in the same level will be transmitted back to the previous level after a delay and become the input signal of the neuron in the previous level, which allows interconnecting neurons in different levels. The Elman



**Fig. 2.** Geometric representation of intuitionistic fuzzy sets.

neural network is a classical feedback-type neural network, which contains input layer delay, neuron self-feedback, output layer delay and two layers of mutual feedback. The neural network adds a layer to the hidden layer, through which the information output at the previous moment in the hidden layer can be stored and remembered, and then fed back to the hidden layer as input information for the nodes in the hidden layer, thus creating an artificial step delay, which completes the computational delay within the network and creates a memory-like capability.

### 3.3.2 Structure of Elman Neural Network

The structure of the Elman neural network model is shown in Fig. 3, which is consisted of four parts: the input layer, the intermediate hidden layer, the output layer and the undertake layer. The three components except the undertake layer are very similar to the feedforward neural network. For example, the input layer is only responsible for inputting information, and does not process any information; the main function of the intermediate hidden layer is to process information. Its neurons usually choose to use nonlinear functions when transmitting information. After processing, the expected data can be obtained, and then the expected data is transmitted to the next layer, namely the output layer and the receiving layer. The receiving layer transfers the stored information at the current time  $t$  to the hidden layer at time  $t + 1$ .

The formulas used in the weight correction algorithm of Elman neural network is introduced as follows:

the output layer:  $y(k) = h(w^3x(k))$ .

the hidden layer:  $x(k) = g(w^2x_c(k) + w^1u(k - 1))$ .

the undertake layer:  $x_c(k) = x(k - 1)$ .

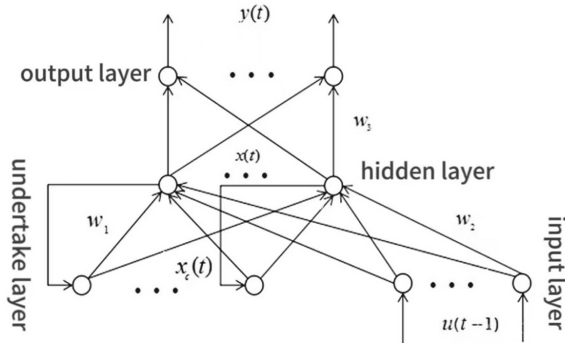


Fig. 3. Elman neural network model.

## 4 Experiments and Evaluation

### 4.1 Experimental Dataset

We use the CIC-IDS2017 dataset produced in 2017, which has the characteristics of long data duration, a large amount of data, multiple data types and diverse storage forms. The dataset, produced by the Canadian institute for cybersecurity research, has a data volume of up to 55GB, which was updated based on CIC-IDS2012 in 2012. Unlike older datasets that are mostly obtained in simulated environments, CIC-IDS2017 contains a large amount of data from actual environments, including the state of the network in various periods. In addition, CIC-IDS2017 covers the most common attacks in daily networks, including: penetration, cracking, denial of service, distributed denial of service, web-based attacks, security vulnerabilities, zombies, port scanning, and the data is newer, facilitating researchers to conduct research and analysis closer to reality and the current situation.

The CIC-IDS2017 dataset records all network data for a five-working day period. The detailed composition of the victim network systems and the attack network systems is shown in Table 1.

### 4.2 Selection of Indicators

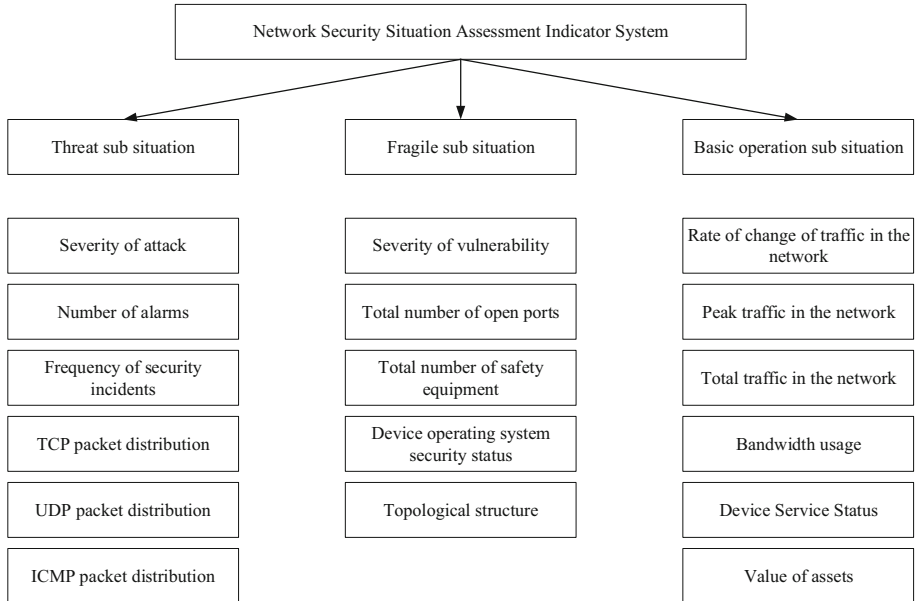
This paper refers to the network information security risk assessment specification GB/T 20984–2007 and combines the network security situation assessment system already established by previous authors, and the network security situation assessment indicator system built is shown in Fig. 4.

### 4.3 Experimental Results

Due to the large statistical data of 180 samples, which cannot be fully displayed in the graph, the data are averaged to produce 30 sets of data. The following are the results obtained from each of the three models (Figs. 5, 6 and 7).

**Table 1.** Network equipment composition.

Host category	Host system	IP
Secure host	Fire	205.174.165.80
	DNS + DC Server	192.168.10.3
Attack host	Kali	205.174.165.73
	Win	205.174.165.69 、 205.174.165.70 、 205.174.165.71
Victim host	Web server 16 Public	192.168.10.50 、 205.174.165.68
	Ubuntu server 12 Public	192.168.10.51 、 205.174.165.66
	Ubuntu 14.4, 32B	192.168.10.19
	Ubuntu 14.4,64B	192.168.10.17
	Ubuntu 16.4,32B	192.168.10.16
	Win 7Pro64B	192.168.10.9
	Win 8.1,64B	192.168.10.5
	Win Vista,64B	192.168.10.8
	Win 10, pro 32B	192.168.10.14
	Win 10,64B	192.168.10.15
	Mac	192.168.10.25



**Fig. 4.** Network security situation assessment indicator system.

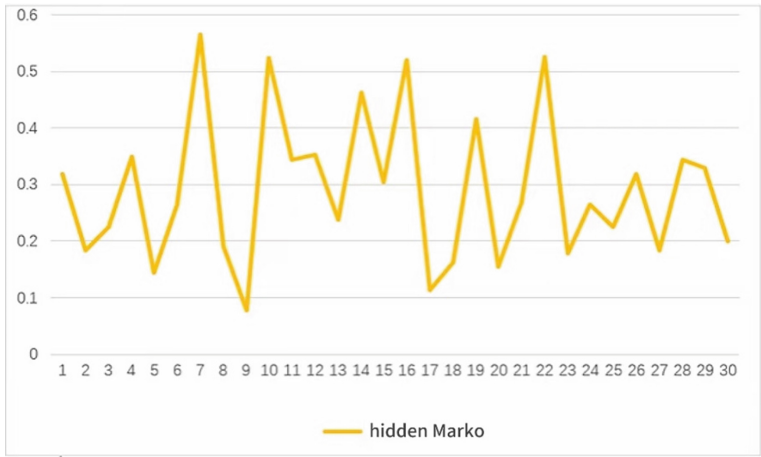


Fig. 5. Change of network security situation assessment value of hidden Markov model.

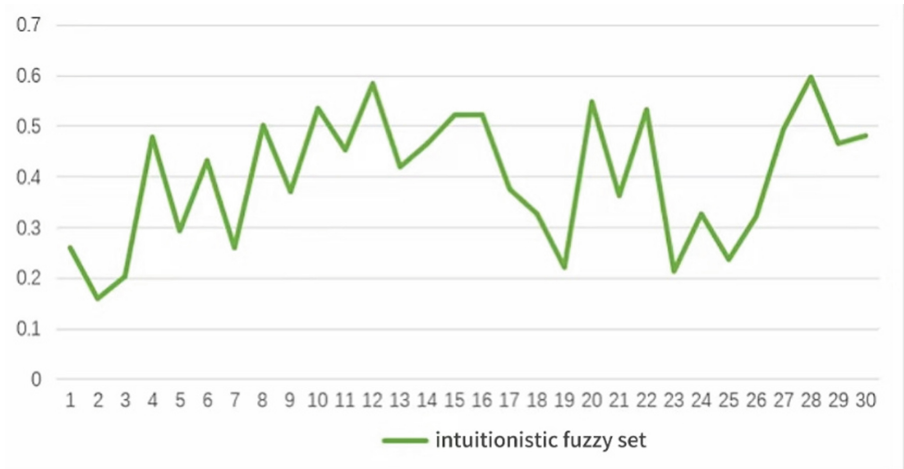


Fig. 6. Change of network security situation assessment value of the intuitionistic fuzzy set model.

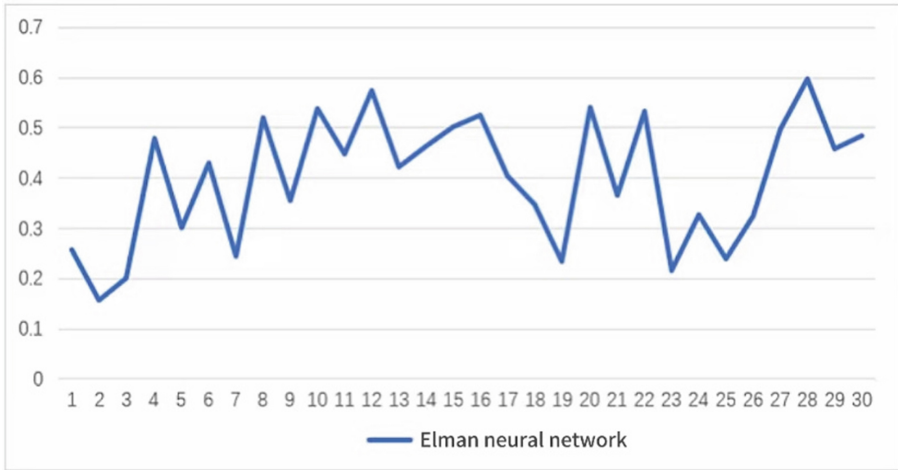
#### 4.4 Comparison and Analysis of Experimental Results

The network security situation assessment of hidden Markov model, intuitionistic fuzzy set model, Elman neural network model and expert assessment are compared, and the results are shown in Fig. 8.

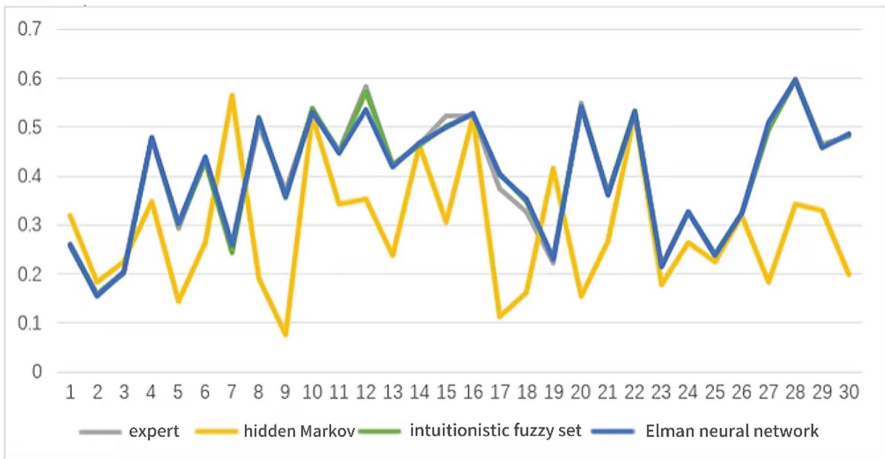
The errors of the hidden Markov model, intuitionistic fuzzy set model and Elman neural network model compared to the expert assessment values, using the expert assessment as the reference, are shown in Fig. 9.

A comparison of the means and variances of the network security situation assessment errors for different models is shown in Table 2.

By analyzing Figs. 8, 9 and Table 2, the results can be summarized as follows:



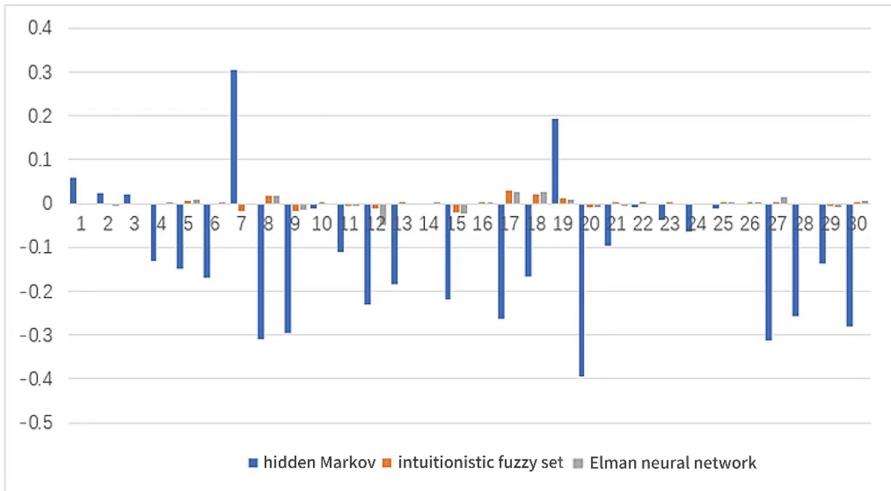
**Fig. 7.** Change of network security situation assessment value of Elman neural network.



**Fig. 8.** Comparison of network security situation assessment values for different algorithms.

1. The hidden Markov model has a large error range and sometimes deviates substantially, probably because the state of the hidden Markov model is only related to its previous state and a higher-order hidden Markov model must be built to utilize more known information, while multiple matrices were not built in the study, hence the deviation.
2. The comparison between the network security situation assessment values of the Elman neural network model and the expert assessment values shows that the error of the Elman neural network model is relatively small, and can better reflect the network security situation of the current network environment. Further improvements may require greater training or algorithmic changes.





**Fig. 9.** Comparison of errors in different models for network security situation assessment.

**Table 2.** Comparison of the means and variances of network security situation assessment errors for different models.

Experimental data	Number	Mean value of error	Error variance
Hidden Marko	30	3.235	0.153
Intuitionistic fuzzy set	30	0.010	0.010
Elman neural network	30	0.016	0.013

3. The average error and variance of the intuitionistic fuzzy set model are both 0.01, which is the smallest of the three models. It provides a more accurate and comprehensive picture of the network security situation in the chosen models.
4. In the case of using the same data set, the average error of the intuitionistic fuzzy set model is 3.225 less than that of the hidden Markov model, and 0.006 less than that of the Elman neural network model, which can more comprehensively and accurately reflect the current network security situation.

## 5 Conclusions

The Internet has brought a lot of convenience to people, but as people become more and more connected to the Internet, many network security issues have emerged, such as data leakage and network paralysis, and the security of the Internet needs to be given more attention. In this paper, hidden Markov model, intuitionistic fuzzy set model and Elman neural network model are selected for Matlab experimental simulation to complete the network security situation assessment. Based on the study of the model theory, the results are compared with expert assessment so as to analyze the advantages and disadvantages

of the models, and to arrive at an algorithmic model that is more in line with the current network environment as the intuitionistic fuzzy set model, providing a useful reference for the security and stability of the network.

**Acknowledgement.** This research was supported by the Fundamental Research Funds for the Central Universities (Grant No. 328202203, 20230045Z0114), China Postdoctoral Science Foundation funded project (Grant No. 2019M650606), First-class Discipline Construction Project of Beijing Electronic Science and Technology Institute (Grant No. 3201012).

## References

1. Wang, J., Xu, Y.: Internet usage, human capital and CO2 emissions: a global perspective. *Sustainability* **13**(15), 8268 (2021)
2. Ørmen, J., Helles, R., Jensen, K.B.: The social uses of the Internet: Introduction to the special section. *New Media Soc.* **23**(7), 1739–1750 (2021)
3. Wu, H., Ba, N., Ren, S., Xu, L., Chai, J., Irfan, M., et al.: The impact of internet development on the health of Chinese residents: transmission mechanisms and empirical tests. *Socioecon. Plann. Sci.* **81**, 101178 (2022)
4. The 51st Statistical Report on Internet Development in China by China Internet Network Information Centre (CNNIC), <https://cnnic.cn/n4/2023/0302/c199-10755.html>. Accessed 20 Jun 2023
5. Saba, T., Rehman, A., Sadad, T., Kolivand, H., Bahaj, S.A.: Anomaly-based intrusion detection system for IoT networks through deep learning model. *Comput. Electr. Eng.* **99**, 107810 (2022)
6. Zhang, K., Zheng, W., Yu, X., Wang, H., Wang, Z.: Research on recognition of network security situation elements based on PSO-TSA model. *J. Hunan Univ. (Nat. Sci.)* **49**(04), 119–127 (2022)
7. Guembe, B., Azeta, A., Misra, S., Osamor, V.C., Fernandez-Sanz, L., Pospelova, V.: The emerging threat of ai-driven cyber attacks: a review. *Appl. Artif. Intell.* **36**(1), 2037254 (2022)
8. Kim, K., Alfouzan, F.A., Kim, H.: Cyber-attack scoring model based on the offensive cybersecurity framework. *Appl. Sci.* **11**(16), 7738 (2021)
9. Lallie, H.S., et al.: Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Comput. Secur.* **105**, 102248 (2021)
10. Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., Michaloliakos, M.: Cybersecurity challenges in the maritime sector. *Network* **2**(1), 123–138 (2022)
11. Tufail, S., Parvez, I., Batool, S., Sarwat, A.: A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid. *Energies* **14**(18), 5894 (2021)
12. Mijwil, M., Doshi, R., Hiran, K.K., Al-Mistarehi, A.H., Gök, M.: Cybersecurity challenges in smart cities: an overview and future prospects. *Mesop. J. Cybersecur.* **2022**, 1–4 (2022)
13. Hussain, A., Mohamed, A., Razali, S.: A review on cybersecurity: challenges & emerging threats. In: *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*, pp. 1–7. Association for Computing Machinery, New York, USA (2020)
14. Bass, T.: Intrusion detection systems and multisensory data fusion: creating cyberspace situational awareness. *Commun. ACM* **43**(4), 99–105 (2000)
15. Blyth, A.: Footprinting for intrusion detection and threat assessment. *Inf. Secur. Tech. Rep.* **4**(3), 43–53 (1999)
16. De Montigny-Leboeuf, A., Massicotte, F.: Passive network discovery for real time situation awareness. In: *Proceedings of the The RTO Information Systems Technology Panel (IST) Symposium on Adaptive Defence in Unclassified Networks*, pp. 288–300 (2004)

17. Yurcik, W., Barlow, J., Lakkaraju, K., Haberman, M.: Two visual computer network security monitoring tools incorporating operator interface requirements. In: ACM CHI Workshop on Human-Computer Interaction and Security Systems (HCISEC) (2003)
18. Cisco: NetFlow Services and Applications. White Paper (1999)
19. Liao, Y., Zhao, G., Wang, J., Li, S.: Network security situation assessment model based on extended hidden Markov. *Mathematical Problems in Engineering* 2020 (2020)
20. Chen, X., Zheng, Q., Guan, X., Lin, C.: Quantitative hierarchical threat evaluation model for network security. *J. Softw.* **04**, 885–897 (2006)
21. Gu, Z., Wang, R.: A security situation assessment model of information system based on improved fuzzyanalytical hierarchy process. *Comput. Eng. Sci.* **38**(10), 2010–2017 (2016)
22. Shi, L., Xu, X., Liu, Y., Liu, J.: An Improved probabilistic neural network method of security situation assessment for industrial control system. *Netinfo Secur.* **21**(03), 15–25 (2021)
23. Elman, J.L.: Distributed representations, simple recurrent networks, and grammatical structure. *Mach. Learn.* **7**, 195–225 (1991)



# Enhancement of IRS-Assisted Wireless Localization System in NLOS Conditions

Boyu Liu<sup>1</sup>, Xudong Wang<sup>2</sup> , Feng Gao<sup>1</sup> , Yanru Wang<sup>3</sup>, Yujie Qiu<sup>2</sup>,  
and Lei Feng<sup>2</sup> 

<sup>1</sup> State Grid Henan Electric Power Company Information and Communication Branch, Henan 450052, China

fenglei@bupt.edu.cn

<sup>2</sup> The State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

<sup>3</sup> Beijing FibriLink Communications Co., Ltd., Beijing 100070, China

**Abstract.** In this paper, a millimeter-wave wireless localization model assisted by IRS is developed to explore the wireless localization problem under NLOS conditions. By deriving and analyzing the Fisher information matrix and Cramer-Rao lower bounds(CRLB), the accuracy index and optimization criteria are quantified, and a phase shift optimization method based on the semi-positive definite relaxation method is proposed to achieve the optimization of the localization performance of the system as a result. Simulation results show that the algorithm proposed in this paper can improve the performance of the system significantly compared with the benchmark solution.

**Keywords:** Non line of sight · Wireless localization · Reconfigurable intelligent surfaces · Cramer-Rao lower bounds

## 1 Introduction

In recent years, Intelligent Reflecting Surfaces(IRSs) have become a popular research object in academia and industry for their low cost, low energy consumption, and low complexity, and are considered as one of the key technologies for the development of next-generation wireless communication systems .IRS can be considered as a planar array which is consisted of a large number of passive reflective elements, each of which is capable of adjusting the amplitudes or phase shifts of incoming signals separately and independently. In the scheme of wireless network deployment, the reflection coefficients of the passive reflecting elements on the IRS can be changed by programming to optimization of transmission channels, which provides a new way to solve the channel fading. Compared to traditional active antenna arrays, IRS can achieve higher quality signal transmission with very low hardware cost and energy consumption [1]. In addition, IRS is usually standard in shape and light in weight, and can be easily deployed and installed in various environments,providing great flexibility.

Many advantages of IRS provide a brand new idea for the development of localization system. How to effectively combine IRS and localization system to overcome the difficulties in traditional localization methods and achieve low-cost, low-loss and high-precision localization is of great research significance.

Recently, IRS has been frequently tried to combine with wireless localization systems, and a series of studies for IRS-assisted localization systems are springing up. Many studies have focused on the derivation of basic boundaries to discuss the feasibility and efficiency of IRS-assisted localization systems [2]. In addition, there are also studies focusing on the localization accuracy and localization quality of the system [3], and many practical algorithms have been proposed to improve the localization performance of the systems.

To solve the problem of severely degraded accuracy of millimeter-wave wireless localization system under NLOS conditions, this paper proposes to establish an IRS-assisted millimeter-wave wireless localization system, derive the Cramer-Rao lower bounds and propose an optimization method, so as to provide high-precision localization service for the UE under NLOS conditions.

In this paper, we model and analyze the optimization problem based on convex optimization theory according to the CRLB. We propose an optimization method based on Semi-positive Definite Relaxation(SDR) method to achieve relaxation of constraints, and then get the optimal results by Gaussian randomization method to achieve the improvement of the localization performance of the system.

## 2 System Model

An IRS-assisted millimeter-wave wireless localization model is showed in Fig. 1, which consists of a base station (BS), a IRS and a user equipment(UE), where the BS and UE are equipped with a single antenna and the IRS is equipped with  $M$  reflective units. In this case, the BS is completely blocked from the UE, the channel is in NLOS conditions, and a cascade channel consisting of the BS, IRS and UE provides a stable LOS link between the two ends.

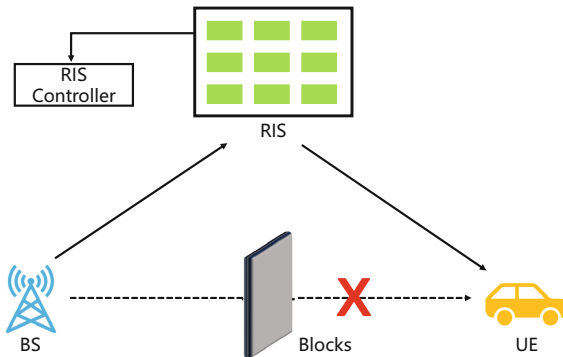


Fig. 1. IRS-assisted millimeter wave wireless localization model.

## 2.1 Geometry Model

In this paper, the center of the IRS is taken as the origin and the corresponding normal of the IRS is taken as the Z-axis to establish a space rectangular coordinate system as shown in Fig. 2.

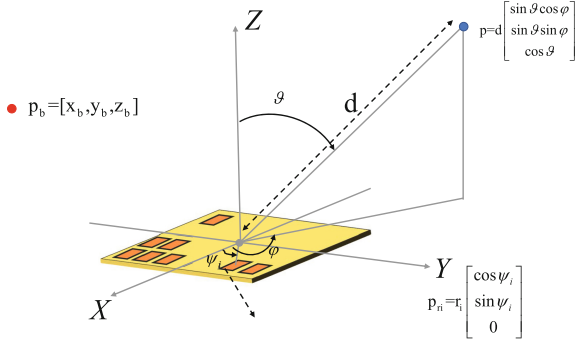


Fig. 2. System coordinates diagram.

The coordinates of the BS are known and are set as  $p_b = [x_b, y_b, z_b]^T$ ; the coordinates of the IRS are denoted as  $p_r$ , and the coordinates of the  $i$ th reflective unit can be written as  $p_{ri} = [x_{ri}, y_{ri}, 0]^T = r_i[\cos \psi_i, \sin \psi_i, 0]^T$  ( $i = 1, 2, \dots, M$ ), where  $r_i$  is the linear distance between the unit and the BS, and  $\psi_i$  is the coordinate angle in the XY-plane. The location of the UE is expressed as  $p = [x, y, z]^T$ . The angle between the Z-axis and the X-axis is expressed as  $\vartheta \in [0, \pi/2]$ , the angle between the projection of the UE in the XY-plane and the X-axis is expressed as  $\varphi \in [0, 2\pi]$ , and  $d$  is the linear distance between the UE end and the BS. Therefore, from the geometric relationship, the location of the UE can be written as  $p = d[\sin \vartheta \cos \varphi, \sin \vartheta \sin \varphi, \cos \vartheta]^T$ .

## 2.2 Signal Model

We assume a narrowband signal model to send the pilot signals  $s_t$ , and the BS transmits  $T$  times with bandwidth  $W$  and transmit power  $P_{TX}$ .  $\Omega_t = \text{diag}(\omega_t)$  denotes the phase shifts of the IRS at the time of the  $t$ th signal transmission, where  $|\omega_t[m]| = 1, \forall t, m$ .

Under NLOS conditions, the received signal at the UE at time  $t$  can be expressed as:

$$y_t = Ch^T(p_b)\Omega_t h(p)s_t + n_t \quad (1)$$

where  $C$  is the the temporal steering matrix to represent the slow phase rotation caused by the Doppler effect due to the movement of the UE [4]:

$$C = \exp(j \frac{2\pi v}{W\lambda}(p_r - p) / \|p_r - p\|) \quad (2)$$

$h(p)$  denotes the channel response between the UE and the IRS, where the IRS is considered as a Uniform Planar Array (UPA) and the channel response can be expressed as  $h(p) = \rho(p) \circ a(p)$ .  $\rho(p)$  denotes the channel gain between the UE and the IRS, then  $a(p)$  is the received array response, and in the near-field model, the channel gain and array response of a uniform planar array are usually given by [5]

$$[a(p)]_i = \exp(-j \frac{2\pi}{\lambda} (\|p - p_{ri}\| - d)) \quad (3)$$

$$\rho(p) = \sqrt{f(\vartheta, \varphi) \frac{A \cos \vartheta}{4\pi d^2}} \quad (4)$$

The definition of  $f(\vartheta, \varphi)$  is similar to [6], the channel response between the BS and the IRS is defined in the same way as  $h(p_b) = \rho(p_b) \circ a(p_b)$ .

We think that  $s_t = \sqrt{E_s}$  and  $n_t$  is an independently distributed zero-mean additive Gaussian noise with variance of 2 in each real dimension.

The received signal in T transmissions can be compactly expressed as

$$y = \sqrt{E_s} \rho C W^T a(p) + n \quad (5)$$

where  $n = [n_1, n_2, \dots, n_T]^T$ ,  $W = [w_1, w_2, \dots, w_T]^T \in \mathbb{M} \times T$  and  $w_t$  is defined as  $w_t = \Omega_t h(p_b) \in \mathbb{M} \times 1$ .

### 3 Localization Performance Metric

In this section, the optimization criteria will be clarified through the derivation of the CRLB of the system.

First, after separating the received signal from the noise, the rest can be expressed as:

$$\mu = \sqrt{E_s} \rho C W^T a(p) + n \quad (6)$$

We define the vector of unknowns as  $\zeta_{\text{sph}} = [\rho, C, p]^T \in \mathbb{5} \times 1$ , and the Fisher Information Matrix (FIM) corresponding to the vector of unknowns as

$$J(\zeta_{\text{sph}}) = \frac{2E_s}{N_0} \Re \left\{ \left( \frac{\partial \mu}{\partial \zeta_{\text{sph}}} \right)^H \frac{\partial \mu}{\partial \zeta_{\text{sph}}} \right\} \quad (7)$$

Each item of  $\partial \mu / \partial \zeta_{\text{sph}}$  can be expressed separately as follows:

$$\frac{\partial \mu}{\partial \rho} = \sqrt{E_s} C W^T a(p) \quad (8)$$

$$\frac{\partial \mu}{\partial C} = \sqrt{E_s} \rho W^T a(p) \quad (9)$$

$$\frac{\partial \mu}{\partial p} = \sqrt{E_s} \rho C W^T \frac{\partial a(p)}{\partial p} \quad (10)$$

For the subsequent derivation, we define  $\partial a(p)/\partial p$  as  $D(p)$ , the corresponding expressions are

$$D(p) = \frac{\partial a(p)}{\partial p} = j \frac{2\pi}{\lambda} \left( \text{diag}(a(p))K^T + a(p) \frac{p^T}{d} \right) \quad (11)$$

where  $K = [e_0, e_1, \dots, e_{M-1}]$  and  $e_i = (q_i - p)/\|q_i - p\|$ .

Substituting the above items into the FIM expression, the individual non-zero terms in the FIM can be found as

$$[J(\zeta_{\text{sph}})]_{1,1} = \frac{2E_s C^2}{N_0} (a^H(p)WW^T a(p)) \quad (12)$$

$$[J(\zeta_{\text{sph}})]_{2,2} = \frac{2E_s \rho^2}{N_0} (a^H(p)WW^T a(p)) \quad (13)$$

$$[J(\zeta_{\text{sph}})]_{3:5,3:5} = \frac{2E_s \rho^2 C^2}{N_0} (D^H(p)WW^T D(p)) \quad (14)$$

$$[J(\zeta_{\text{sph}})]_{1,3:5} = \frac{2E_s \rho C^2}{N_0} (a^H(p)WW^T D(p)) \quad (15)$$

$$[J(\zeta_{\text{sph}})]_{2,3:5} = \frac{2E_s \rho^2 C}{N_0} (a^H(p)WW^T D(p)) \quad (16)$$

After getting the FIM of the vector of unknowns, the FIM of the locations is obtained by

$$J(p) = [J(\zeta_{\text{sph}})]_{3:5,3:5} - [J(\zeta_{\text{sph}})]_{3:5,1:2} [J(\zeta_{\text{sph}})]_{1:2,1:2}^{-1} [J(\zeta_{\text{sph}})]_{1:2,3:5} \quad (17)$$

The CRLB of the locations of the UE can be expressed as:

$$\text{CRLB} = \sqrt{\text{trace}([J^{-1}(p)]_{3:5,3:5})} \quad (18)$$

## 4 Optimization Method for Localization

From the derivation results of CRLB, it is not difficult to find that the localization performance of the system is actually only related to the users' locations and the phase shifts of the IRS. Under the assumption that the users' locations are known, the optimization goal is to achieve the improvement of the system localization performance by optimizing the phase shifts of the IRS.

We set  $\Omega = [\Omega_1, \Omega_2, \dots, \Omega_T]$ , to denote the set of the phase shifts of the IRS, and the optimization problem can be expressed as:

$$\min_{\Omega} \text{CRLB}(\Omega) \quad (19)$$

$$s.t. \quad |[\omega_t]_m| = 1 \quad (20)$$

It is obvious that the constrained constant modulus in (19) makes the optimization problem a non-convex problem. Therefore, the first step is to transform



the non-convex problem into a convex one. And for the non-convex problem generated by the constrained constant modulus, the SDR method is a great solution idea without a doubt [7].

First, we define  $V = \Omega\Omega^T$ , which is obviously a positive semi-infinite matrix, and according to the properties of positive semi-infinite matrices, the optimization problem can be re-expressed as

$$\min_V \text{CRLB}(V) \quad (21)$$

$$s.t. \text{tr}(V) = MT \quad (22)$$

$$V \succeq 0 \quad (23)$$

$$\text{rank}(V) = T \quad (24)$$

After converting the problem into the standard SDR form, it is easy to find that (24) is actually non-convex, and this rank constraint should be ignored to achieve the constraint relaxation and transform the whole problem into a convex one.

According to the linear character of the FIM, the constraints satisfy the linear matrix inequality (LMI) form now. Meanwhile, by introducing Schur's complement and the auxiliary matrix  $Q$ , the problem can be represented in the standard convex semi-free program (SDP) form. Thus, the optimization problem can finally be expressed as

$$\min_V \text{tr}(Q) \quad (25)$$

$$s.t. \text{tr}(V) = MT \quad (26)$$

$$V \succeq 0 \quad (27)$$

$$\begin{bmatrix} Q & I \\ I & J^{-1}(p) \end{bmatrix} \succeq 0 \quad (28)$$

The problem has been completely transformed into a standard SDP form, and the CVX toolbox can be used to find the optimal result at this point. After getting  $V^*$ , we can get  $\Omega^*$  by Gaussian randomization.

## 5 Simulation Results

In this section, several simulations are provided to test the system performance and optimization method, and through the simulation results, we discuss the influence factors of system performance, verify the feasibility and superiority of the optimization method by analyzing from different perspectives.

We set the frequency of carriers  $f_c$  is 30 GHz, the number of transmissions  $T$  is 60, the noise spectral density  $NSD$  is  $-174$  dBm/Hz, the Bandwidth  $B_w$  is 0.001 GHz, the noise factor  $N_f$  is 8dB. In addition, the locations of the IRS and BS are set as  $[0, 0, 0]^T$ m and  $[0, 0, 5]^T$ m.

### 5.1 System Performance and Affecting Factors

In this part, we compare the actual performance of the system under different conditions by adjusting parameters such as the number of IRS reflective units, transmitting power, and the number of transmissions.

**5.1.1 Number of IRS Reflective Units** Figure 3 shows the distribution of the CRLB at different distances for the number of reflective units  $M = 32 \times 32, 40 \times 40, 45 \times 45$  and  $50 \times 50$  in the random phase shifts configuration. It is obvious that the CRLB at different distances with the increase of the number of IRS reflective units, all other conditions being constant. In other words, the higher the number of reflective units in the system, and the higher the localization accuracy.

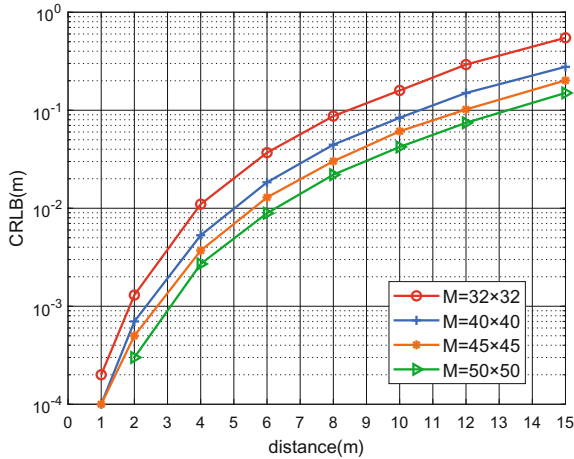


Fig. 3. Distribution of CRLB with different number of reflective units.

**5.1.2 Transmitting Power** With the random phase shifts configuration of  $M = 32 \times 32$  and straight-line distances of 5, 10, and 15 m as sampling points, Fig. 4 shows the variation of the CRLB of the system for different transmitting powers. It is obvious that the CRLB at different distances decreases with the increase of the transmitting power, and the performance improvement is especially obvious at the middle and long distances. At the distance of 10 m and 15 m, for every 5 dBm increases in transmitting power, the CRLB decreases by 42.2 and 43.4% on average. It shows that improving the transmitting power is undoubtedly an important means to improve the performance of the system.

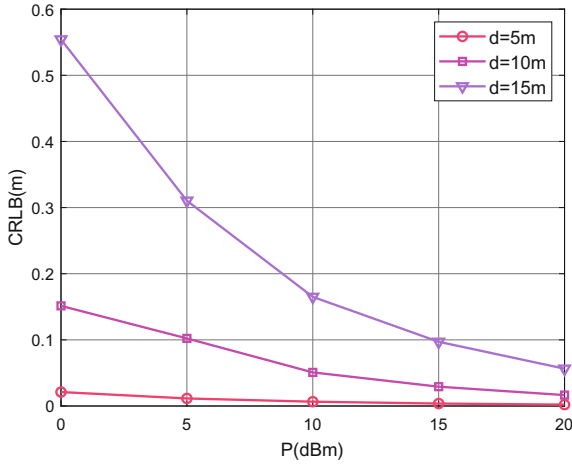


Fig. 4. Transmitted power and CRLB.

**5.1.3 Number of Transmissions** The same as above, the straight-line distances of 5, 10 and 15 m are set as the sampling points to explore the effect of the variation of transmission times on the overall performance of the system with  $M = 32 \times 32$ .

It is obvious in Fig. 5 that as the number of transmissions  $T$  increases, the quality of the received signal becomes better, and the localization performance of the system becomes better as a result. However, as the number of transmissions gradually increases, the improvement of the system performance becomes smaller and smaller. Especially in the middle and close distances, after the num-

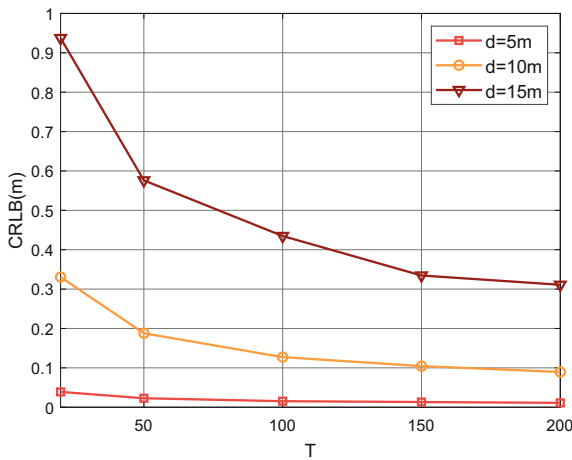


Fig. 5. Number of transmissions and CRLB.

ber of transmissions reaches 100, the average reduction of CRLB is only 14.8 and 16.1% for each additional 50 transmissions. This indicates that the number of transmissions can be reasonably set in the actual deployment to avoid unnecessary waste of resources.

### 5.2 Analysis of Optimization Method

In this part, we set  $M = 32 \times 32$  and  $M = 45 \times 45$  respectively and use the random phase shifts configuration in the vast majority of studies as the benchmark scheme to contrast with the optimization method proposed in this paper. Figure 6 shows the CRLB of the system after applying the optimization method and compare it with the the benchmark scheme. It is clear that the performance of the system is significantly improved, which proves the feasibility and effectiveness of the optimization method.

## 6 Conclusions

In this paper, we focus on the problem of IRS-assisted wireless localization in millimeter-wave communication systems, and realizes the optimization of IRS phase shifts through SDR-based optimization method, which in turn achieves the optimization of the localization performance of the system. Based on convex optimization theory, this paper completes the simulation, verification and comparison to prove the effectiveness and feasibility of the optimization method.

**Acknowledgment.** This work presented in this paper has been supported by the Research and Application of Multi-mode Merging Positioning and Synchronous Timing Technology in Power Safety Production Business (5700-2022242 07A-1-1-ZN).

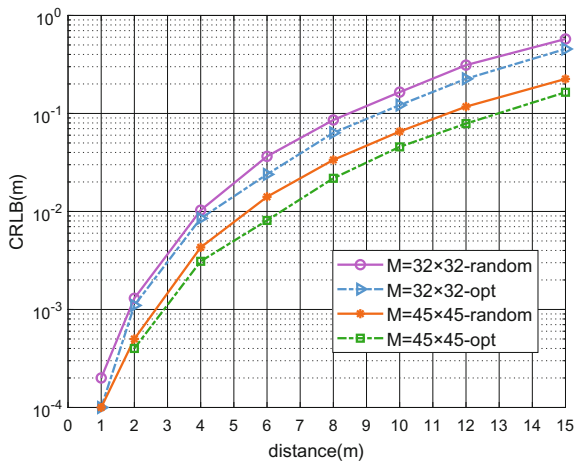





Fig. 6. Effectiveness of the optimization method.

## References

1. Wu, Q., Zhang, S., Zheng, B., You, C., Zhang, R.: Intelligent reflecting surface-aided wireless communications: a tutorial. *IEEE Trans. Commun.* **69**(5), 3313–3351 (2021). <https://doi.org/10.1109/TCOMM.2021.3051897>
2. Elzanaty, A., Guerra, A., Guidi, F., Alouini, M.: Reconfigurable intelligent surfaces for localization: position and orientation error bounds. *IEEE Trans. Signal Process.* **69**, 5386–5402 (2021). <https://doi.org/10.1109/TSP.2021.3101644>
3. Dardari, D., Decarli, N., Guerra, A., Guidi, F.: LOS/NLOS near-field localization with a large reconfigurable intelligent surface. *IEEE Trans. Wireless Commun.* **21**(6), 4282–4294 (2022). <https://doi.org/10.1109/TWC.2021.3128415>
4. Keskin, M., Wymeersch, H., Koivunen, V.: MIMO-OFDM joint radar-communications: is ICI friend or foe? *IEEE J. Sel. Top. Signal Proc.* **15**(6), 1393–1408 (2021). <https://doi.org/10.1109/JSTSP.2021.3109431>
5. Rahal, M., Denis, B., Keykhosravi, K., Uguen, B., Wymeersch, H.: IRS-Enabled Localization Continuity Under Near-Field Conditions (2021). <https://doi.org/10.48550/arXiv.2109.11965>
6. Abu-Shaban, Z., Keykhosravi, K., Keskin, M., Alexandropoulos, G., Seco-Granados, G., Wymeersch, H.: Near-field Localization with a Reconfigurable Intelligent Surface Acting as Lens, *ICC 2021—IEEE International Conference on Communications, Montreal, QC, Canada*, pp. 1–6 (2021). <https://doi.org/10.1109/ICC42927.2021.9500663>
7. Luo, Z., Ma, W., So, A., Ye, Y., Zhang, S.: Semidefinite relaxation of quadratic optimization problems. *IEEE Signal Process. Mag.* **27**(3), 20–34 (2010). <https://doi.org/10.1109/MSP.2010.936019>



# Current Situation and Prospect of Multi-energy Complementary Tidal Power Station Under Dual Carbon Background

Mingyang Sun  and Hongwei Li  

Shenyang Agricultural University, Shenyang 110866, Liaoning, China  
13386888406@189.cn

**Abstract.** Driven by the double carbon target, the energy revolution is imperative, and traditional single-energy power stations are gradually being transformed into a new system form with new energy complementary types, integrating digitalization and intelligence. China is promoting the development of multi-energy complementary tidal power stations, which incorporate and complement the use of green renewable energy sources such as light, wind, and tidal energy in an efficient manner. On this basis, multi-energy complementary tidal power stations should also combine the current digital, intelligent, networked, and platform-based technology features with building an intelligent platform to solve the new energy power station grid connection and other problems, thus improving the pressure on electricity and achieving clean use. In addition, China's rapid technological and social development, energy and enterprise transformation, and upgrading are imminent, so high efficiency, high integration, and friendly power stations have become an important trend for future development, with broad development prospects.

**Keywords:** Dual-carbon target · Energy integration · Complementary utilization

## 1 Introduction

China strives to achieve carbon peaking by 2030 and carbon neutrality by 2060. The dual carbon target is a major strategic deployment made by China after careful consideration. It is, moreover, a commitment by China to the world and is related to the sustainable development of the Chinese nation and the building of a community of human destiny. China's total annual carbon emissions are now equivalent to the combined carbon emissions of the European Union, the United States, and Japan. With the rapid social and economic development, China's electricity consumption and carbon emissions are also rising. According to the module calculation, carbon emissions from energy activities must be controlled at 7–9 billion tons in 2035 [1]. Therefore, the transformation of the energy structure is urgent. China's tidal energy reserves are 110 million KW [2], and as the earliest and largest green renewable energy source developed in China, its characteristics should be used efficiently. Other local green renewable energy sources should be integrated with digital, intelligent, and networked means for complementary

power generation, thus effectively reducing carbon emissions to achieve “carbon peaking” and “carbon neutral” in China. This will effectively reduce carbon emissions and thus contribute to achieving “carbon peaking” and “carbon neutrality” in China.

This paper introduces the principles of tidal energy generation and summarizes the multi-energy complementary tidal power plants at home and abroad. In addition, the paper analyses the problems of sedimentation, turbine attachment, and grid connection of new energy plants in tidal power stations. It proposes that digital twins should be used to solve these problems.

## 2 Principles and Characteristics of Tidal Energy Generation

Tidal energy is a non-fuel-consuming, non-polluting, inexhaustible, green, and renewable energy source not constrained by natural factors. Under the gravitational pull of the Moon and the sun, seawater will experience periodic changes in its rise and fall, known as the tidal phenomenon. When the positions of the Sun, the Earth, and the Moon are on the same line, a large tide is generated due to tidal forces, and when the relative positions of the three are perpendicular, a small tide is generated.

Tidal energy is mainly utilized in the power generation industry, and there are single-reservoir unidirectional, single-reservoir bidirectional, and double-reservoir continuous types [3]. Its power generation principle is similar to that of hydroelectric power generation when the water level rises at high tide, seawater enters the reservoir through the flow channel and impacts the turbine, converting the substantial potential energy of seawater into the kinetic energy of the turbine, pushing the turbine to rotate, which in turn drives the generator to rotate and generate electricity; at low tide, as the water level decreases, the same At low tide, the kinetic energy of the turbine is also converted into electrical energy to generate electricity. The main methods of tidal power generation are natural and tidal power generation [4]. Natural tidal power generation means that during high tide and low tide, generated by the gravitational force of the sun and the moon, a large amount of seawater will enter and leave the reservoir, and the kinetic energy generated will be transformed into mechanical energy and then into electricity; tidal power generation means that a dam is built at a place with a significant difference in seawater, and water is stored at high tide and released at low tide. The difference between high and low tide levels can be used to generate electricity.

Tidal energy is also highly regular and predictable and is not affected by weather or climate, and the power tends to be stable during high and low tides. Tidal power can only be generated daily at high and low tides, so it is intermittent, and seawater’s potential and pressure energy cannot be used. Therefore, tidal power generation must have a sizeable tidal level difference; the terrain can store water and other conditions, and proper site selection is essential. China’s eastern coastal areas are mainly plains and harbors, with many ports. Using favorable local favorable terrain to build dykes and use tidal energy for power generation can effectively drive the economic development of the local and surrounding areas.

### 3 Development of Complementary Tidal Power Plants

In recent years, the complementary power generation mode of tidal energy with renewable resources such as light and wind energy has attracted widespread attention from experts at home and abroad. Rich reserves and superior energy matching mode can effectively reduce carbon emissions. In the context of the policy of sustainable development of green energy, tidal energy complementary power generation for the power system to maximize the efficiency of power generation, with the rapid growth of society, increasing electricity consumption and energy reform, multi-energy complementarity, multidisciplinary integration, and digital integration become the main direction.

#### 3.1 Development of Tidal Complementary Power Station in China

China's coastline is more than 18,000 km long, and the islands have more than 14,000 km of coastline, making a total of more than 32,000 km of coastline rich in tidal energy resources, making it one of the wealthiest countries in the world in terms of tidal energy. Recently completed tidal power stations include the Wenling tidal power station, the Huanghe tidal power station, and the Baisakou tidal power station. The newly constructed Wenling Tidal Power Station has a photovoltaic area of 1.333 km<sup>2</sup>. It uses a single group of two-way power generation to control the timing and power of tidal power generation, to smooth out fluctuations in photovoltaic power generation, and to establish a digital platform to facilitate intelligent and integrated control of reporting, faults and power generation. With an average annual power generation of over 100 million kWh, Wenling Tidal Complementary Power Station saves over 30,000 tons of coal. It reduces carbon emissions by over 84,000 tons compared to thermal power stations [5], forming a complete tidal industry that has evolved from adapting to grid operation to supporting it and demonstrating the importance of green renewable energy in achieving China's dual carbon goals and energy revolution.

Secondly, the installed capacity of the Xingfuyang tidal power station in China is 1,280 KW, which adopts the ebb tide type of power generation and has an annual power generation capacity of 3,151,700 kWh; the installed capacity of the Baisakou tidal power station is 960 KW, which adopts the single bank and single item type of power generation and has an annual power generation capacity of 2 million kW·h [6]. Specific domestic and foreign tidal energy power station data are shown in Table 1.

**Table 1.** Current status of domestic tidal energy power stations

Name	Capacity(MW)	Annual (kW·h)	Method	Time
Wenling	100	10 billion	Solar and tidal	2022
Xingfuyang	1.28	3.15 million	One-way Ebb type	1989
Baishakou	0.96	2 million	One-way unidirectional	1978
Yuepu	1.5	0.31 million	One-way unidirectional	1971
Haishan	0.15	3 billion	Double storage	1975



### 3.2 Development of Tidal Complementary Power Station Abroad

The development and construction of tidal complementary power stations has been achieved in the last hundred years, and some of the more famous tidal power stations have been built in several countries around the world, such as: France's Lens tidal power station, which was put into operation in 1966, with an installed capacity of 240 MW, ranking second in the world [7]; the UK has announced a £1.7 billion Swansea tidal complementary power project in recent years, including hydro turbines, photovoltaic The UK has announced a £1.7 billion Swansea tidal complementary power project in recent years, including technologies such as hydro turbines, photovoltaic panels and battery storage [8]; the Annapolis tidal power station in Canada was completed in 1984 with an installed capacity of 20 MW [9]; the Shihwa Lake tidal power station in South Korea was officially opened in 2011 and has an annual capacity of 552 million kWh, making it the largest tidal power station in the world [10]; and the Kyushu Power Systems Company in Japan is starting to use wave and tidal power on a large scale in 2022—experiments using waves in conjunction with tides (Table 2).

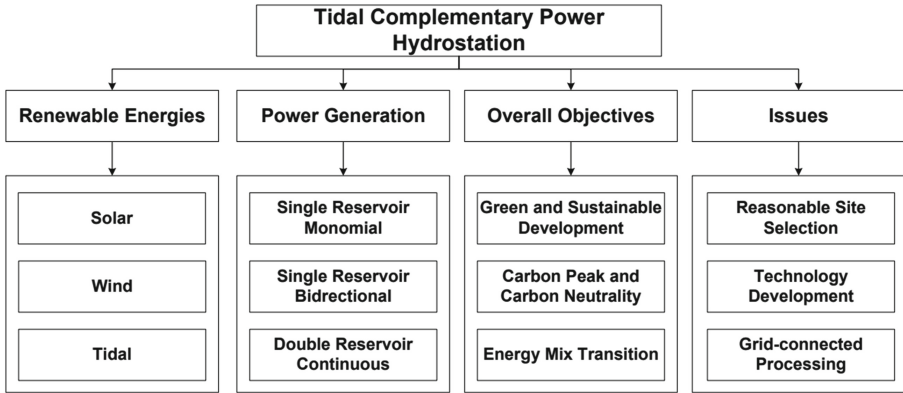
**Table 2.** Status of tidal power plants abroad

Name	Location	Capacity(MW)	Annual (kW·h)	Method
Lens	France	0.24	5.44 billion	One-way bidirectional
Annapolis	Canada	20	50 million	One-way unidirectional
Shihwa Lake	South Korea	254	5.2 billion	One-way unidirectional

From China's newly completed Wenling tidal-optical complementary power station to the UK's announcement of a tidal-optical complementary project to Japan's large-scale tidal-wind complementary experiments, it is easy to see that complementary renewable energy generation will become the main battleground of the energy revolution. The development of tidal energy will not only ease the problem of energy tension but also generate considerable revenue and can effectively promote the transformation of the energy structure, with a wide range of development potential (Fig. 1).

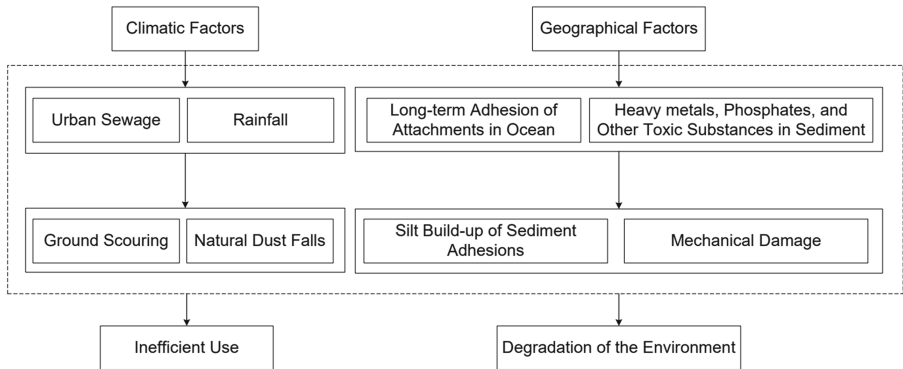
## 4 Bottlenecks and Suggestions in the Development of Tidal Power Plants in China

The tidal complementary power stations are built in the eastern coastal areas with a monsoon climate and plains. However, the two main factors that cause siltation are climatic and geographical factors, i.e., the discharge of urban sewage, ground wash water formed by rainfall, and natural dust fall. Similarly, during high and low tides, adhering materials in seawater can also enter the turbines and other equipment with seawater. On the one hand, siltation will lead to a reduction in reservoir capacity, reducing the influential head of the hydropower station and, in severe cases, losing some of its functions [11]. On the other hand, siltation contains heavy metals, phosphates, and other



**Fig. 1.** Types, role, and impact of tidal complementary power plants

toxic substances, which will pollute the water quality after a long period of siltation, causing the ecological environment to enter a vicious circle; adhering to the turbine for a long time will cause mechanical damage, and the vibration level will increase, significantly reducing efficiency. Long-term adhesion will also lead to erosion of the turbine blades. Suppose tidal energy is to be used efficiently for power generation. In that case, the siltation caused by seawater [12] and the adhesion of the turbine to the turbine are two critical issues in the operation and maintenance of water resources. Therefore, while tidal energy is being developed to complement other renewable energy sources for power generation, the problems of siltation and adhesion must be addressed (Fig. 2).



**Fig. 2.** Bottlenecks and suggestions

The following two suggestions and ideas are given concerning the problems of sedimentation and attachment, taking into account the characteristics of tidal energy and the current level of development of intelligent digital equipment:

1. For the problem of sediment siltation: the water level of reservoirs and inlets is generally deep enough for some of the vessels to enter, and the existing sand flushing technology can be used based on a group of two boats to clean up the sediment siltation, one of which is designed with an image recognition retractable hanging long probe for it, and at the same time, a particular space is set up to contain the sediment pumped out by the sand pumping vessel, and is compatible with the sand pumping vessel and submersible sand pump. The long probe can be used during operation and maintenance. During operation and maintenance, the long probe can be used for image recognition to determine the location where the silt needs to be removed, and the image is analyzed and uploaded to the designated screen of the sand pumping vessel, after which the sand pumping vessel travels to the specified location and releases the sand pump for sand pumping. The sediment pumped out by the submersible sand pump can be discharged directly into the exclusive flow channel. The sediment pumped out by the sand pump on the vessel is temporarily stored in another vessel and later released into the flow channel, which will eventually be discharged to the designated destination.

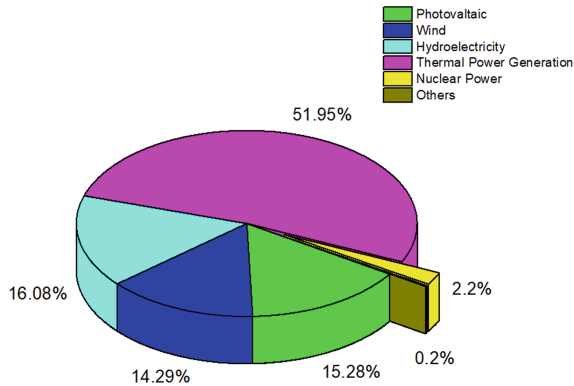
2. For the problem of microbial adhesion on the turbine blade: according to the specifications of the existing turbine blade, a kind of vinyl resin coating rotating type device for removing the adhesion on the turbine blade can be designed on the front and rear sides of the turbine blade, spraying anti-corrosion and anti-rust coatings to the device and the turbine blade, making full use of the time after the tide and before the tide, during the maintenance period, the turbine blade is first fixed by the caliper, after which During maintenance, the turbine blades are held in place by a caliper, after which the direction of rotation and speed of the device is controlled through intelligent control, thereby cleaning the turbine blades of the adhering material.

The above suggestions and ideas are intended to provide new ideas for the operation and maintenance management of tidal complementary power stations.

## **5 Grid Connection Problems and Recommendations for Multi-energy Generators**

China's manufacturing carbon emissions have increased from 1.866 billion tons in 2000 to 6.855 billion tons in 2018 [13]. To achieve "peak carbon" and "carbon neutrality," China must control its carbon emissions in power generation, which is why complementary power generation is essential. On the one hand, it reduces carbon emissions from burning coal. On the other hand, it protects the local ecological environment. China is rich in green renewable energy, with 110 million kW of tidal power available [14], 160 GW of wind energy available [15], and an average annual horizontal irradiation of about 1493.4 kWh/m<sup>2</sup> [16]. China's green and sustainable development strategy, with broad development prospects (Fig. 3).

There are also problems with the electrical system that should be noted. In the context of the large-scale installation of new energy sources and the continuous connection of new types of energy plants to the power system, problems such as the inability to predict loads promptly and the impact on the traditional power grid and energy storage will arise:



**Fig. 3.** Share of renewable energy in China

1. For the power grid side, the construction scale of the power grid is expanding, and the allocation and regulation capacity of green energy is being strengthened. With the addition of renewable energy generation equipment, the power security capacity should be gradually strengthened for the power supply side. For the load side, as China's economy grows steadily and rapidly, the demand for electricity from various sources is increasing daily. At the same time, new industries such as trams and automated factories are emerging, which also bring difficulties to the power system regarding peak regulation.

For the power grid side, to improve the stability of power grids around the country and to achieve the double carbon goal, the flexibility of coal power should be improved, the construction of pumped storage and tidal power plants should be expanded, and they should be equipped with electrochemical energy storage devices to cope with contingencies, to promote the upgrading of traditional solutions, to speed up the degree of matching of various power-using equipment with new energy equipment, and thus to promote the transformation of new power systems. For the power supply side, as all types of current new energy generation equipment are cyclical, taking pumped energy storage as an example, China mainly uses single-cycle combustion turbines. With the lack of oil and gas resources, more than gas-fired peaking power stations are needed. Thus the regulation performance is not high, and the current regulation energy is still dominated by coal power, so it is necessary to reasonably equip electrochemical energy storage equipment, which not only ensures that no electricity is wasted but also reduces the burden for grid-side dispatching, which can be used with dispatch. For the load side, scholars worldwide use neural networks, digital twins, and other methods to build load forecasting models. Extensive data analysis can effectively analyze the electricity consumption and power generation at various times in the past and thus get the optimal and most effective solution. However, it should be noted that if the current power system adopts digital twins and other methods on a large scale, it is necessary to strengthen the network security problem and always prevent data theft and hacking the trial.

2. China's current part of new energy generation equipment is distributed; when distributed, equipment for grid connection needs to have the corresponding laws and regulations to support and also to ensure that the grid interface unified problem, otherwise

can not be adapted to all provinces and cities in China, also can not meet the needs of grid connection, at the same time, in the grid interface design, but also pay attention to safety issues, to avoid accidents. Secondly, as new energy sources are volatile, dispersed, and cyclical, they must be dispatched in time to reduce the impact on the grid (Fig. 4).

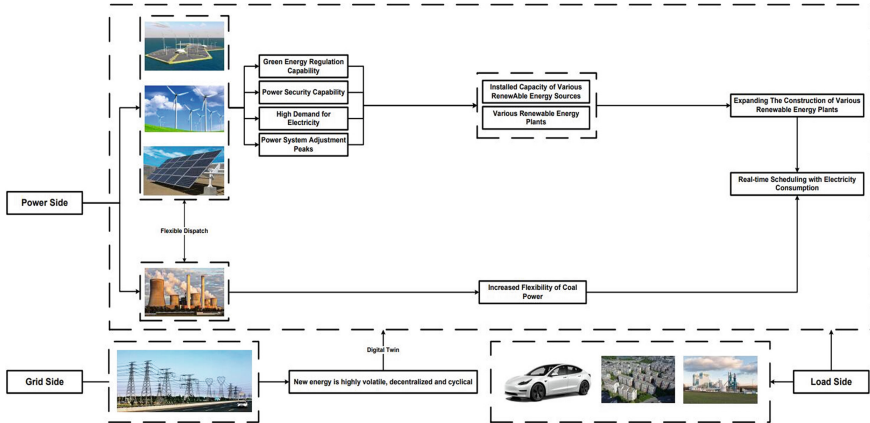


Fig. 4. Power system overview

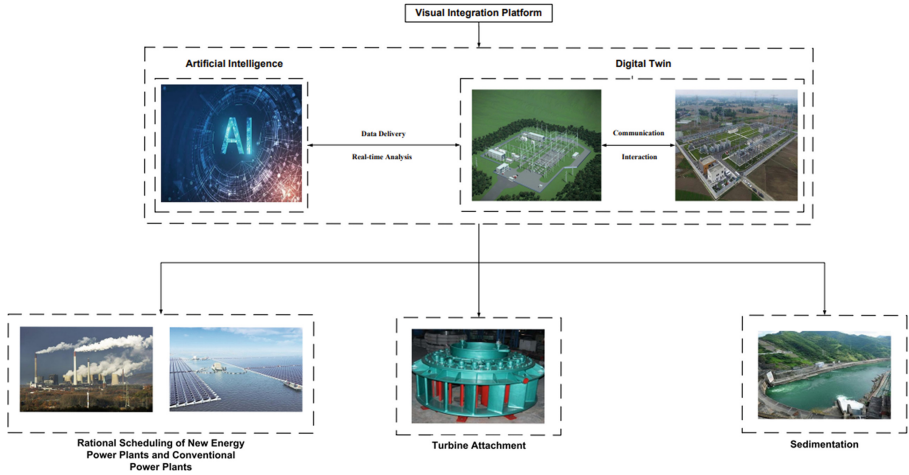
The above suggestions and ideas are intended to provide new ideas for the operation and maintenance management of tidal complementary power stations.

## 6 Application of Digital Twin and Artificial Intelligence in Multi-energy Complementary Power Plants

Digital Twin and Artificial Intelligence can fully use the communication and interaction between the virtual model and the actual object for real-time monitoring and analysis of massive amounts of data and platform it (Fig. 5).

1. Based on the above method, digital twin and artificial intelligence can be used for the problem of sedimentation. In large platforms such as control centers, virtual 3D models of the areas where the problem occurs should be created and interact with the physical models in real-time. The first step is to equip the working vessel with sensors that can acquire the status of the probes in real-time and transmit the various status information to a small digital twin platform on the boat. After this, the small platform can communicate in real time with the large platform in the control center to analyze the data in real-time. In addition, a predictive solution can be improved for staff by analyzing data on areas prone to siltation in previous years and presenting this on the mini-platform to enhance staff efficiency and solve siltation problems accurately.

2. On the basis of the above method and in dealing with the problem of turbine attachment, a large number of photographs of the attachments that may be attached to the turbine are first entered into a platform based on a combination of digital twin and artificial intelligence. Taking advantage of the intermittent nature of tidal power generation, image recognition is used in the interval to scan each blade and its surrounding



**Fig. 5.** Digital twin application

devices and match and analyze them with the library created by the platform to determine whether attachments are attached and the number of attachments. The virtual model shows the actual situation, helping staff find the attachment's location more efficiently and finally generating an optimal cleaning plan, using visualization to improve staff efficiency and provide convenience, avoiding significant economic losses.

3. Digital twins and artificial intelligence can also be applied to the problem of matching new energy plants with traditional ones. A virtual model is created for a region's grid side, load side, and grid measurement, forming an integrated visualization platform and capturing each region's electricity consumption and generation capacity in real-time. When there is a sudden increase in electricity consumption at a certain point in time, the platform can make reasonable forecasts based on data from previous years and alert staff to possible problems in advance. The platform should also propose an optimal dispatch plan for the team and reasonably dispatch new energy sources in the vicinity according to a predetermined algorithm. If any faults are encountered during dispatch, the team will be promptly alerted to resolve the faults as quickly as possible. It will play a decisive role in speeding up the transformation of the new power system.

## 7 Conclusion

As China enters a phase of high-quality development, electricity consumption is increasing, even to the extent that demand exceeds supply, and carbon emissions will also increase as electricity consumption increases, making the role of supporting the ecological environment more and more prominent. China is rich in tidal, light, wind, and other green energy sources. Therefore, vigorously developing new energy complementary power generation is a feasible and necessary path, which also occupies an important position in the sustainable development of energy and has a huge demand, with broad development prospects and potential. At the same time, the vigorous development of

new energy generation will also bring social and economic benefits to the local and surrounding areas. It will continue to make a solid effort to improve the quality of the ecological environment, thus achieving a beautiful picture of harmony between man and nature.

## References

1. Chao, Q.: The scientific meaning of carbon peaking and carbon neutrality and our policy measures. *Environ. Sustain. Dev.* **46**(02), 14–16 (2021)
2. Zhang, H.: Discussion on tidal power generation and its development prospect in China. *Energy and Energy Conserv.* **05**(164), 53 (2019)
3. Zhang, B.: Tidal power technology and prospects. *Sci. Technol. Inf.* **12**(09), 3–4 (2014)
4. Li, X., Qiao, C., Wang, X., Xie, W., Zhang H.: An overview of tidal power of China. In: *Henan Water Resources and South-to-North Water Diversion*, vol. 50, no. 10, pp. 81--82 (2021)
5. Hong, H., Qu, Y., Li, P., Jiang, Y.: China's first tidal complementary photovoltaic power plant commissioned. *Science and Technology Daily*, 1 (2022)
6. Liu, B., Su, J., Wang, L.: Research and development of tidal power generation in China. *Hydropower and New Energy* **32**(11), 3–4 (2018)
7. Apponai, C.: The experience of operating and managing a tidal power station in lens, France. *Express Water Resour. Hydropower Inf.* **32**(09), 29–30 (2011)
8. Tian, Y.: Independent audit report for the Swansea Bay Tidal Lagoon Power Project, UK. *Express Water Resour. Hydropower Inf.* **38**(09), 10 (2017)
9. Gao, Y., Li, Y., Zhang, H.: Outlook for tidal power technology. *J. Shandong Electric Power College* **19**(06), 61–62 (2016)
10. Yang, M.: Turning to the ocean for development momentum. *Economic Times*, 1 (2012)
11. Lu, Y., Xu, H., Li, G., Shang, Q., Sun, K.: Evaluation of the impact of sedimentation on the function of different types of reservoirs. *Yangtze River* **52**(S2), 238–240 (2021)
12. Han, C.: The state of development and prospects of tidal power generation. *Pract. Electron.* **06**(242), 237 (2013)
13. Li, X., Wang, Y.: Analysis of the drivers of carbon emissions in China's manufacturing sector based on LMDI decomposition. *Stat. Decis.* **38**(12), 60–62 (2022)
14. Yang, W.: Marine energy resources. *Hydro Sci. Cold Zone Eng.* **11**, 22 (2014)
15. Zhou, D.: Our wind energy resources. *Sino-Global Energy* **24**(07), 73 (2019)
16. Li, Y.: China's annual wind and solar resource bulletin 2021 released. *China Meteorological News*, 1 (2022)



# Resource Security Management Mechanism Based on Dynamic Key and Blockchain in Network Slicing Environment

Guoyi Zhang<sup>(✉)</sup>, Yang Cao, Huihong Luo, Hailong Zhu, Feifei Hu, and Xubin Lin

Power Control Center of China Southern Power Grid, Guangzhou 510623, China  
guoyizhang2021@163.com

**Abstract.** In order to solve the problem of economic loss caused by malicious use of underlying network resources by network attackers, this paper proposes a resource security management mechanism based on dynamic key and blockchain in the network slicing environment. First, a resource security management architecture based on dynamic key and blockchain in the network slicing environment is designed. The architecture includes two modules: the bottom network provider and the service provider. Each module consists of three sub modules: the certification center, the resource management center, and the resource settlement center. The overall mechanism of resource security management based on dynamic key and blockchain in the network slicing environment includes three steps: the service provider obtains the permission to apply for resources, the service provider applies for and obtains resources, and the underlying network provider completes the resource cost settlement. Through the analysis of resource security performance from three aspects of preventing man in the middle attack, preventing data tampering, and data leakage, we can see that the resource security management mechanism proposed in this paper can better solve the problem of economic loss caused by malicious use of underlying network resources by network attackers.

**Keywords:** Network virtualization · Resource allocation · Resource security · Dynamic key · Blockchain

## 1 Introduction

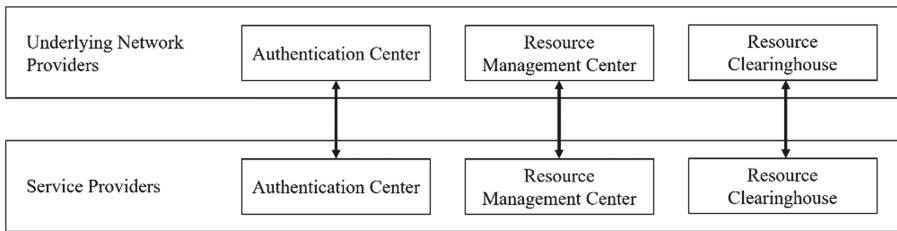
In the network slicing environment, the traditional physical network is divided into an underlying network and a virtual network. The underlying network is built and operated by the underlying network provider [1]. The virtual network is rapidly built by the service provider by leasing the resources of the underlying network and deploying professional services on it. In this context, service providers can quickly build virtual network environments so that they can concentrate on research and development of professional services, which provide richer services to end users [2]. As the underlying network providers make profits by renting network resources to the service providers, thus supporting the operation of the underlying network. The application and use of resources



by service providers is the source of profit for the underlying network providers. However, due to the increase in the number of cyber attacks and cyber crimes, network resources are maliciously requested and used by attackers, resulting in financial losses to the underlying network providers.

## 2 Architecture and Overall Mechanism

The resource security management architecture based on dynamic key and blockchain in the network slicing environment is shown in Fig. 1, including two modules of the underlying network provider and service provider. The underlying network provider is responsible for the creation and operation of the underlying network resources, which mainly consists of three parts: authentication center, resource management center and resource settlement center. The authentication center is responsible for authenticating service provider identity information and creating communication keys to encrypt communication data. The resource management center is responsible for resource allocation and performance management. The resource clearing center is responsible for charging the service provider for the use of resources.



**Fig. 1.** Dynamic key and blockchain-based resource security management architecture in network slicing environment.

The service provider is responsible for the application of the underlying network resources and the expenditure of resource fees, which also consists of three parts: the authentication center, the resource management center, and the resource clearing center. The authentication center is responsible for authenticating the underlying network provider and applying for obtaining communication keys. The resource management center is responsible for requesting resources from the underlying network provider and tracking the usage of resources and the performance data of resources. The resource clearing center is responsible for paying the underlying network provider for the use of resources.

The overall mechanism of dynamic key and blockchain-based resource security management in the network slicing environment includes three steps: service providers obtain the authority to apply for resources, service providers apply for and obtain resources, and the underlying network provider completes resource cost settlement. Each of them is described in detail below.

### 3 Service Provider Access to Request Resources

This step is initiated by the authentication center of the service provider to authenticate the underlying network provider. After the authentication is passed, the authentication center of the underlying network provider is responsible for completing the authentication of the service provider and the generation of the communication key. This step includes three sub-processes: authentication of the underlying network provider by the service provider, communication key generation by both parties, and issuance of resource application license certificate by the underlying network provider for the service provider.

#### 3.1 Service Provider Authentication of the Underlying Network Provider

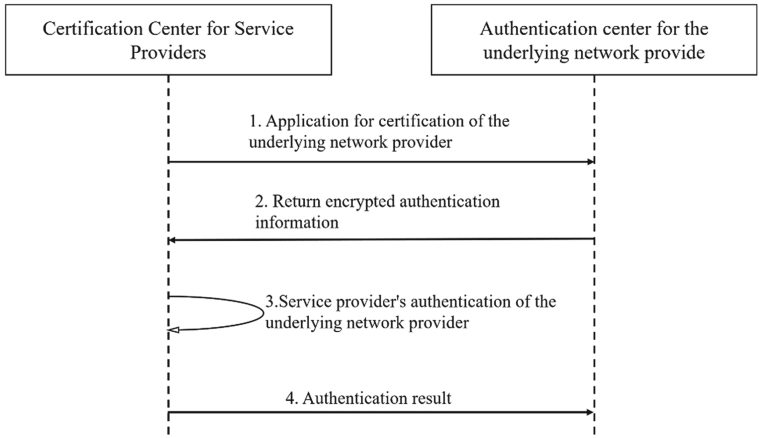
The process of authentication of the underlying network provider  $InP_j$  by the service provider  $SP_i$  (see Fig. 2) is as follows.

- (1) The service provider  $SP_i$  applies for authentication of the underlying network provider  $InP_j$ . When authenticating, the service provider carries attribute information including identity information, public key information, and service provider authentication random number P.
- (2) Returns the encrypted authentication information. The authentication information includes: service provider public key encryption (underlying network provider private key encryption (P)), service provider public key encryption (underlying network provider private key encryption (G)). Where, G is the authentication random number generated by the underlying network provider.
- (3) The service provider authenticates the underlying network provider. The service provider decrypts the data with its own private key, and then decrypts the data with the public key of the underlying network provider to get the certified random number G generated by the underlying network provider and the service provider certified random number P. The decrypted certified random number P is compared with the certified random number sent to the underlying network provider. If they are the same, the authentication is successful.
- (4) Return authentication results.

#### 3.2 Both Parties Generate Communication Keys

In order to secure the communication between the service provider and the underlying network provider, both parties generate communication keys and then encrypt the subsequent communication data. The process of communication key generation by both parties (see Fig. 3) is as follows.

- (1) The service provider  $SP_i$  calculates and sends the dynamic key parameters: the service provider generates the key value  $X'$ , uses the formula  $X'' = G^{X'} \text{ mod } P$  to calculate the service provider  $SP_i$  dynamic key parameters  $X''$ , encrypts them with the public key pair  $X''$  of the underlying network provider  $InP_j$  and sends them to the underlying network provider  $InP_j$ .



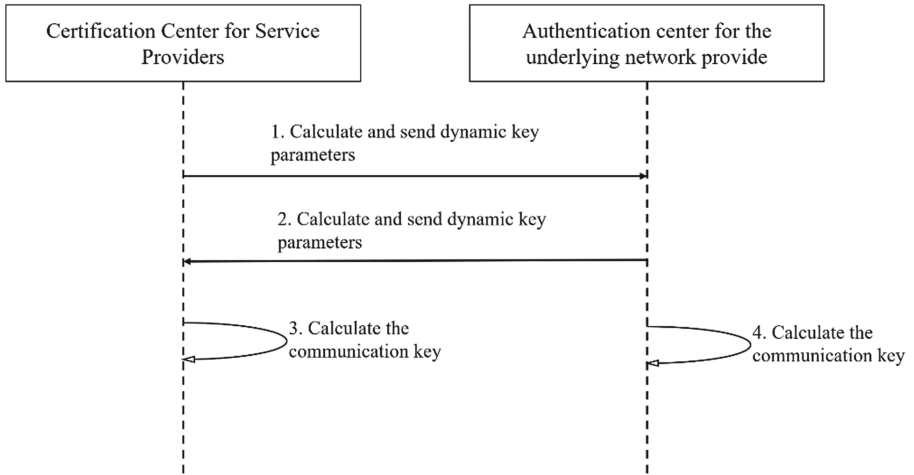
**Fig. 2.** Service provider authenticates to the underlying network provider

- (2) The underlying network provider  $InP_j$  calculates and sends the dynamic key parameters: the underlying network provider  $InP_j$  generates the key value  $Y'$ , uses the formula  $Y'' = G^{Y'} \text{ mod } P$  to calculate the dynamic key parameters  $Y''$  of the underlying network provider  $InP_j$ , uses the public key pair  $Y''$  of the service provider to encrypt and sends to the service provider  $SP_i$ .
- (3) Service provider  $SP_i$  calculates the communication key: the service provider  $SP_i$  decrypts the data using its own private key and calculates the communication key  $Key_{ij}$  using the formula  $Key_{ij} = Y''^{X'} \text{ mod } P$ .
- (4) The underlying network provider  $InP_j$  calculates the communication key: the underlying network provider  $InP_j$  uses its own private key to decrypt the data and uses the formula  $Key_{ij} = X''^{Y'} \text{ mod } P$  to calculate the communication key  $Key_{ij}$ .

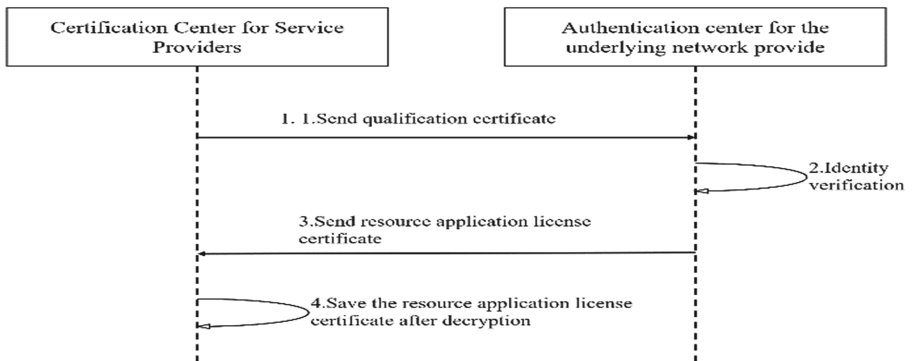
**3.3 Underlying Network Provider Issues Resource Request Licenses for Service Providers**

The steps for the underlying network provider to issue a resource request license certificate for the service provider (see Fig. 4) are as follows.

- (1) Sending the qualification certificate: The service provider  $SP_i$  sends the qualification certificate as identity information. The sent information is encrypted using the communication key, the public key of the underlying network provider.
- (2) Identity verification: After decryption using the communication key and its own private key, the underlying network provider  $InP_j$  verifies the service provider's qualification certificate.
- (3) Send resource application license certificate: After encrypting the resource application license certificate  $RL_i$  with the communication key and the public key of the service provider, send the resource application license certificate.
- (4) Save the resource application license certificate after decryption  $RL_i$ .



**Fig. 3.** Both parties generate communication keys.



**Fig. 4.** Underlying network provider issues resource request licenses for service providers.

### 3.4 Service Providers Apply and Obtain Resources

This step is initiated by the resource management center of the service provider to request resources, and the resource management center of the underlying network provider is responsible for completing the resource allocation. The steps of this process (see Fig. 5) are as follows.

- (1) Generate resource request. The resource request center of the service provider generates the resource request  $RR_i$ , including the type of resources needed, the number of resources and the resource reliability requirements.
- (2) Send encrypted resource request. Use its own private key and communication key to encrypt the resource application request  $RR_i$  and resource application license certificate  $RL_i$ , and then send them to the underlying network service provider.

- (3) Authenticate and establish a secure communication connection. The authentication center of the underlying network service provider authenticates the service provider. After decryption, the validity of the resource request license certificate  $RL_i$  is verified and a secure communication connection between the resource allocation center of the underlying network service provider and that of the service provider is established. If the verification does not pass, the process ends.
- (4) Allocate the resource request. The resource request  $RR_i$  is sent to the resource allocation center.
- (5) Allocate resources. The resource allocation center allocates resources using the resource allocation algorithm.
- (6) Request for blockchain bill generation. If the allocation is successful, the allocation result  $RA_i$  will be sent to the resource clearing center, and if the allocation fails, the resource allocation center will be notified of the failed allocation.
- (7) Generate blockchain bills. The resource clearing house uses blockchain technology to generate blockchain bills  $BCB_i$  based on the allocation results  $RA_i$ .
- (8) Return blockchain billing. The resource clearing house returns a blockchain bill  $BCB_i$  to the resource allocation center.
- (9) Return resource allocation results. The resource allocation center returns the allocation result to the service provider resource request center. If it succeeds, the allocation result  $RA_i$  and blockchain bill  $BCB_i$  are returned. In case of failure, the allocation failure result is returned.

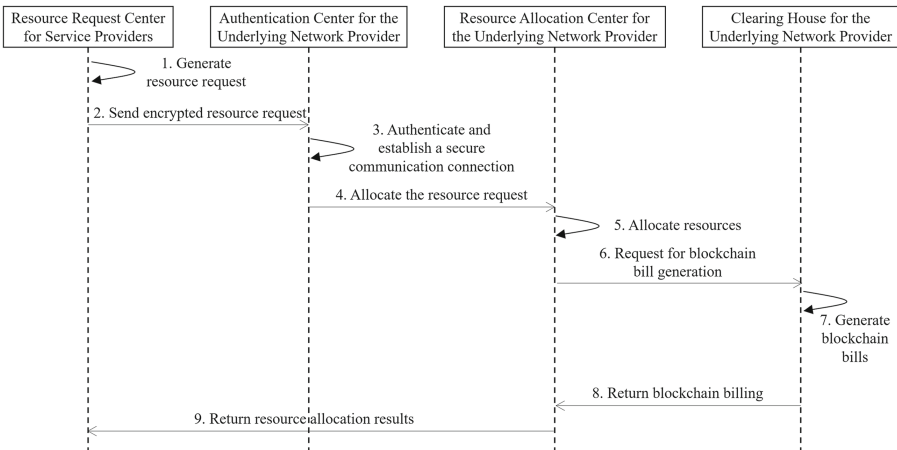


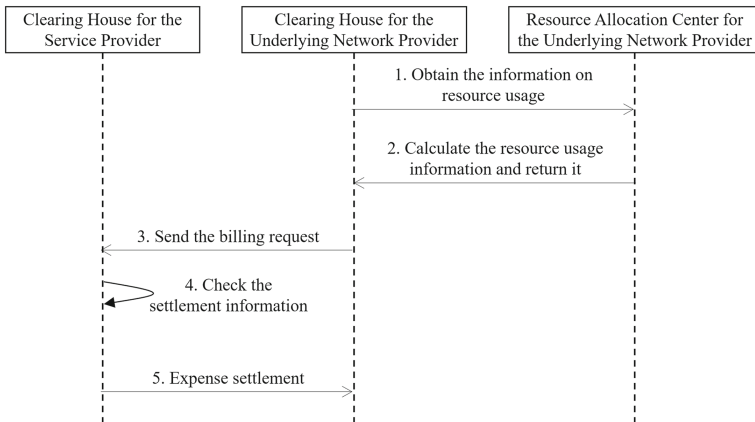
Fig. 5. Service providers apply and obtain resources.

### 3.5 Underlying Network Providers Complete Resource Cost Settlement

This step is initiated by the resource settlement center of the underlying network provider, and the resource cost settlement is completed with the cooperation of the resource settlement center of the service provider. The resource cost settlement is carried out based

on the secure communication link established by the authentication center, which can ensure the security of data. This step (see Fig. 6) mainly includes the following processes.

- (1) Obtain the information on resource usage. The clearing center of the underlying network provider gets the billing information that needs to be settled according to the settlement rules. Based on the billing information, the resource usage information is requested from the resource management center.
- (2) Calculate the resource usage information and return it. The main contents include the amount of resource usage and the fulfillment of resource usage service level agreement.
- (3) Send the billing request. The underlying network provider gets the cost information that needs to be settled according to the resource usage information and the service quality agreement. The settlement center of the underlying network provider sends a settlement request to the clearing house of the service provider, including blockchain billing and resource usage information.
- (4) Check the settlement information. The clearing house of the service provider checks the settlement information. It mainly checks the authenticity of the blockchain bill and the accuracy of the resource usage.
- (5) Expense settlement. According to the settlement requirements, the service provider gives the underlying network provider a fee settlement.



**Fig. 6.** Underlying network providers complete resource cost settlement.

## 4 Security Performance Analysis

Resource security performance analysis is conducted in three aspects: prevention of man-in-the-middle attacks, prevention of data tampering, and data leakage.

#### 4.1 Analysis of Man-In-The-Middle Attack Prevention

The possible problem of man-in-the-middle attack is that the attacker plays the role of the underlying network provider or service provider. In the process of authentication mechanism, the service provider authenticates the underlying network provider based on the public key information of the underlying network provider. The underlying network provider authenticates the service provider based on the public key and qualification certificate of the service provider. The mutual authentication of both parties better prevents the occurrence of man-in-the-middle attack events.

#### 4.2 Analysis of Data Tampering Prevention

The main disagreement in the process of service usage is the disagreement of billing. In order to prevent the bill data from being tampered with, the use of blockchain technology to store the bill data effectively solves the problem of data tampering.

#### 4.3 Analysis of Data Leakage Prevention

The underlying network service provider and service provider use each other's public key encryption in the identity authentication process to prevent data leakage in the identity authentication. In the process of data communication, the communication key and the public key of both parties are used to encrypt, preventing the data leakage from happening.

## 5 Conclusion

Network virtualization technology has emerged as an effective method to improve network resource utilization and quality of service. However, with the increase of malicious use of underlying network resources by cyber attackers, it has led to more and more underlying network providers suffering financial losses. To solve this problem, this paper proposes a resource security management mechanism based on dynamic keys and blockchain in a network slicing environment. First, a resource security management architecture based on dynamic keys and blockchain in a network slicing environment is designed. Secondly, the overall mechanism is designed, which includes three steps: service providers obtain the authority to apply for resources, service providers apply for and obtain resources, and the underlying network providers complete the resource cost settlement. Finally, it is verified that the mechanism in this paper improves the security of resources in three aspects: preventing man-in-the-middle attacks, preventing data tampering, and data leakage.

**Acknowledgement.** This work presented in this paper has been supported by the National Key R&D Program of China (Grant No. 2020YFB0906003).

## References

1. Zhang, Y., Liang, L., Zhang, X., Zhang, J., Feng, X.: Resource allocation of wireless networks based on improved heuristic optimization algorithm. *J. Data Acquis. Process.* **37**(6), 1288–1296 (2022)
2. Sun, S., Peng, L.: Network resource correlation-aware virtual network mapping algorithm. *Appl. Res. Comput.* **40**(3), 1–6 (2022)
3. Zhao, H., Li, S., Zuo, P., Wei, Z.: Security resource allocation method for internet of things based on reinforcement learning. *Netinfo Secur.* **22**(6), 44–52 (2022)
4. He, Z., Wang, K., Niu, B., You, W., Tang, H.: 5G network slicing function migration strategy based on security threat prediction. *J. Comput. Appl.* **39**(2), 446–452 (2019)
5. Qi, P., Wang, F., Xu, J., Li, X.: Trust based multi-resource computation offloading strategy in mobile edge computing environment. *Comput. Integr. Manuf. Syst.* **26**(6), 1616–1627 (2020)
6. Ma, B., Chen, X., Xie, X., Zhong, S.: Vertical handover algorithm considering terminal security and resource scheduling. *J. Electron. Inf. Technol.* **44**(8), 2792–2801 (2022)





# A Secure and Efficient Access Control Mechanism for Network Slice Resources in Distributed Environment

Guoyi Zhang<sup>(✉)</sup>, Hailong Zhu, Huihong Luo, Yang Cao, Feifei Hu, and Xubin Lin

Power Control Center of China Southern Power Grid, Guangzhou 510623, China  
guoyizhang2021@163.com

**Abstract.** In order to solve the problem of low security in transactions between multi service providers and multi bottom network providers, this paper proposes a secure and efficient network slice resource access control mechanism in a distributed environment. First, a secure and efficient network slice resource access control architecture in distributed environment is designed. The framework consists of multiple domains. The roles of each domain include multiple service providers, multiple underlying network providers, authentication servers, and resource use license servers. The overall mechanism of secure and efficient network slice resource access control in a distributed environment includes six steps: the service provider applies for identity authentication to the authentication server, the service provider applies for resources to the resource use license server, the resource use license server returns the list of underlying network providers to the service provider, the underlying network provider allocates resources to the service provider, the service provider applies for resources from a resource use license server outside the domain, and the resource use license server outside the domain returns a remote list of underlying network providers to the service provider. Finally, the mechanism in this paper has good performance.

**Keywords:** Network virtualization · Distributed environment · Access control · Data security

## 1 Introduction

In the network slice environment, the traditional physical network is divided into an underlying network and a virtual network. The underlying network is built and operated by underlying work providers [1]. The virtual network is built by service providers leasing the underlying network resources. Service providers deploy professional services on the virtual network. This context allows service providers to quickly build virtual network environments so that they can concentrate on research and development of professional services, providing a richer range of services to end users. As the scope of service providers' services expands, more and more service providers need to rent network resources from multiple underlying network providers [2]. However, with the increase in network frauds, cases of service providers and underlying network providers

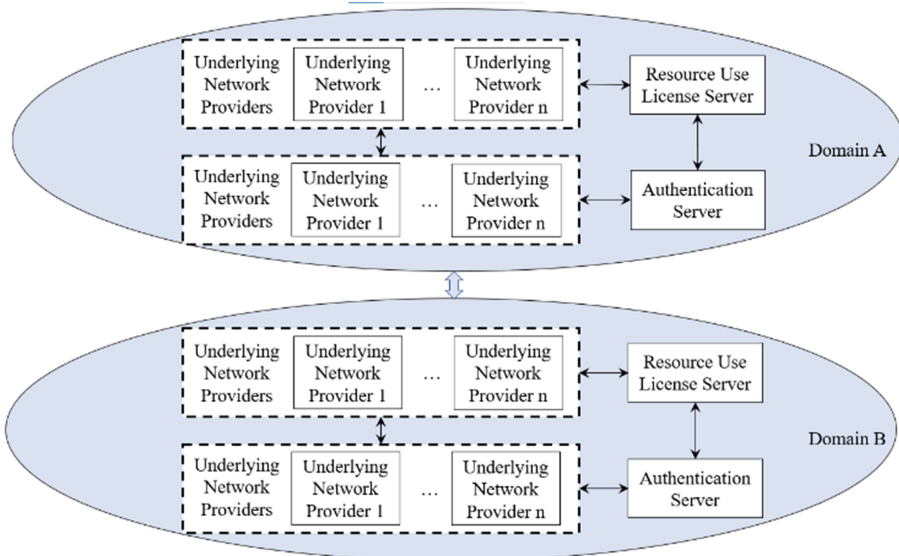
being defrauded have occurred, causing large economic losses to the companies involved. In this context, how to build a secure transaction scenario for multiple service providers and multiple underlying network providers has become an urgent problem to be solved.

To solve the problem of low security when sharing spectrum resources by unmanned aerial vehicles (UAVs), literature [3] proposed a blockchain-based spectrum sharing mechanism. In order to solve the problem of data eavesdropping during UAV communication, literature [4] proposed a secure data offloading strategy for multi-UAV wireless networks based on minimum energy consumption. To solve the problem of resources being attacked by network in heterogeneous cloud computing environment, literature [5] proposed a resource allocation algorithm based on rotation strategy. To solve the problem of low security in the management of virtual network function resources, literature [6] proposed a resource allocation algorithm using secure service chains. The analysis of the existing studies shows that more results have been achieved in the secure communication of data. However, the problem of low security when transacting with multiple service providers and multiple underlying network providers is still an urgent problem to be solved. In order to solve the problem of low security when transacting with multiple service providers and multiple underlying network providers, this paper proposes a secure and efficient access control mechanism for network slice resources in a distributed environment. Through performance analysis, it is verified that the mechanism in this paper has good application value.

## 2 Architecture and Overall Mechanism

A secure and efficient network slice resource access control architecture in a distributed environment consists of multiple domains (see Fig. 1). The roles of each domain include multiple service providers, multiple underlying network providers, authentication servers, and resource use license servers. Among them, the main responsibility of service providers is to apply for network slice resources to construct virtual networks and thus provide services to end users. The main responsibility of the underlying network provider is to build the underlying network resources and use virtualization technology to divide the underlying network resources into network slices, so as to flexibly allocate network resources to service providers. In order to ensure the reliability of the underlying network resources, the energy consumption and reliability of the resources are optimized using optimization strategies on the premise of satisfying the number of service providers' demands for the underlying network resources. The main responsibility of the authentication server is to perform security authentication of the service provider, thus ensuring the authenticity of the service provider's identity. The main responsibility of the resource use license server is to allocate resources for service providers. When allocating resources, it is necessary to first determine whether there are available resources for allocation based on the resource requests from service providers.

In order to achieve secure interaction of data communication, the following key information generation and sharing are required offline or encrypted. First, for key sharing, the service provider shares each other's key information with the authentication server and the authentication server shares each other's key information with the resource use license server. These two key sharing strategies can ensure the security of data transmission in the identity authentication process. Second, for communication key generation,



**Fig. 1.** Secure and efficient network slice resource access control architecture in distributed environment.

communication keys are dynamically generated between the service provider and the resource use license server, and between the service provider and the underlying network provider. These two dynamically generated communication keys can ensure the security of data during resource application and also effectively prevent man-in-the-middle attacks or fraud events.

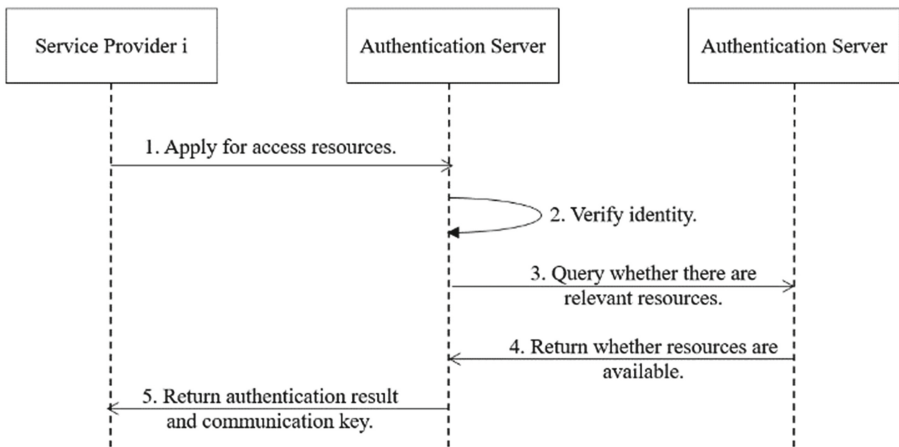
The overall mechanism of secure and efficient network slice resource access control in distributed environment consists of the following six steps. (1) The service provider applies for identity authentication to the authentication server; (2) The service provider applies for resources to the resource use license server; (3) The resource use license server returns a list of underlying network providers for the service provider; (4) The underlying network provider allocates resources to the service provider; (5) The service provider applies for resources from a resource use license server outside the domain; (6) The resource use license server outside the domain returns a “list of remote underlying network providers” to the service provider. The following is a detailed description of each.

### 3 Key Steps

#### 3.1 Service Provider Applies for Identity Authentication to Authentication Server

The main process of the service provider applying for identity authentication to the authentication server (see Fig. 2) is as follows.

- (1) The service provider applies to the authentication server for access resources. Application information includes identity information, type and quantity of resources needed.
- (2) Authentication server verifies identity: The authentication server authenticates the service provider based on the identity information of the service provider.
- (3) The authentication server queries whether there are relevant resources. The authentication server sends the resource requirements to the resource use license server and requests to determine whether the requirements are met.
- (4) The resource use license server returns whether resources are available. The resource use license server queries the known resource information, matches the required resources with the existing resources according to their types and quantities, and calculates whether the requirements are met.
- (5) The authentication server returns the service provider authentication result and the encrypted authentication information. The encrypted authentication information includes the communication key dynamically generated between the service provider and the resource use license server.



**Fig. 2.** Service provider applies for identity authentication to authentication server.

### 3.2 Service Provider Applies for Resources to Resource Use License Server

The service provider's application for resources from the resource use license server mainly includes the following processes.

- (1) The resource license server determines whether the requested resource is an in-domain resource or an out-of-domain resource based on the attribute information of the applied resource. The attribute information of the applied resource includes the location of the resource, the type of the resource and other constraints.
- (2) If the applied resource is an in-domain resource, the fourth step is executed.

- (3) If the applied resource is an out-of-domain resource, first find the resource use license server outside the domain which can provide the resource. Next, interact with the out-of-domain resource use license server to generate a new communication key. Finally, return the address of the out-of-domain resource license server, the communication key of the out-of-domain resource license server and other information to the service provider and execute the fifth step.

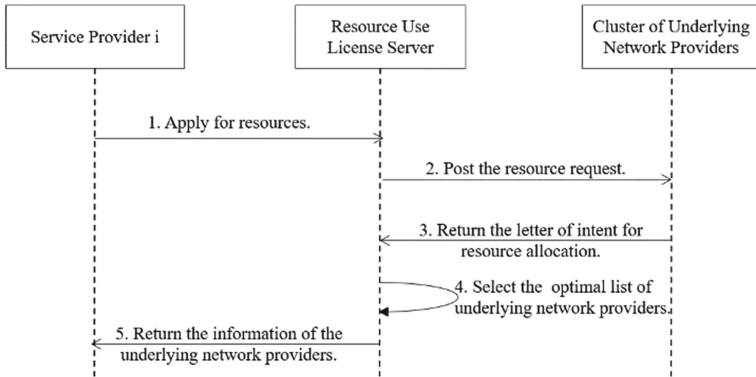
### **3.3 Resource Use License Server Returns a List of Underlying Network Providers for Service Provider**

The Resource Usage License Server returns the list of underlying network providers for the service provider in the following steps (see Fig. 3).

- (1) The service provider applies for resources from the resource use license server. The interaction information includes the type of resources required, the duration of use, and the expected price of service. To ensure data security, the interaction information is encrypted using a communication key.
- (2) Post the resource request. The resource use license server issues resource requests to all underlying network service providers.
- (3) Return the letter of intent for resource allocation. After receiving the resource application, all the underlying network service providers determine whether their resources meet the requirements and set the service price according to the service quality assurance agreement, and then return the letter of intent to allocate resources. The letter of intent includes their own identity information, the service price provided, and the service quality assurance agreement signed.
- (4) Select the optimal list of underlying network providers. The resource use license server uses the underlying network provider selection algorithm to find the list of available underlying service providers. The search criteria mainly include the type, quantity and constraints of resources (e.g., location, reliability, price, service quality commitment, etc.), and generate the information of the underlying network providers. This information is the communication keys of the relevant underlying network providers that satisfy the resource application, and each underlying network provider and service provider. The underlying network provider selection algorithm can use existing research results, and the goal is to obtain the optimal list of underlying network providers.
- (5) Return the information of the underlying network providers. The resource use license server returns the service provider resource allocation information. This information includes the list of the underlying network providers and the communication keys between each underlying network provider and service provider.

### **3.4 Resource Use License Server Returns a List of Underlying Network Providers for Service Provider**

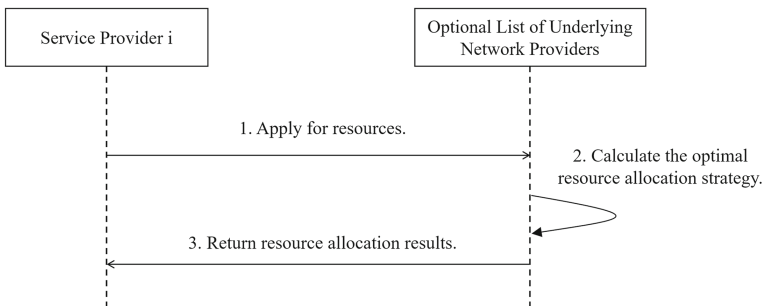
The step of resource allocation for service providers by the underlying network provider starts with the service provider making a resource request to the underlying network



**Fig. 3.** Resource use license server returns a list of underlying network providers for service provider.

provider. The requested resources are optimally scheduled and allocated by the underlying network provider and the algorithm ends. The main process of this step is as follows (see Fig. 4).

- (1) Request for resources. The service provider requests resources from the bottom network provider in the bottom network provider list.
- (2) Calculate the optimal resource allocation policy. The underlying network provider uses an energy consumption and reliability optimization algorithm to allocate resources to the service provider. The energy consumption and reliability optimization algorithm can use existing research results to obtain the optimal resource allocation policy.
- (3) Return resource allocation results. The underlying network provider returns the resources to the service provider.



**Fig. 4.** Underlying network providers allocate resources to service providers.

### **3.5 The Process of Requesting Resources from Servers Outside the Domain by the Service Provider**

When a service provider requests resources from a resource usage license server outside the domain, the service provider communicates using the address and the communication key of the resource usage license server outside the domain returned by the resource usage license server in this domain. First, the service provider finds the location of the out-of-domain resource license server based on its address information. Second, the resource request information is encrypted using the communication key of the out-of-domain resource use license server, and then the resource request is made to the out-of-domain resource use license server.

The out-of-domain resource license server returns a “remote list of underlying network providers” to the service provider in a similar manner to the in-domain resource request process in step 4. After completing this step, the algorithm moves to step 4.

## **4 Performance Analysis**

### **4.1 Security Analysis**

This paper adopts two key mechanisms, key sharing and dynamic communication cipher, which can ensure that the data communication in the three stages of identity authentication, resource application and optimal scheduling can be double encrypted to ensure the security of data.

### **4.2 Efficiency Analysis**

- (1) High efficiency of one authentication. When each service provider applies for resources, only one authentication is needed to complete the authentication and get the secure communication key, which is more efficient.
- (2) High efficiency of resource pre-allocation. In the identity authentication mechanism, the underlying network resources are first verified by the resource usage license server to see if they meet the customer requirements, which can effectively avoid passing the authentication but not meeting the customer requirements, improving the efficiency of resource allocation and enhancing the customer experience of resource allocation service.
- (3) High efficiency of two-level resource allocation policy preference. The combination of external scheduling and internal scheduling improves the efficiency of resource allocation and use. External scheduling is performed by the resource usage license server. The resource usage license server selects the best one from many underlying network providers and provides the best underlying network provider for service providers. Internal scheduling is performed by the underlying network provider. The underlying network provider analyzes the resources under its jurisdiction according to itself, and provides the service provider with the optimal service while effectively reducing the energy consumption of network resources.

### 4.3 Availability Analysis

As the number of service providers and underlying network providers increases, and the scope of services increases, the underlying network resources required by service providers must need to be collaborated and allocated among different domains in order to quickly build virtual networks and thus rapidly deploy services. This paper allows secure access control for both in-domain and out-of-domain scenarios. In addition, this paper unifies the authentication of service providers by local authentication servers, which not only improves the efficiency of authentication, but also ensures the security of resource allocation.

## 5 Conclusion

The number of cases of fraudulent transactions between service providers and underlying network providers is gradually increasing, causing large economic losses to the companies involved. To solve this problem, this paper firstly designs a secure and efficient network slicing resource access control architecture in a distributed environment. Secondly, a secure and efficient network slicing resource access control mechanism in a distributed environment is proposed. Finally, the resource access control mechanism of this paper is analyzed from three aspects of security, efficiency and availability, and it is verified that the mechanism of this paper has better performance.

**Acknowledgement.** This work presented in this paper has been supported by the National Key R&D Program of China (Grant No. 2020YFB0906003).




## References

1. Peng, X., Huang, J.: Research on dynamic allocation of optical network resources based on machine learning technology. *Laser J.* **43**(7), 144–148 (2022)
2. Zheng, Z., Zhou, J.: Game optimization strategy for multi-tenant network resource allocation. *Comput. Eng.* **48**(5), 170–177 (2022)
3. Zhou, P., Zhu, J.: Spectrum sharing mechanism based on blockchain in UAV cooperative communication system. *Telecommun. Eng.* **62**(8), 1029–1036 (2022)
4. Cui, G., Xu, Y., Zhang, S., Wang, W.: Secure data offloading strategy for multi-UAV wireless networks based on minimum energy consumption. *J. Commun.* **42**(5), 51–62 (2021)
5. Ni, S., Hu, H., Liu, W., Liang, H.: Heterogeneous cloud resource allocation algorithm based on rotation strategy. *Comput. Eng.* **47**(6), 44–51+67 (2021)
6. Huang, R., Zhang, H.: Research on algorithm of VNF allocation and scheduling problems in security service chain. *Appl. Res. Comput.* **36**(3), 890–895 (2019)





# Multicast Wireless Resource Optimization for High-Precision Clock Synchronization Timing Service in 5G-TSN

Yue Liu<sup>1</sup>, Jizhao Lu<sup>1</sup>, Yanru Wang<sup>2</sup>, Hui Liu<sup>2</sup>, Yalin Cao<sup>3</sup> , and Lei Feng<sup>3</sup>  

<sup>1</sup> State Grid Henan Electric Power Company Information Communication Company, Henan, China

<sup>2</sup> Beijing Zhongdian Feihua Communications Co, Ltd, Beijing, China

<sup>3</sup> Beijing University of Posts and Telecommunications, Beijing, China

fenglei@bupt.edu.cn

**Abstract.** In the context of utilizing 5G wireless technology for facilitating the timing service of the industrial Internet of Things (IoT), achieving precise clock synchronization while considering the balance between 5G wireless resource utilization and network performance becomes imperative. Firstly, an incomplete observation clock synchronization model is established. Subsequently, the Kalman filter algorithm is employed to determine the boundedness of clock synchronization error, enabling the formulation of an optimization model for 5G wireless resource allocation aimed at ensuring clock synchronization accuracy. Furthermore, a two-step optimization framework is introduced, employing a clustering algorithm and Lyapunov method, combined with multi-agent deep reinforcement learning, to effectively address the proposed problem. Simulation results corroborate the efficacy and superiority of the proposed model and methodology in achieving a joint optimization of clock synchronization accuracy and throughput.

**Keywords:** High-precision clock synchronization · 5G deterministic network · Resource allocation · Lyapunov optimization

## 1 Introduction

With the development of the industrial Internet of Things, some core production control businesses, such as robotic arms and automatic guided vehicle (AGV), not only rely on the ultra-reliable low latency communication (URLLC) capabilities provided by the 5G network but also require precise timing synchronization through the synchronous clock offered by the 5G radio access. This places higher demands on the deterministic communication capabilities of wireless networks. Existing clock synchronization research has made significant contributions to the field. References [1–3] provide quantitative expressions for the covariance of synchronization errors. In reference [4], the problem of clock synchronization accuracy in unreliable networks is modeled as an incomplete observation measurement model. However, it is important to note that the trade-off between ensuring deterministic boundaries for delay and the associated time resource costs of 5G wireless communication radio access is often overlooked.

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2024

Y. Zhang et al. (Eds.): CENet 2023, LNEE 1127, pp. 190–199, 2024.

[https://doi.org/10.1007/978-981-99-9247-8\\_19](https://doi.org/10.1007/978-981-99-9247-8_19)

The 5G-TSN network needs to meet the accuracy requirements of clock synchronization of IIoT devices, while it needs to consume much communication resources to carry out single-link timing service transmission for each user. In view of this problem, the reference [5] uses the 5G network multicast mechanism to group users and transmit service data, so as to achieve flexible allocation and reuse of resources and improve resource utilization. However, it focus on the packet mechanism of data transmission services, which is not applicable to timing service.

In addition, for wireless resource allocation and optimization in multi-user networks, in the current research, reference [6] mainly transforms the problem based on Lyapunov optimization theory, and then decomposes it into multiple sub-problems, which are solved using optimization algorithms or heuristic algorithms; References [7, 8] propose a complete optimization framework based on Lyapunov and deep reinforcement learning algorithm. However, for the multi-user clock synchronization network, the problem is too complex to be solved using the above optimization or heuristic algorithm, which is unacceptable for wireless networks that need to ensure high-precision timing service.

In response to the aforementioned issues, this paper presents a 5G resource allocation optimization technique for achieving high-precision clock synchronization in industrial cellular networks. The proposed technique is based on a deterministic delay evaluation model, which effectively adjusts time slot overhead, allocates base station transmission power, and achieves joint optimization of throughput and clock synchronization accuracy. The main contributions of this study are as follows:

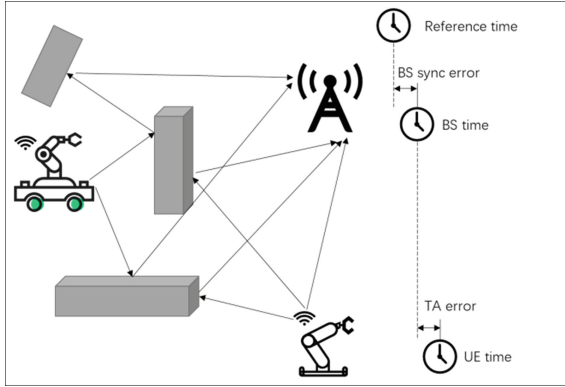
- (1). A two-way exchanging based incomplete clock synchronization model is established. Based on the Kalman filtering algorithm, an estimation method for the error covariance of clock synchronization accuracy in the presence of clock observation variable loss is proposed.
- (2). A joint optimization problem of clock synchronization accuracy and throughput is formulated and analyzed by Lyapunov optimization theory. A deep reinforcement learning algorithm framework based on clustering algorithm and Lyapunov optimization is proposed to effectively solve this problem.

The organizational structure of this paper is as follows: Sect. 2 analyzes the clock synchronization process, and establishes a time-domain configuration optimization model for clock accuracy assurance; Sect. 3 studies the Lyapunov optimization and solution process of the problem model; Sect. 4 is the analysis of simulation results; Finally, Sect. 5 summarizes the full text.

## 2 System Model

### 2.1 Two-Way Exchanging Based Incomplete Observation Clock Synchronization Model

We consider a wireless communication system comprising a 5G base station (BS) and multiple industrially crucial time service terminals with high sensitivity to delays. In this scenario, a clock synchronization system is established based on a two-way information exchanging mechanism between the 5G base station and each individual time service terminal, as illustrated in Fig. 1.



**Fig. 1.** Clock synchronization system of industrial wireless cellular network

For the clock synchronization system of each single link in the network, based on the reference [9], the recurrence equation of the clock state variable of the base station node  $gNB_i$  or terminal node  $UE_i$  can be expressed as:

$$x_i(k) = ax_i(k - 1) + w_i(k) + b \tag{1}$$

where,  $k$  represents the  $k$  th cycle of clock synchronization process,

$$x_i(k) = [\beta_i(k)\vartheta_i(k)]^T \tag{2}$$

$\beta_i(k)$  and  $\vartheta_i(k)$  are respectively instantaneous clock offset and cumulative clock offset of  $gNB_i$ , i.e., frequency offset and phase offset of instant clock synchronization signal; offset coefficient matrix  $A = \begin{bmatrix} 1 & 0 \\ \tau_0 & 1 \end{bmatrix}$ ,  $\tau_0$  represents the sampling period;  $w_i(k)$  represents Gaussian process noise, and the mean value is 0, the covariance matrix  $E[w_i(k)w_i^T(k)] = Q$ ; Constant matrix  $b = [0 - \tau_0]^T$ .

Based on the above definition of clock synchronization state variables, a timestamp observation model based on two-way information exchange mechanism is established [10]. We can get the base station node clock observation model of  $gNB_i$ :

$$y_{i,k} = Cx_i(k) + v_i(k) \tag{3}$$

where  $C$  is the observation matrix and the observation noise  $v_i(k)$  is a Gaussian random variable subject to  $N(0, R)$  distribution.

In the industrial wireless 5G network, the transmission of the link is no longer reliable, and the timestamp packet cannot be guaranteed to arrive. The modified clock observation model is as follows:

$$z_{i,k} = \gamma_k [Cx_i(k) + v_i(k)] \tag{4}$$

where,  $\gamma_k$  is a binary Bernoulli random variable, when  $\gamma_k = 1$ , it indicates that the target node has received the clock synchronization information of the sending node; Otherwise,  $\gamma_k = 0$ .

And the Kalman filter algorithm is used to obtain the steady-state error covariance of the clock synchronization accuracy  $P_k$ :

$$E[P_k] = AXA^T + Q - \lambda AX C^T (CXC^T + R)^{-1} CXA^T \quad (5)$$

where  $X = E[P_{k-1}]$ ,  $\lambda = E[\gamma_k]$ .

## 2.2 Time-Domain Resource Allocation Optimization Problem Model

In order to prevent the clock synchronization error from causing the collision of data packets during the data transmission process, a guard time bound is added to the 5G OFDMA time domain to protect each transmission time slot. According to reference [11], the setting of the length of the system guard time bound  $B_k$  must meet the following constraints:

$$B_k \geq \Delta E_k + Tr(E[P_k]) \quad (6)$$

where  $\Delta E_k$  represents the fixed error in the synchronization process, and  $Tr(E[P_k])$  is the trace of  $E[P_k]$ .

In this paper, the transmission rate calculation method considering the transmission error rate [12] is adopted to obtain the high reliability throughput:

$$U(B_k, p_k) = W_B(B_k) \log_2 [1 + snr_k(p_k) - \sqrt{\frac{V_k}{L}} f_Q^{-1}(1 - \lambda_k)] \quad (7)$$

In addition, this paper proposes to group users in a cell based on the arrival rate of user packets and the wireless channel environment as the dimension of multicast subgroups.

Consider the cellular network of multi-user high-precision clock timing service composed of  $K$  users in the cell, and transmit the timing service based on the multicast mechanism of 5G network. The users are divided into  $M$  multicast subgroups, with the number of users in each group  $\mathbf{u} = \{u_1, u_2, \dots, u_m \dots u_M\}$ , the transmission power allocated by each group  $\mathbf{p} = \{p_1, p_2, \dots, p_m \dots p_M\}$ , and the length of the time guarantee band of each user in the cell  $\mathbf{B} = \{B_1, B_2, \dots, B_m \dots B_M\}$ . The rate of the  $k$  th user in the  $m$  th subgroup in the cell  $R_{m,k}$  can be calculated from (7), then the total throughput of the multicast system  $R_{total}$  is calculated as follows:

$$R_{total} = \sum_{m=1}^M \sum_{k=1}^{u_m} R_{m,k} \quad (8)$$

The average clock synchronization accuracy error covariance of the system  $P_{avg}$  is calculated as follows:

$$P_{avg} = \frac{\sum_{m=1}^M \sum_{k=1}^{u_m} Tr(E[P_{k,t}(p_m)])}{K} \quad (9)$$

where  $P_{k,t}$  is the synchronization error covariance matrix of the  $k$  th terminal at time  $t$ . The fairness of resource allocation among different users in the network is also considered,

so as to meet the user's business needs as much as possible. The index  $sf$  to measure the fairness of the system is calculated as follows:

$$sf = \frac{(\sum_{m=1}^M \vartheta_m)^2}{M \sum_{k=m}^M \vartheta_m^2} \quad (10)$$

where, the value range of  $sf$  is  $[0, 1]$ .

Based on the above analysis of deterministic networks considering clock synchronization accuracy, it is necessary to balance the cost of wireless resources under the condition of ensuring clock synchronization accuracy constraints, while maximizing network throughput and taking into account system fairness. This problem P1 can be expressed as follows:

$$P1 \quad \max_{\mathbf{B}, \mathbf{p}} \{R_{total}(\mathbf{B}, \mathbf{p}) + c_0 * sf\} \quad (11)$$

$$s.t. C1 : \sum_{k=1}^K \lim_{t \rightarrow \infty} \frac{E[P_{k,t}]}{t} = 0$$

$$C2 : T_S \geq B_m \geq P_{avg,m} + \Delta E, \forall B_m \in \mathbf{B}$$

$$C3 : 0 < p_{min} \leq p_m \leq p_{max}, \forall p_m \in \mathbf{p}$$

$$C4 : \sum_{m=1}^M p_m = p_{sum}$$

$$C5 : \sum_{m=1}^M u_m = K$$

where, constraint  $C1$  indicates that the sequence of error covariance tends to be stable under long-term observation, that is, to ensure the accuracy of clock synchronization; The constraint  $C2$  limits the length of the user time band in the subgroup to be not less than the critical value of data collision and not more than the length of the time slot; Constraint  $C3$  limits the transmit power allocated by the base station to each subgroup to  $[p_{min}, p_{max}]$ . Constraints  $C4$  and  $C5$  are the total power of the base station and the total number of users.

### 3 Problem Solving

This section proposes a two-step optimization framework to solve problem P1. First, users are divided into multicast subgroups based on K-means++ clustering algorithm; Then, Lyapunov optimization method is used to transform the problem, and the solution algorithm based on multi-agent deep reinforcement learning is used to analyze and solve the problem.

### 3.1 K-Means++—Based Multicast Grouping Mechanism and Lyapunov-Based Problem Transformation

In order to ensure that the users in each multicast group can meet the deterministic service requirements at the same time, this paper uses the grouping mechanism based on the deterministic delay of user to delimit the groups. Specifically, since the user's delay certainty is mainly affected by the arrival of packets and the randomness of the wireless environment, based on the packet arrival rate of each user  $\lambda_{a,k}$  and channel gain-to-noise ratio  $h_k$  two dimensions, the k-means++ clustering algorithm is used to cluster users, divide users into  $M$  multicast subgroups, and adaptively select the number of clusters based on the Calinski-Harabaz index. The value of  $M$  is set to the number of clusters when the Calinski-Harabaz index reaches the maximum value. Compared with the subgroup division strategy based only on distance or SNR, the grouping mechanism considering user delay determinacy in this paper can better meet the needs of users with different delay determinacy between subgroups.

Then, based on Lyapunov optimization theory, problem P1 is transformed into a joint optimization problem of clock synchronization accuracy error covariance and throughput, as follows:

$$P2 \min_{\mathbf{B}, \mathbf{p}} \{V_1 * P_{avg,t}(\mathbf{p})E[a_{k,t}] - V_2 * [R_{total}(\mathbf{B}, \mathbf{p}) - c_0 * sf]\} \quad (12)$$

*s.t.* C2, C3, C4, C5

where,  $V_1$  and  $V_2$  are the control coefficients. By adjusting the relative size of the two coefficients, the influence of objective function and penalty function on the overall optimization result can be flexibly controlled.  $c_0$  is a constant of proportionality.

### 3.2 Solving Algorithm Based on Multi-agent Deep Reinforcement Learning

This section further transforms and solves problem P2 based on the multi-agent deep reinforcement learning algorithm. Considering the complexity of the problem, this paper adopts MATD3 (multi-agent Twin Delayed Deep Deterministic policy gradient) algorithm to solve the problem, MATD3 algorithm is the multi-agent version of the TD3 [15] algorithm. The basic components of the model are defined as follows:

**Observation:** Each agent's observation variable is  $O_m = \{P_{avg,m}, R_m, B_m, p_m, \lambda_{avg,m}\}$ ,  $\mathbf{O} = \{O_m, \mathbf{m} \in \mathbf{M}\}$ . It reflects the set of variables affecting the value function in the environment observed by each agent under the current number of iteration steps.

**Action:** The action set  $A_m = \{p_m, B_m\}$ ,  $\mathbf{A} = \{A_m, \mathbf{m} \in \mathbf{M}\}$  of each agent is a two-dimensional continuous action space, which determines the base station transmitting power and guard time bound length allocated to each subgroup respectively.

**Reward:** Reward function  $r = c_1 * \{lya_{pre} - lya_{cur}\}$ , where  $lya_{pre}$  and  $lya_{cur}$  is the value of the objective function of P2 in each iteration before and after the update of the algorithm respectively. It embodies the reduce the value of the objective function of algorithm in the iteration. When the algorithm obtains the optimal solution, the value tends to be stable, and the system converges to the best state. Because of the cooperative relationship between multiple agents, all agents share the same reward value.

## 4 Numerical Results and Performance Analysis

### 4.1 Simulation Parameter Setting

This section verifies and compares the actual effect of the proposed strategy and algorithm through experimental simulation. The settings of main parameters in the experiment are shown in Table 1, where  $I_2$  represents the second-order identity matrix.

Specifically, the user grouping strategy of the clustering algorithm is verified by experiment firstly; then the optimization method proposed will be compared with DDPG (deep deterministic policy gradient) and DQN (Deep Q-Network) algorithm, validation the final result of optimization indexes of the algorithm under different parameter settings, and the average value of each algorithm running 10 times is taken as the final comparison result.

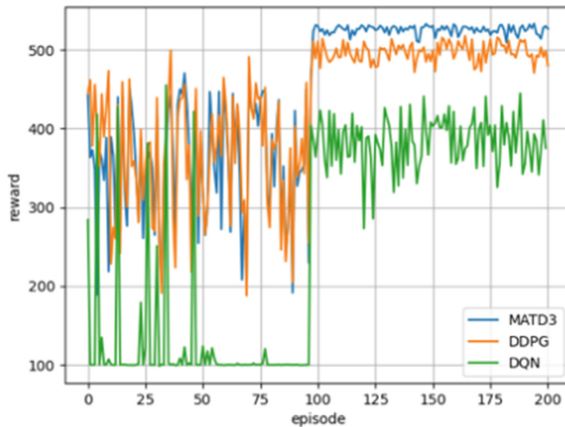
**Table 1.** Simulation parameter setting.

Variable	Simulation parameter	Value	Varibale	Simulation parameter	Value
$W$ (MHz)	System bandwidth	20	$\Delta E_k$ (ms)	Clock synchronization fixed error	$10^{-5}$
$\sigma$	Rayleigh distribution parameter	$1/\sqrt{2}$	$V1$	Lyapunov control parameter	$10^{10}$
$\alpha$	Delay upper bound scaling factor	1/3	$V2$	Lyapunov control parameter	$10^{-7}$
$d$	Path loss factor	3	$b_k$	The exit process of the virtual queue $P_k$	0.01
$\tau_0$	Sampling period	0.1	$p_{max}$ (dBm)	Transmit power maximum constraint	50
$R$	Random time delay covariance	0.1	$p_{min}$ (dBm)	Transmit power minimum constraint	10
$Q$	Process noise covariance	$2.7 \times 10^{-15} I_2$	$V_k$	Channel dispersion	1
$C$	Observation coefficient	[02]	$M_{max}$	Maximum number of user groups	10

### 4.2 Analysis of Simulation Results

Figure 2 shows the average reward function curve of the training and execution process of the three kinds of algorithms in the 10-round iteration. Among them, since the DQN algorithm can only receive discrete actions, the action design of the algorithm is

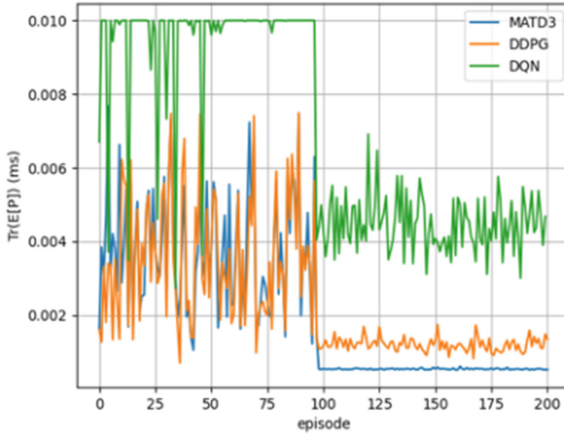
respectively the increase, decrease and constant value of each multicast subgroup of the base station transmission power and the configured guard time bound length, which is a  $6M$  action space. In this figure, the first 100 episodes are the training curve, and the last 100 episodes fix the network parameters and make action decisions based on themselves. The results show that the reward value of the three kinds of algorithms gradually increases with the training episode, and the MATD3 algorithm has obtained a higher reward value than the other two kinds of algorithms. This is because the continuous action space brings more accurate solution space and the agreement of multi-agents to game problem contained in the problem. In the execution stage of the algorithm, both MATD3 and DDPG can reach a stable and high value, while DQN fluctuates greatly, and MATD3 has the highest value. In addition, since each agent in MATD3 does not require global state variables during algorithm execution, that is, there is no need for mutual communication between multiple agents after training, which is advantageous for deployment in actual scenarios.



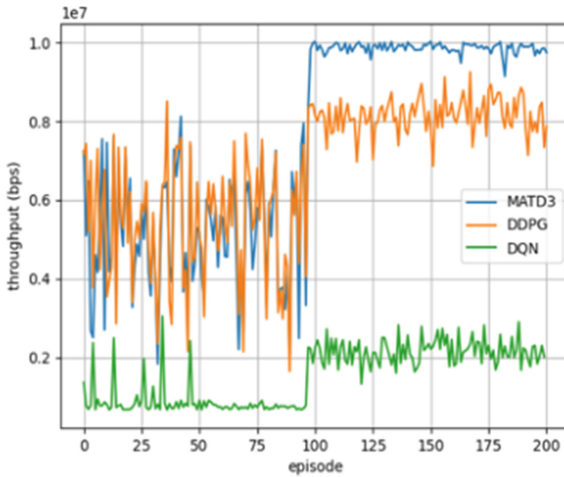
**Fig. 2.** Rewards versus episodes in training and execution process

Figures 3 and 4 respectively show the changing curves of system clock synchronization accuracy and network throughput during algorithm training and execution in Fig. 2. Where, the trace of average clock synchronization precision error covariance and average throughput of each user in the system are taken as comparison indexes respectively. It can be seen from the figure that MATD3 algorithm reaches the optimal effect of the two indexes compared with other comparison algorithms.





**Fig. 3.**  $Tr(E[P])$  versus episodes in training and execution process



**Fig. 4.** Throughput versus episodes in training and execution process

## 5 Conclusion

This study addresses the optimization of 5G network resource allocation for achieving high precision clock synchronization for industrial cellular networks. Initially, an incomplete observation clock synchronization model based on two-way information exchange mechanism is proposed considering the unreliability characteristics of wireless networks. Furthermore, an estimation method utilizing the Kalman filter algorithm is introduced to assess the accuracy of clock synchronization. To tackle the challenge at hand, a joint optimization problem model focusing on ensuring timing accuracy is formulated, and a solution is obtained through the implementation of a clustering algorithm, Lyapunov theory, and the two-step optimization framework of the MATD3 algorithm. Simulation

results evident that the proposed strategy model and optimization algorithm have certain advantages over the existing models and algorithms in the joint optimization of clock synchronization accuracy and throughput.


**Acknowledgement.** This work presented in this paper has been supported by the Research and Application of Multi-mode Merging Positioning and Synchronous Timing Technology in Power Safety Production Business (5700-202224207A-1-1-ZN).

## References

1. Sun, Y., Zeng, L., Wu, X., Lu, Y., Sun, Y.: Synchronization algorithm based on clock skew estimation for WSN. *J. Commun.* **36**(9), 26–33 (2015)
2. Jin, Y., Deng, W., Fang, C.: Distributed synchronization in large-scale wireless sensor networks using group consensus protocol. *Electron. Meas. Technol.* **39**(7), 160–164 (2016)
3. Huang, Y., Chen, Z., Li, D., Tang, C.: Second-order consensus time synchronization for wireless sensor networks. *J. Electron. Inf. Technol.* **39**(1), 51–57 (2017)
4. Wang, T., Guo, D., Cai, C., Tang, X., Wang, H.: Clock synchronization in wireless sensor networks: analysis and design of error precision based on lossy networked control perspective. *Math. Probl. Eng. Probl. Eng.* **2015**(2), 1–17 (2015)
5. Zhang, W., Ni, J., Liu, X., Mao, S., Xiao, H.: Research on grouping strategy and resource allocation algorithm for multicast transmission in 5G communication. *Comput. Appl. Softw.* **38**(12), 128–134 (2021)
6. Zeng, J., Li, L., Xin, N., Li, J., Zhang, L.: QoE-Aware fair resource allocation strategy for integrated satellite and terrestrial networks. *J. Data Acquis. Process.* **36**(2), 222–231 (2021)
7. Bi, S., Huang, L., Wang, H., Zhang, Y.: Lyapunov-guided deep reinforcement learning for stable online computation offloading in mobile-edge computing networks. *IEEE Trans. Wireless Commun.* **20**(11), 7519–7537 (2021)
8. Xu, S., Xing, Y., Guo, S., Yang, C., Qiu, X., Meng, L.: Deep reinforcement learning based task allocation mechanism for intelligent inspection in energy Internet. *J. Commun.* **42**(5), 191–204 (2021)
9. Luo, B., Wu, Y.: Distributed clock parameters tracking in wireless sensor network. *IEEE Trans. Wirel. Commun.* **12**(12), 6464–6475 (2013)
10. Wang, T., Duan, S., Huang, Q., Tang, X., Li, Y.: Reliability analysis of time precision boundary for tight slots of TDMA in deterministic scheduling of industrial internet of things. *Chin. J. Sci. Instrum.* **39**(06), 120–131 (2018)
11. Nasir, A.: Min-max decoding-error probability-based resource allocation for a URLLC system. *IEEE Commun. Lett.* **24**(12), 2864–2867 (2020)
12. Fujimoto, S., Hoof, H. and Meger, D.: Addressing function approximation error in actor-critic methods. In: *Proceedings of the 35th International Conference on Machine Learning*, pp. 1587–1596, Stockholm, SWEDEN, (2018)



# Accurate Close Contact Identification: A Solution Based on P-RAN, Fog Computing and Blockchain

Meiling Dai<sup>1</sup>(✉) , Yutong Wang<sup>1</sup>, Zheng Zhang<sup>1</sup>, Xiaohou Shi<sup>1</sup>, and Shaojie Yang<sup>2</sup>

<sup>1</sup> China Telecom Research Institute, Beijing, China  
daiml1@chinatelecom.cn

<sup>2</sup> Beijing University of Posts and Telecommunications, Beijing, China

**Abstract.** The COVID-19 epidemic is rampant, affecting the normal life of people all over the world. It also has a sustained impact on the global economy, bringing global crises and challenges. In order to effectively prevent and control the epidemic situation and curb the further spread of COVID-19, the identification of close contacts has become a current research hotspot. The low accuracy, insufficient user privacy protection ability, and limited effectiveness have become important issues to be solved. In this paper, we propose a solution based on P-RAN, fog computing and blockchain to support accurate, safe and effective COVID-19 close contact identification. A three-layer accurate close contact identification architecture (ACCCD) is established by combining P-RAN, fog computing and blockchain. P-RAN and fog computing are combined to collect close contact information, and blockchain technology enables reliable, safe and automatic close contact information management and close contact track tracking. Based on ACCCD architecture, the blockchain network deployment scheme and accurate close contact identification process are designed, and the implementation potential and future challenges of this solution are analyzed and explained in detail. The application of ACCCD architecture in specific scenarios is described, and we design simulations to verify the effectiveness of the solution.

**Keywords:** Close contact · Fog computing · Blockchain · Proximity radio access network

## 1 Introduction

Since the COVID-19 broke out at the end of 2019, more than 520 million people have been diagnosed with COVID-19 infection worldwide [1]. It has become the most widespread global pandemic in the past hundred years, which not only disrupted the normal life of people in all countries, but also had a sustained impact on the global economy, bringing serious crises and challenges to the world. Fighting against the epidemic has become the most urgent problem. As an infectious virus, COVID-19 is mainly transmitted through human to human contact and respiratory droplets [2]. In a small space, the transmission and infection rate of COVID-19 is closely related to the distance, time, behavior and other factors between people. When sneezing or coughing, or

even when talking quietly, a large number of droplets wrapped in the coronavirus contact the mucous membrane of other people, the epidemic will spread. Facing the strong infectivity of COVID-19, quickly and effectively cutting off the transmission path of the virus has become the main solution to curb the further spread of the virus. The key point of the implementation of this method is to accurately identify, track and manage the close contacts of the confirmed patients, so as to prevent the further spread of the virus.

At present, researchers have proposed a variety of solutions for automatic tracking of close contacts based on location data using base station [3], GPS [4], Bluetooth [5], etc., which have been applied in many countries. For example, the Chinese government forecasts and monitors the overall trend of the epidemic situation by obtaining anonymous mobile phone base station data from telecom operators, and monitors users' visits to public places to achieve the determination of "time and space contact" type close contacts. However, this solution for the determination of close contact is limited in the accuracy, and requires more time to query the whereabouts of the diagnosed patients, which is inefficient; The Korean and Israeli governments use GPS technology to obtain the mobile phone location data of diagnosed people to track their whereabouts. This kind of big data can better identify close contacts, but it is easy to be rejected by users because it violates users' privacy; The Singapore government has launched the "Trace Together" APP, which uses Bluetooth technology to bind mobile phone numbers to record who users have contacted in the past 21 days. Compared with the tracking method based on GPS and base station, the tracking method based on Bluetooth can search surrounding devices more accurately. However, the method relies on users to open the Bluetooth search service, and its effectiveness depends on the number of people who independently install and use the application.

In order to solve the problems such as low accuracy, insufficient user privacy protection ability, and limited effectiveness of current close contacts tracking, this paper proposes an accurate COVID-19 close contact identification (ACCCD) solution that relies on the operator's P-RAN [6] and combines blockchain [7] and fog computing [8] technology.

P-RAN is a proximity access solution used to enhance the communication capability of the telecommunication access network side. Supported by D2D [9] communication technology, it can enhance the signal coverage capability of the base station side by encouraging idle mobile phones to become P-ran relays. With the combination of P-RAN and fog computing, p-ran relay actively undertakes the responsibility of collecting, caching and recording the information of close contact. It automatically realizes the close contact recognition of mobile terminal users within the range of several meters, effectively providing the accuracy and effectiveness of the close contact identification. Blockchain, as a special distributed ledger technology widely concerned, has the characteristics of anonymity, non-tampering, traceability, etc. With the support of blockchain, users, telecom operators and regulatory authorities jointly manage the encrypted close contact data in a distributed manner to provide user privacy protection. It can achieve safe and reliable distributed encrypted information storage by combining multiple cryptographic mechanisms. In addition, blockchain smart contract technology can support programmable data access control, further ensuring the security of user data.

The main contributions of this paper are as follows:

- Propose an ACCCD architecture. P-RAN and fog computing are combined to collect close contact data, and blockchain technology enables reliable, safe and automatic close contact data management and close contact track tracking;
- Design and implement an ACCCD management platform, complete the construction of the blockchain network, and specify the process of close contact identification;
- Analyze the potential and challenges of the proposed solution in terms of security, feasibility and effectiveness;

The following contents of this paper are organized as follows: We introduced the ACCCD architecture; Design a ACCCD management platform based on consortium blockchain; Combed out the process of the reliable ACCCD; The potential and challenges of the proposed solution are analyzed theoretically; The use cases are displayed and the simulations are carried out; The full text is summarized.

## 2 The Architecture of Accurate Close Contact Identification

Figure 1 illustrates the proposed architecture of the close contacts identification based on P-RAN and blockchain, which describes the P-RAN network architecture, blockchain-based flow modulation information management, and the adaptation scenario from the bottom up.

**P-RAN Layer:** The basic network architecture of the P-RAN network is composed of near-area network, cellular network, and ground-to-air link. Two roles of P-RAN relay and P-RAN user are set in the network architecture. P-RAN users refer to enter the site and join the site P-RAN near domain network users, the hands with D2D ability of smart phones, tablet computers and other smart devices as the most edge of the P-RAN network, through the proximity links (PL) to share the user's location, stay time and other travel track information to the relay. Relay is the core role of P-RAN network architecture, which is composed of one or more high-performance smart terminals and gateways set by the site manager. P-RAN relay collects down the visit information of P-RAN users within the coverage of the service, completes the information encryption calculation with the help of the sinking computing resources of fog computing, and connects up with 5G/6G cellular base stations and satellites through the cellular link (CL) or the Non-Terrestrial link (NTL) to initiate the block chain transaction request. Accurate travel analysis of a P-RAN user is achieved by using the on-line and off-line status within the coverage of a P-RAN relay. The coverage of close contact research and judgment is reduced and the accuracy of judgment is improved.

**Blockchain layer:** This layer can be regarded as an information security storage layer running on top of the P-RAN layer, where the conventional blockchain consensus node stores the location information, access time, departure time, and health identification of P-RAN users. The Operation service node is usually handled by the network operator. It is mainly responsible for the access authentication of P-RAN users and relays, and the release of the investigation conclusion of close contacts. The most critical feature of this layer is to ensure the privacy and trust of the travel information of P-RAN users through the consensus mechanism, and realize the rapid synchronization of the epidemic

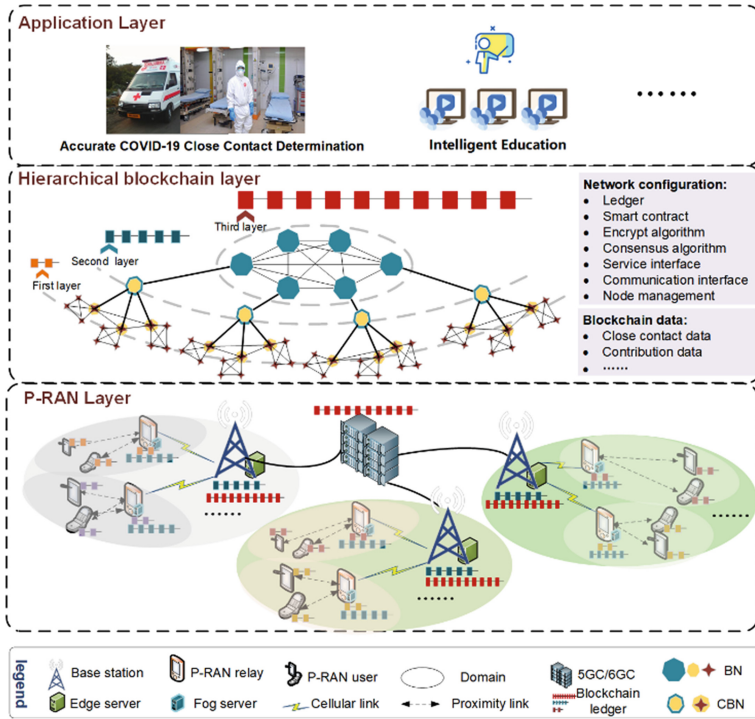


Fig. 1. Overview of ACCCD architecture.

dynamics across the whole region, so as to make the close contact research and judgment more scientific and efficient.

**Adaptation scenario:** The proposed solution can be used to determine COVID-19 close contacts in medical centers, community service stations, supermarkets, transportation hubs and other scenarios. The above scenarios usually have the characteristics of large area, high population density, large flow of people, and important social functions. At the same time, they can meet a certain degree of cellular or satellite network service coverage. In this scenario, mobile terminal move with users and identify each other to support accurate collection of close contacts' information.

The collaborative form of blockchain and P-RAN as well as the design of close contacts identification workflow will be described in detail later.

### 3 Management Platform of Accurate Close Contact Identification

#### 3.1 Network Deployment

As shown in Fig. 2, the network deployment scheme for close contact identification management is proposed. The P-RAN users, relay nodes, operator nodes and regulator nodes involved in the scheme proposed in this paper will be set as the following types of blockchain node roles while completing relevant functions.

**User node:** blockchain light node. The smart phone terminals can register unique digital identities in the blockchain network and obtain the randomly generated keys. The user node uses the network services shared by the relay node through the P-RAN network and pays relevant fees through blockchain tokens. This type of node does not participate in the transaction authentication and consensus mechanism of the blockchain network, nor does it save the ledger information of the entire blockchain. User node only synchronizes its related blockchain information with the relay node through heartbeat, such as location information, health identification, connection duration, etc.

**Relay node:** blockchain light node. The relay node can be an IoT terminal or smart phone terminal registered in the blockchain network. This node can share idle network resources for user nodes to obtain blockchain tokens as rewards. This type of node does not participate in the transaction authentication and block consensus of the blockchain network, nor does it save the ledger information of the entire blockchain. This node will summarize the information of each connected user node through the heartbeat, and report the user node information to the service node through the blockchain network.

**Operator node:** blockchain consensus node. This type of node is the core node of the blockchain consensus network, which synchronizes the entire blockchain ledger information, and it is mainly responsible for the generation and broadcasting of blocks, transaction verification and confirmation, and the execution of smart contracts.

**Service node:** blockchain full node. The service node is composed of National Regulatory Authority, National Health Commission, Disease Control Centers, National Healthcare Security Administration and other relevant epidemic prevention and control departments, providing encrypted communication, data caching, service billing, bandwidth control and routing services. This type of node monitors the health status of each user in real time according to the information reported by the relay nodes, gives a health warning prompt, and executes the point settlement between the user node and the relay node at the same time, and the relevant information will be published on the blockchain. As a full node, it will synchronize the entire blockchain ledger information, and sign and broadcast the transactions.

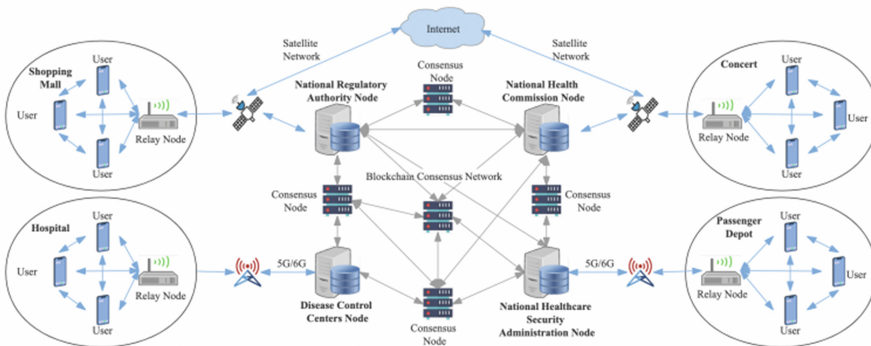


Fig. 2. Network deployment of the management platform.

### 3.2 Procedure of Close Contact Identification

Taking full advantage of blockchain, P-RAN and fog computing technology, we divide the main process of ACCCD into four parts: access authentication, location awareness, user-user close contact identification, and judgement of close contact. The detailed process is shown in Fig. 3. This process mainly involves P-RAN user, P-RAN relay, operator, blockchain and regulator authority. P-RAN user will actively participate in the access authentication, user-user close contact identification process, and passively participate in the location awareness and judgement of close contact processes; P-RAN relay mainly participates in the access authentication and location awareness processes, and passively participates in the user-user close contact identification and judgement of close contact. Processes; The operator passively participates in the access authentication and judgement of close contact processes and does not initiate active participation; The blockchain passively participates in all processes based on the unique smart contract technology, mainly providing the ability to record user and relay authentication information (public key, etc.), relay identity authentication and close contact information, and query the close contact list; The regulator only actively participates in the process of judgement of close contact, and does not involve other three processes.

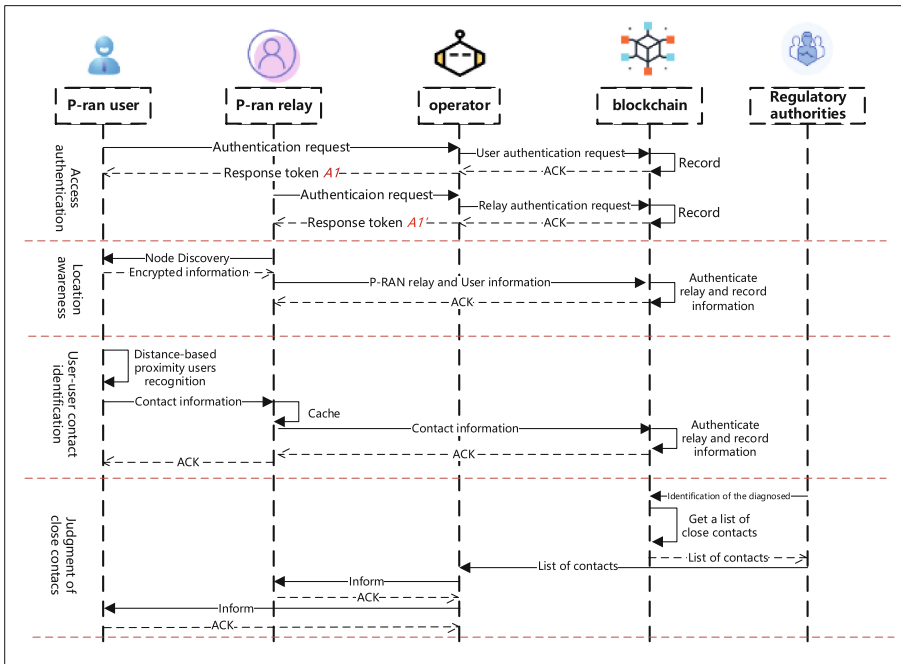


Fig. 3. Process of close contact identification.

**Access authentication:** The design of access authentication mainly includes two steps: operator access authentication and block link access authentication. Before officially launching the "authentication request" to obtain the communication service, in



addition to the existing identity - SIM card, the mobile terminal user needs to use the asymmetric encryption algorithm to generate a pair of public and private keys, store the private key securely locally and package the public key as a "blockchain identity" into the "authentication request". Therefore, the "authentication request" packets of P-ran user and P-ran relay both include SIM card identity authentication information and "blockchain identity", and the service startup instruction can be added to the relay authentication request. After the operator receives the "authentication request" and completes the authentication of the user and relay, it forwards the "request" to the blockchain by category to trigger the smart contract to continue to verify the authenticity of the "blockchain identity" declared by the mobile terminal user. After receiving the request, the blockchain checks the identity information recorded in the "ledger" by means of cryptographic methods (such as multi-party computing) corresponding to the different identities of the user and relay. For the identity information of the user who has been verified, the blockchain smart contract uses the public key of the regulator to encrypt and complete the uplink record, and simultaneously responds to the operator with confirmation characters. After receiving the blockchain response, the operator starts the corresponding relay service management, and simultaneously returns the P-RAN service certificate to support mutual authentication between user and relay.

**Location awareness:** Any P-RAN relay that passes identity authentication will be given the user location awareness capability. P-RAN relay that completes the access authentication will periodically send node discovery signals within its small-scale coverage. After receiving the signal, the user entering the coverage area of P-RAN relay signal returns a token based on the source address marking of the received signal. After relay completes the user authentication, it sends the user visit information to the blockchain and record it. To ensure the reliability of the user's visit information record, relay will use the private key to sign the user's visit information, and the triggered visit information smart contract will complete the verification by calling the relay public key information.

**User-user close contact identification:** Under the condition of optimizing the energy consumption of the equipment, set the P-ran user to have the ability of small range D2D communication. When the user reaches a certain relay coverage area and the dwell time exceeds  $T$ , the distance based adjacent user identification function is enabled. If other user B enters the signal coverage range  $m$  of current user A and stays for a period of time, user A will record that user B is encrypted and send encrypted contact information (including B's public key information, time point, time length, shortest distance, etc.) to the adjacent P-RAN relay, which caches such information and periodically generates blockchain transaction completion information for storage on the blockchain.

**Judgement of close contact:** Supported by the contact information recorded by the blockchain, the regulatory authority sends the identity of confirmed cases to the blockchain through the whole node of the blockchain for operation and maintenance, and triggers the secret connection determination smart contract to obtain the list of secret connection personnel. In this process, the authority management module in the blockchain smart contract will set that the regulator can only obtain the cryptographic information in the corresponding management physical area, and relay encrypts such information with the public key of the regulator before uploading it. Only the regulatory

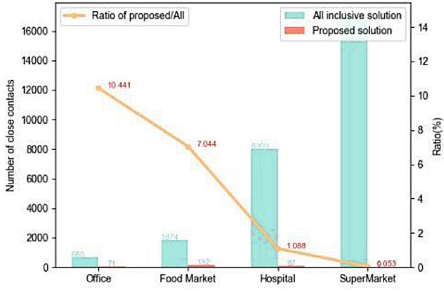
authority with corresponding management authority can obtain a complete list of plain-text public keys of mobile terminal users. After obtaining the list of encrypted public keys, the regulatory authority will send the list to the operator, identify the real identity of the corresponding P-RAN user/relay through the operator, and promptly notify the corresponding mobile terminal user, so as to achieve accurate targeting while effectively protecting the user's identity privacy.

## 4 Simulations

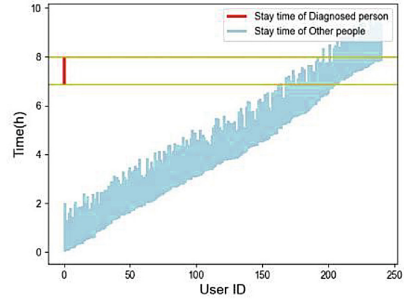
Use Python to carry out specific scene simulation according to the parameters in Table 1. Based on the three different arrival methods and collective visit locations of users, detailed partition visit is simulated: in office building scenario, users stay in offices (25 partitions), meeting rooms (10 people), activity rooms (3 partitions such as reading rooms and gyms), canteens (1 partition) and other places; In vegetable market scenario, there are 82 stalls of 13 categories of goods (36,5,3,4,10,6,2,2,3,4,2,4,1) for users to choose from. The number of stalls for each user is within [2,13], and the duration of each stall is [6–15 min]; In hospital scenario, there are 26 (3, 4, 7, 6, 6) diagnostic areas on 5 floors, and the user's stay time in a single diagnostic area is [5–60 min]; In supermarket scenario, the total area of the supermarket is 24000 square meters, there are 2000 commodity zones, the number of zones visited by users is [5, 20], and the overall stay time of customers is [0.5–3 h].

Randomize the visit of users, and get the number of close contacts as shown in Fig. 4a. With the support of the solution proposed in this paper, it can more accurately determine the people who have contact with the diagnosed patients at the same time and in the same small-scale space. With the continuous expansion of the site and the increasing randomness of personnel flow, the proportion of people who have close contact with all visitors decreases. The experimental results show that in general, the probability of direct contact between users is negatively related to the size of the site. The larger the size of the site visited, the smaller the probability of direct contact between two users. Compared with the All-inclusive solution, which determines that all users who visit a place on the same day are encrypted, the solution proposed in this paper can support the regulatory authority to narrow the scope of encrypted connection determination and more accurately locate the group of encrypted users.

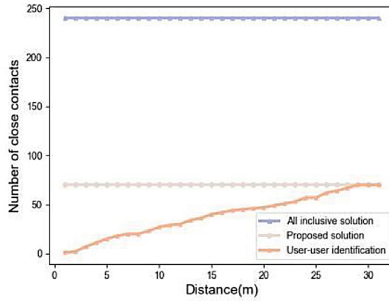
The arrival time, departure time and stay time of confirmed cases and other users are shown in Fig. 4b. The interval distance of users in the zone is set within [0.5, 30 m], and users are set to walk randomly and record the shortest contact distance between users. Based on the analysis of the shortest contact distance and contact time with the confirmed case, the schematic diagram of the number of close contacts changing with the contact distance setting is obtained as shown in Fig. 4c. Combined with the arrival situation as shown in Fig. 4b, with the increasing distance, the patients judged to be close contact will be closer to the total number of people in the room. The identification of people at different distances can help disease control departments implement targeted individual user management and control, and greatly improve the accuracy of epidemic prevention and control.



(a) Comparison in four scenarios



(b) Arrival and departure time



(c) User-user contact identification

Fig. 4. Analysis of close contact identification in different scenarios

### 5 Conclusion

The outbreak of COVID-19 has brought severe challenges to human social life. In the face of the highly infectious COVID-19, the main means of prevention and control of the COVID-19 epidemic is to accurately identify and control close contacts. Faced with the needs of close contacts, this paper proposes ACCCD solution integrating P-RAN, fog computing and blockchain technology. The blockchain is used to provide distributed storage of users' encrypted data; P-RAN and fog computing are used to complete close proximity user identification, user-user close identification, etc., so as to improve the accuracy of secret connection determination. The simulation results show that the proposed solution can achieve accurate close contact person positioning in various scenarios, indirectly reduce social and economic losses, improve people's sense of well-being, and greatly meet the needs of accurate prevention and control under the current severe and complex epidemic situation.

### References

1. Zhang, S., Ventura, M. and Yang, H.: Network modeling and analysis of COVID-19 testing strategies. In: 2021 43rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), Mexico, 2021, pp. 2003–2006 (2021)

2. Tahir, H., Iftikhar, A. and Mumraiz, M.: Forecasting COVID-19 via registration slips of patients using ResNet-101 and performance analysis and comparison of prediction for COVID-19 using faster R-CNN, mask R-CNN, and ResNet-50. In: 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 2021, pp. 1–6 (2021)
3. Naveed, M., Qazi, S. and Khawaja, B.: UAV-based life-saving solution for police to maintain social-distancing during Covid-19 pandemic using 4G-LTE technology. In: 2021 International Conference on Communication Technologies (ComTech), Rawalpindi, Pakistan, 2021, pp. 28–32 (2021)
4. Fors, K., Alexandersson, M., Stenumgaard, P.: The Impact from Covid-19 pandemic lockdown on the electromagnetic interference in the GPS frequency band. In: 2022 International Symposium on Electromagnetic Compatibility–EMC Europe, Gothenburg, Sweden, 2022, pp. 36–41 (2022)
5. Kumar, S., Gautam, V., Kumar, A., Kumari, P.: Social distancing using bluetooth low energy to prevent the spread of COVID-19. In: 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2021, pp. 563–567 (2021)
6. Bi, Q.: P-RAN: a distributed solution for cellular systems in high frequency bands. *IEEE Netw.* **36**(4), 86–91 (2022)
7. Shen P.: A survey on safety regulation technology of blockchain application and blockchain ecology. In: 2022 IEEE International Conference on Blockchain (Blockchain), Espoo, Finland, 2022, pp. 494–499 (2022)
8. Rabay'a, A., Schleicher, E., Graffi, K.: Fog Computing with P2P: enhancing fog computing bandwidth for IoT scenarios. In: 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 2019, pp. 82–89 (2019)
9. Lv, Y., Jia, X., Niu, C., Wan, N.: D2D network coverage analysis based on cluster user equipment classification and spectrum sharing allocation. In: 2020 IEEE 6th International Conference on Computer and Communications (ICCC), Chengdu, China, 2020, pp. 529–534 (2020)



# Trusted Reputation System for Heterogeneous Network Resource Sharing Based on Blockchain in IoT

Jingwen Li<sup>1</sup>, Meiling Dai<sup>1</sup> (✉) , Yi Lu<sup>1</sup>, and Shaojie Yang<sup>2</sup>

<sup>1</sup> China Telecom Research Institute, Beijing, China  
daiml1@chinatelecom.cn

<sup>2</sup> Beijing University of Posts and Telecommunications, Beijing, China

**Abstract.** With evolution of 5G networks and IoT technology, enormous amount of network resource demands are raising. How to effectively promote the interconnection and comprehensive sharing of resources which belongs to different resource providers to meet the demands of diversified services is a critical issue. Considering the superior advantages of blockchain technology in distributed systems, we propose a blockchain-based decentralized solution for network resource sharing and define a trusted reputation system in this paper. A two-layer distributed network resource sharing architecture are proposed. Based on this architecture, a reputation system are designed. Based on the behavior of network resource provider during, the sharing reputation are quantified to provide a reference for network resource requester to choose suitable resources. Then a reputation-based shard parallel consensus algorithm are developed. Finally, the simulation experiments are designed to analyze the performance of reputation system. The results show that with the support of the reputation system, the resource sharing system will develop healthily.

**Keywords:** Resource sharing · Reputation system · Blockchain · IoT

## 1 Introduction

With the rapid evolution of 5G networks and IoT technology in recent years, an increasing number of devices are connected to the Internet, producing an enormous amount of data and network resource demands [1]. The Internet today has evolved into a relatively open platform with complex and rich resources to adapt to the diverse network environment. Therefore, for these diverse network resources, how to effectively promote the interconnection and comprehensive sharing of resources to meet the demands of diversified services is a critical issue in the future development of computer network technology.

However, the complex and rich resources in the network belong to different enterprises of individuals, and provide ubiquitous and universal network services through flexible resource sharing and mutual cooperation. Constrained by the subjective or objective

intentions of multiple network resource provider, the sharing and collaboration of public/private resources are difficult to guarantee the quality of network service due to lack of trust. Meanwhile, the existence of many problems such as unfair resource scheduling and unequal income distribution hinders the further development of the future network.

As an emerging technology, blockchain proposes a decentralized solution for network resource sharing to solve the above problem [2]. Distributed ledger in blockchain network is a type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner. Blockchain has core technical such as smart contracts, incentive mechanism, encryption algorithm and distributed consensus, and has the following technical features: decentralization, tamper-proof, traceability, publicity, anonymity, and automatic operation. Compared with centralized network resource sharing, blockchain-based distributed network resource sharing realizes trusted resource collaboration in a trustless environment without endorsement of third parties. With the support of the above features, blockchain can provide decentralized and trust support for network resource sharing [3–8]. The distributed network resource sharing based on blockchain provides network resource provider with a trusted resource sharing system to share multi-dimensional network resource.

Based on above features, we propose a distributed network resource sharing system in this paper, define components of the system in detail. Considering the important of user reputation in resource sharing, we specifically propose a reputation system [9–11] for supporting resource sharing. The main contributions are as follows:

- Propose a distributed network resource sharing architecture which consists of two layers. Distributed network resource sharing architecture includes management layer and resource layer, the specific resource sharing procedures for network resource provider and network resource requester are designed based on this architecture.
- Develop a reputation system. Based on the behavior of network resource provider during resource sharing, we quantify the sharing reputation to provide a reference for network resource requester to choose suitable resources.
- Design a reputation-based shard parallel consensus algorithm. We specify the consensus process based on NRR's reputation and the type of network resource.

The remainder of this article is organized as follows. In section II, we present the related work. Section III presents the system model including the distributed network resource sharing architecture and the reputation model. The reputation-based zoning parallel consensus algorithm is designed in section IV. Simulation results and analysis are presented in section V and Section VI conclude this paper.

## 2 System Model

### 2.1 Overview of the Blockchain-Based Distributed Network Resource Sharing Architecture

As shown in Fig. 1, there are two layers in the blockchain-based distributed network resource sharing architecture, resource layer and management layer. In resource layer, there are three types of entities, including resource providers, resource requesters and infrastructure builders. Resource providers involves cloud resource providers, edge

resources providers and user resource providers, where edge resources provided by edge resources providers are deployed in the edge of the network nearby the base station. Resource requesters is the one who wants to rent resources (computing, storage, communication or other resources) to meet their needs. In common, resource requesters will provide a request that illustrate the resource requirements, and then one of the resource providers who has the suitable resources will respond to the requirements and share the resources. Infrastructure builders are the builder of the basic environment for resource sharing, including providing network infrastructure, resource invocation interface and so on. Supported by infrastructure, there are point to point resource sharing capabilities between resource providers and resource requesters.

In management layer, there is a logic blockchain network, which is formed by the participated resource sharing related entities. The management layer involves two types of nodes, normal nodes (yellow) and base nodes (orange). The base nodes are the initial anchor nodes of the blockchain network, they are responsible for maintaining the underlying blockchain network and ensuring its continuous operation. Base nodes are usually played by infrastructure builders. The normal nodes are usually played by the resource providers and the resource requesters. This type of nodes can choose to be a consensus nodes or just a client node to share resource.

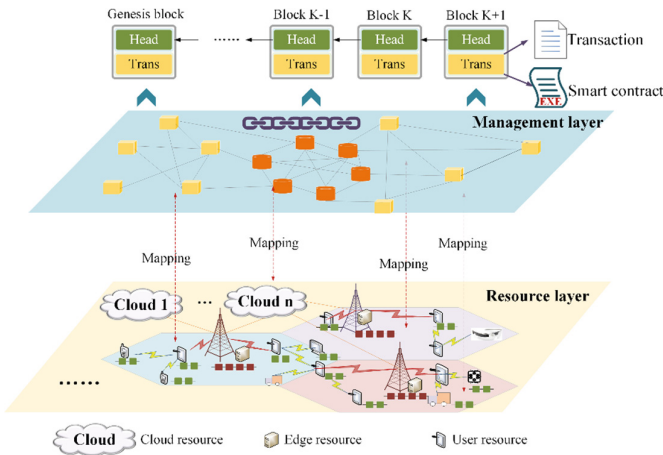


Fig. 1. Blockchain-based distributed network resource sharing architecture

## 2.2 Reputation Model

### Evaluation indicator

To ensure the safe and stable operation of the system, it is necessary to manage users in the system based on their reputation. For users with high reputation, higher permissions can be granted; For users with low reputation, their permissions in the system need to be restricted. In the system, the user reputation is evaluated based on three dimensions: their

online duration, activity, and historical behavior. Among them, the evaluation result of online duration information is called the online duration evaluation value, the evaluation result of activity is called the activity evaluation value, and the evaluation result of historical behavior is called the historical behavior evaluation value. The definitions of the evaluation values are as follows:

*Online duration.* Total duration online  $Tz_i$  refers to the total duration online of a user after entering the system.

It is in an online state after the user  $i$  successfully joins the network resource sharing system when the user's starting time online is recorded as  $Tcs_i$ . There are two situations when a user is in an offline state, i.e. the actively exiting, or an error interrupt exiting. In the status of actively exiting, the user sends a termination request to the ecosystem which will update the status and record the exiting time  $Tce_i$ ; In the status of error interrupt exiting, the system periodically checks the user's status where the monitoring signal detects the disconnection of the user's node, and then records the exiting time as the detection time  $Tce_i$ . Therefore, the service coverage duration for the user  $i$  is  $Tce_i - Tcs_i$ , and the total duration online is:

$$Tz_i = \sum (Tce_i - Tcs_i) \quad (1)$$

Working duration online  $Tw_i$  refers to the total duration that the user has been in a working state since entering the system.

During the working period of resource sharing, the system records the users' starting time to start a resource sharing task as  $Tss_i$ , and the ending time for this resource sharing task as  $Tse_i$ . Therefore, the working duration of the users within a working period of resource sharing can be defined as  $Tse_i - Tss_i$ , and the total working duration online is:

$$Tw_i = \sum (Tse_i - Tss_i) \quad (2)$$

*Activity.* User's activity  $Vt_i$ : refers to the activity of user  $i$  in the system.

After the network resource sharing system starts running, the total number of transactions that occur in the system is  $N$ , and the number of transactions that user  $i$  participates in is  $Vi$ . Therefore, the user's activity is:

$$Vt_i = Vi/N \quad (3)$$

*Historical behavior.*

- Type of resource sharing  $Re_i$ : Refers to the types of resources shared by user  $i$ , including four types: computing power, storage, network, and data.
- Frequency of honest resource sharing  $Ca_i$ : Refers to the number of times user  $i$  has honestly participated in resource sharing.
- Frequency of crimes resource sharing  $Es_i$ : Refers to the number of times user  $i$  has engaged in malicious behavior in resource sharing without integrity.
- Total amount of resource sharing  $Ms_i$ : Refers to the total amount of sharing resources in which user  $i$  participants.



**Normalization model of indicator value**

Based on the various assessment indicators in the three dimensions of online duration, activity, and historical behavior mentioned above, considering the non-uniformity of each indicator in terms of dimensions, the normalization model for the values of relevant indicators in each dimension is defined.

Considering that users with long-lasting stability, honesty, positivity, and high-quality services should achieve higher reputation, this section designs a relative indicator normalization scheme. In the user set  $R = \{1, 2, \dots, n\}$ , we sort the indicators and obtain the maximum value of the current indicators. Set  $X$  as any indicator (such as the total duration online), the system obtains the maximum value  $X_{max}$  of the indicator  $X$  through sorting in the current system, and the value of user  $i$  on the indicator  $X$  is  $X_i$ , then the normalized indicator value of user  $i$  is

$$N_{X,i} = \frac{X_i}{X_{max}} \tag{4}$$

*Evaluation values for various dimensions.*

Evaluation value of online duration  $ST_i$ : The weights of the indicators related to online duration such as the total duration online and the working duration online are  $a_1, a_2$  respectively, where  $a_1 + a_2 = 1, a_1 \geq 0, a_2 \geq 0$ .

Based on the normalization model of indicator values, the normalized values of user  $i$  on the total duration online and the working duration online are obtained as  $\frac{Tz_i}{Tz_{max}}, \frac{Twi}{Twm_{max}}$  respectively.

Therefore, by normalizing and weighting on this indicator, the evaluation value of online duration is defined as

$$ST_i = a_1 * \frac{Tz_i}{Tz_{max}} + a_2 * \frac{Twi}{Twm_{max}} \tag{5}$$

*Evaluation value of activity VT<sub>i</sub>:*

According to the definition of activity, the evaluation value of activity can be defined by normalizing and weighting on the indicator:

$$VT_i = \frac{Vt_i}{Vt_{max}} \tag{6}$$

*Evaluation value of historical behavior AT<sub>i</sub>.*

Define the time when system user  $i$  successfully joins the network resource sharing system as  $T_0$ , and the current time is  $T_n$ . Select two moments between  $T_0$  and  $T_n$  which are denoted as  $T_1$  and  $T_2$  (where  $T_0 < T_1 < T_2 < T_n$ ). Define time interval  $T_0, T_1$  as the long term, time interval  $T_1, T_2$  as the medium term, and time interval  $T_2, T_n$  as the short term. For a user  $i$ , the impact of short-term behavior is greater than that of medium-term behavior, and the impact of medium-term behavior is greater than that of long-term behavior. Therefore, the impact factors for short-term, medium-term, and long-term are defined as  $c_1, c_2, c_3$  respectively, where  $c_1 > c_2 > c_3 > 0$ .

According to the defined time interval and based on the normalization model of indicator values, the indicator values on the frequency of honest resource sharing, the frequency of crimes resources sharing, and the total amount of resource sharing in the “long-term” are denoted as  $Cfa_i$ ,  $Efs_i$ ,  $Mfs_i$ , and the corresponding normalized quantization values are  $\frac{Cfa_i}{Cfa_{max}}$ ,  $\frac{Efs_i}{Efs_{max}}$ ,  $\frac{Mfs_i}{Mfs_{max}}$ ; the indicator values on the frequency of honest resource sharing, the frequency of crimes resources sharing, and the total amount of resource sharing in the “medium-term” are denoted as:  $Cma_i$ ,  $Ems_i$ ,  $Mms_i$ , and the corresponding normalized quantization values are  $\frac{Cma_i}{Cma_{max}}$ ,  $\frac{Ems_i}{Ems_{max}}$ ,  $\frac{Mms_i}{Mms_{max}}$ ; the indicator values on the frequency of honest resource sharing, the frequency of crimes resources sharing, and the total amount of resource sharing in the “short-term” are denoted as  $Cra_i$ ,  $Ers_i$ ,  $Mrs_i$ , and the corresponding notification values are  $\frac{Cra_i}{Cra_{max}}$ ,  $\frac{Ers_i}{Ers_{max}}$ ,  $\frac{Mrs_i}{Mrs_{max}}$ .

Combining the impact factors of time, we obtain the evaluation value corresponding to the frequency of honest resource sharing  $Ca_i$  is:

$$Ca_i = c_1 * \frac{Cra_i}{Cra_{max}} + c_2 * \frac{Cma_i}{Cma_{max}} + c_3 * \frac{Cfa_i}{Cfa_{max}} \quad (7)$$

Combining the impact factors of time, we obtain the evaluation value corresponding to the frequency of crimes resources sharing  $Es_i$  is:

$$Es_i = c_1 * \frac{Ers_i}{Ers_{max}} + c_2 * \frac{Ems_i}{Ems_{max}} + c_3 * \frac{Efs_i}{Efs_{max}} \quad (8)$$

Combining the impact factors of time, we obtain the evaluation value corresponding to the total amount of resource sharing  $Cs_i$  is:

$$Ms_i = c_1 * \frac{Mrs_i}{Mrs_{max}} + c_2 * \frac{Mms_i}{Mms_{max}} + c_3 * \frac{Mfs_i}{Mfs_{max}} \quad (9)$$

Define the weights of indicators related to historical behavior, such as the frequency of honest resource sharing, the frequency of crimes resources sharing, and the total amount of resource sharing as  $d_1$ ,  $d_2$ ,  $d_3$  respectively, where  $d_1 + d_2 + d_3 = 1$ ,  $d_1 \geq 0$ ,  $d_2 \geq 0$ ,  $d_3 \geq 0$ . Considering that crimes has negative impact, the weighted evaluation value of historical behavior is

$$AT_i = d_1 * Ca_i - d_2 * Es_i + d_3 * Ms_i. \quad (10)$$

### Overall weighted score:

Define the three dimensions for evaluating user reputation: the weights of online duration, activity, and historical behavior are  $w_1, w_2, w_3$  respectively, and meet  $w_1 + w_2 + w_3 = 1$ ,  $w_1 \geq 0$ ,  $w_2 \geq 0$ ,  $w_3 \geq 0$ . Therefore, the weighted quantification value of the user's reputation is:

$$Crd_i = w_1 * ST_i + w_2 * VT_i + w_3 * AT_i. \quad (11)$$

### 3 Reputation System for Resource Providers

The trust reputation system are realized based on the smart contract technology in blockchain. Based on resource providers' behaviours in resource sharing period, the blockchain will automatically caculate a reputation value and store it in the blockchain ledger. There are two phases in the reputation system: reputation initialization and reputaion update.

#### 3.1 Reputation Initialization

The reputation initialization phase can first complete the account registration of the resource providers. The provider's public and private key pair is generated on the client side, the private key is saved on the client side, and the public key is exposed to all nodes in the blockchain network. The registration information of a resource node includes the type of services/resources provided, amount of resources available for services, registration time, and public key. After the registration, the resource user will complete the initialization score.

Set the initial reputation value of the common resource provider to 0. Considering the initial participation incentive of resource-sharing users to join the system, the initial score is awarded to the former  $AU$  user accounts registered after the system is launched. After stable operation of the system (number of users  $> AU$ ), considering the "slow start" phenomenon of the reputation score of the newly added node, set the user account within  $T$  time (e.g. one week) as the new account, establish a separate reputation list, and score alongside other users. After more than one week, the reputation ranking is returned to the general list.

#### 3.2 Resource Sharing Based on Reputation

Based on users' behaviors, there are five steps for reputation update and resource sharing.

Step 1: The smart contract completes node access authentication and updates the associated credit value. The result of identity authentication will clearly limit the user's operation rights in the resource sharing system and the blockchain network.

Step 2: Start to sharing resource/provide service. Resource providers provide service information such as node ID, time stamp, service type, and available service resources. Resource providers obtain service access permissions and change the service status to start services by invoking smart contracts. At the same time, the service information (the on-chain service information) is broadcast synchronously to all nodes in the system through the blockchain, indicating that the relay node has started services and can be discovered by users. Start waiting for the service to connect.

Step 3: Provide resource request. Resource requester proposes a request and invoke smart contract to find the suitable resource with high reputation.

Step 4: Establish a resource sharing connection. The requester sends the application for establishing a connection to the provider node, the provider invokes the blockchain smart contract to verify the requester's identity information and the provider's identity information will be provided for requester to confirm the connection information. The requester and provider who complete the mutual verification establish a connection

between each other. The blockchain will record the service transaction to provide data for the reputation system.

Step 5: The smart contract completes the reputation update and updates the status of the resource providers. The provider synchronizes the transaction settlement information to the blockchain, the blockchain calls smart contract to complete the transaction settlement, and update the reputation. After every resource sharing, the blockchain recalculates the reputation value of the provider.

### 3.3 A Shard Parallel Consensus Algorithm Based on Reputation

To support widely distributed resource sharing services, we propose a shard parallel consensus algorithm based on trusted reputation ranking. Resource providers will gain the right to participate in consensus competition based on the reputation value in the reputation system. Nodes that provide the same resources at the same time will form blockchain shards with requesters requesting such resources. Every shards will complete efficient consensus within the shard, and then initiate asynchronous net wide consensus by the nodes with high reputation. The algorithm pseudocode is shown below.

- Smart contracts are used to analyze the types of resources shared by nodes and node reputation
- Form network shards based on the resource type and form shard set  $\{s_1, s_2, \dots, s_n\}$  (Nodes that share multiple types of resources can participate in multiple shards)
- Start consensus within every shards:
  - Select the winning node by integrating all resources and reputation value
  - Package resource sharing and other transactions form blocks, and start broadcasting verification
  - Distribute reputation rewards
- The winning node in each shard will hash the generated blockchain, and generate transactions, broadcast to the whole network to form the basis for transaction verification within the shard.

## 4 Simulation

To analyze the performance of the reputation system, we select 4 users with different behaviors from N resource provider users to analyze the changes in reputation values with the frequency of resource sharing. In the figure, x represents the frequency of resource sharing, y represents the user reputation value, and the four dashed lines show the changes in reputation values corresponding to four different users (Fig. 2).

4 users are simulated. User 1 is a real honest user, with 100% of their behavior being honest; User 2 is a basic honest user, with 70% of their behavior being honest; User 3 is a fundamentally dishonest user, with 30% of their behavior being honest; User 4 is a malicious user, with 1% of their behavior being honest.

Analyze the quantitative changes in user reputation values under different weights. For one user, the x-axis represents the change in transaction quantity, and the y-axis represents the change in user reputation under different weights (Fig. 3).

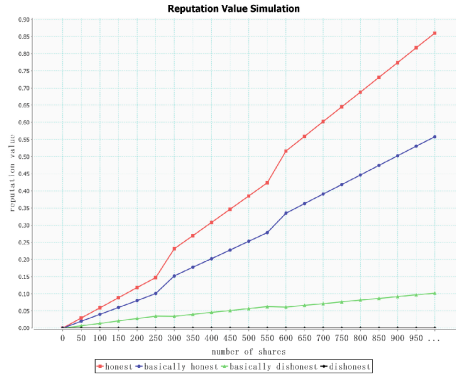


Fig. 2. The reputation changes with number of shares increases.

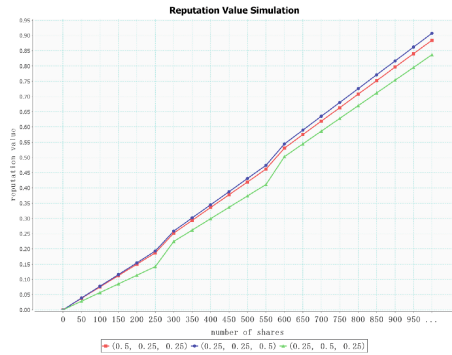


Fig. 3. The reputation with different weights.

For an honest user, simulations are conducted on the changes of reputation when the weights of online duration, activity, and historical behavior  $w_1$ ,  $w_2$ ,  $w_3$  are (0.5, 0.25, 0.25), (0.25, 0.25, 0.5), and (0.25, 0.5, 0.25), respectively.

### 5 Conclusion

To support distributed resource sharing in IoT, we propose a trusted reputation system based on blockchain. At first, we develop a blockchain-based two-layer resource sharing architecture, and define the reputation model. Then we describe the reputation system and design a reputation-based parallel consensus algorithm, which construct the shard blockchain network based on resource type, and give the consensus right based on reputation value. Finally, we design the simulation experiments to analyze the reputation system. It is found that the honest nodes will get more benefits in the process of resource sharing, and the dishonest nodes will be punished. With the support of the reputation system, the resource sharing system will develop healthily.

## References

1. Singh, J., Pasquier, T., Bacon, J., et al.: Twenty security considerations for cloud-supported internet of things. *IEEE Internet Things J.* **3**(3), 269–284 (2017)
2. Yue, K., Zhang, Y., Chen, Y., et al.: A survey of decentralizing applications via blockchain: the 5G and beyond perspective. *IEEE Commun. Surv. Tutor.* **23**(4), 2191–2217 (2021)
3. Varma, R., Agrawal, A., Bhatia, A., Tiwari, K.: Multi-vendor IoT-based resource sharing using OAuth and blockchain. In: 2022 International Conference on Information Networking (ICOIN), Jeju-si, Korea, Republic of, 2022, pp. 74–77 (2022)
4. Li, M., Huang, G.: Blockchain-enabled workflow management system for fine-grained resource sharing in E-commerce logistics. In: 2019 IEEE 15th International Conference on Automation Science and Engineering (CASE), Vancouver, BC, Canada, 2019, pp. 751–755 (2019)
5. Gorla, P., Chamola, V.: CellularBlockB5G: a blockchain-based multi operator spectrum sharing simulator for 5G and beyond networks. In: 2022 IEEE International Conference on Communications Workshops (ICC Workshops), Seoul, Korea, Republic of, 2022, pp. 265–270 (2022)
6. Cheng, H., Hu, Q., Zhang, X., Yu, Z., Yang, Y., Xiong, N.: Trusted resource allocation based on smart contracts for blockchain-enabled internet of things. *IEEE Internet of Things J.*, **9**(11), 7904–7915 (2022). (1 June 2022)
7. Le, Y., et al.: Resource sharing and trading of blockchain radio access networks: architecture and prototype design. *IEEE Internet of Things J.*
8. Guo, Z., Zhang, J., Gao, Z., Wang, A., Pan, C., Li, X.: Blockchain-based multi-party cooperation and resource-sharing scheme for space-air-ground integrated networks. In: 2021 IEEE 21st International Conference on Communication Technology (ICCT), Tianjin, China, 2021, pp. 947–952 (2021)
9. Mukhametov, D.: Self-organization of network communities via blockchain technology: reputation systems and limits of digital democracy. In: 2020 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Svetlogorsk, Russia, 2020, pp. 1–7 (2020)
10. Debe, M., Salah, K., Rehman, M., Svetinovic, D.: Towards a blockchain-based decentralized reputation system for public fog nodes. In: 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 2019, pp. 1–6 (2019)
11. Wang, X., Ji, S., Y. Liang, Q., Chiu, D.K.W.: An impression-based strategy for defending reputation attacks in multi-agent reputation system. In: 2016 9th International Symposium on Computational Intelligence and Design (ISCID)



# Multi-objective Reinforcement Learning Algorithm for Computing Offloading of Task-Dependent Workflows in 5G enabled Smart Grids

Yongjie Li, Jizhao Lu, Huanpeng Hou, Wenge Wang<sup>(✉)</sup>,  
and Gongming Li

State Grid Henan Electric Power Company Information and  
Communication Branch, Henan 450052, China  
wgzx\_gw@163.com

**Abstract.** Computational offloading is considered a promising emerging paradigm for addressing the limited resources of edge devices in expanding power grids. However, with the advancement of intelligent technologies such as digitalized power grids, applications often consist of several interdependent subtasks, forming interconnected automated workflows. This paper focuses on the computational offloading technique within task-dependent workflows. It proposes a multi-objective optimization problem for offloading, considering both time and energy consumption. The model takes into account the constraints of task duration, communication capacity, and computational capacity. Additionally, a predictive-guided multi-objective reinforcement learning algorithm based on Pareto optimization (MORLBP) is introduced. This algorithm combines the principles of multi-objective optimization, Pareto optimality theory, and deep reinforcement learning. It utilizes the quality of the Pareto front as a metric and is compared against NSGA-II and MOPSO algorithms. The proposed algorithm's effectiveness and advancement are validated through simulations, demonstrating its efficiency and innovation in tackling the multi-objective offloading problem within task-dependent workflows.

**Keywords:** Task-dependent workflows · Task offloading strategy · Multi-objective reinforcement learning · Pareto optimization

## 1 Introduction

The advent of 5G networks has brought about a revolutionary transformation in various domains by leveraging the proliferation of mobile devices. For example, through 5G-connected sensors, data from renewable energy sources such as solar and wind energy can be collected and transmitted to smart grids for analysis and optimization, enabling efficient utilization and management of energy resources [1]. However, the limited computing power and battery life of mobile devices

(MDs) hinder the comprehensive implementation of computation-intensive applications. Multi-access edge computing (MEC) emerges as a promising solution that overcomes this obstacle by providing abundant computing and storage resources around MDs [8].

One of the most crucial issues when employing offloading techniques is the offloading decision problem [10, 12, 13]. The offloading decision determines which tasks within an application should be offloaded to edge servers and which tasks should be executed locally on MDs, thereby ensuring a satisfactory Quality of Experience (QoE) for end-users. However, task dependencies cannot be overlooked as the results obtained from executing certain tasks act as prerequisites for executing other tasks [3]. For example, in an alarm response workflow, when an abnormal grid state is detected, an alarm notification is generated. Subsequently, maintenance personnel are assigned to perform device repairs. Only after the device repairs are completed can the alarm be cleared and the repair status recorded. If we disregard the dependencies between tasks while offloading such applications, the execution of the application may fail. Therefore, task dependency offloading holds significant importance in MEC. Due to the NP-hardness of the problem, most research on task dependency offloading relies on heuristic or metaheuristic algorithms. Inspired by nature, Kishor *et al.* proposed a metaheuristic scheduler called Smart Ant Colony Optimization (SACO) for task offloading of IoT sensor applications in fog environments [2]. Saemi *et al.* introduced a novel optimization approach, the Multi-Objective Discrete Water Cycle Algorithm (MDWCA), to schedule tasks from mobile source nodes to processor resources in a hybrid MCC architecture comprising public clouds, small clouds, and mobile devices [6]. The optimal selection of task offloading is necessary to minimize response time and energy consumption. However, these studies have not been perfectly adapted to dynamic MEC scenarios due to the complexity and time-consuming nature of the aforementioned algorithms.

Deep Reinforcement Learning (DRL), which combines Reinforcement Learning (RL) with Deep Neural Networks (DNN), can address sequential decision-making problems in dynamic MEC scenarios, as DRL enables behavior adaptation to changes in the MEC environment, such as the quality of the time-varying wireless channel [7]. The Offload Dependency Task (ODT) problem falls within the realm of sequential decision-making problems that DRL can resolve. Recently, many researchers have employed RL-based methods to handle MEC systems and achieved promising performance in computational offloading [9, 11]. The completion time of the application and the consumption of MD energy are typically considered the two most critical criteria for performance evaluation. These objectives are mutually conflicting, implying that improving one objective would lead to the deterioration of the other. However, recent studies have mostly defined user utility in computational offloading as a weighted scalarization of each objective, employing methods like the weighted sum approach or interrelation-based approaches. Nevertheless [5], these single-strategy methods face challenges such as difficulty in finding an appropriate set of objective preferences, handling nonlinearity in utility functions, and poor compatibility, resulting in suboptimal computational offloading performance.



The core idea of Pareto analysis lies in distinguishing primary and secondary factors that have a decisive impact among numerous factors when determining something, identifying some key factors that play a determining role, and numerous minor factors that have a relatively small influence [4]. For multi-objective problems, Pareto optimization helps us find an acceptable solution, namely an efficient solution. Therefore, this paper combines the multi-objective optimization problem with Pareto optimization theory and deep reinforcement learning algorithm and proposes a multi-objective reinforcement learning optimization algorithm based on Pareto optimization. The advantages that reinforcement learning can better guide the solution vector of the population to solve the Pareto solution vector better to solve the multi-objective optimization problem, and the past offspring population is used to predict the expected improvement direction of the population. The excellent individuals in the population are selected by the selection optimization algorithm for iteration so that the population is gradually close to the Pareto frontier.

The multi-agent deep reinforcement learning algorithm studied in this paper has important theoretical and practical significance for solving the optimal offloading problem of multi-workflow. By reducing the overall completion time of the workflow and the total energy consumption of mobile devices, this method provides an innovative solution for practical applications in intelligent power grids and other fields.

## 2 System Model and Problem Formulation

### 2.1 Network Model

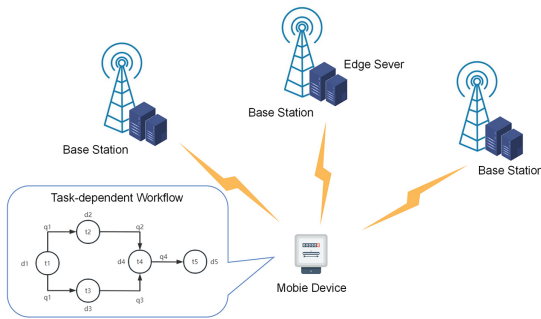


Fig. 1. Mobile edge network with task-dependent workflow.

Figure 1 shows an MEC system consisting of single MD and multiple edge servers. In this system,  $x_i$  represents either an MD or an edge server,  $i \in [0, M]$ . Specifically, when  $i$  is equal to 0, it denotes the mobile device, while  $i \neq 0$  represents an

edge server.  $M$  indicates the number of edge servers, and  $i$  in this context represents the identifier of the edge server. The mobile device hosts an application that generates a substantial volume of workflow tasks. It is assumed that each mobile device generates only one type of workflow. The workflow process in the MEC system can be described as follows: Initially, the mobile device sends a request to the proxy server for offloading workflow tasks. Subsequently, the proxy server periodically makes task offloading decisions, determining the optimal offloading location for each workflow task generated by the mobile device. The offloading decisions are then communicated back to the corresponding mobile device. Based on the received offloading strategy, the mobile device dispatches the workflow tasks to the edge servers. Finally, each edge server executes the offloaded workflow tasks and returns the computation results to the respective mobile device.

## 2.2 Task-Dependent Workflow Model

Taking the workflow model within the mobile device depicted in the diagram as an example, our model assumes that tasks are composed of several dependent subtasks, represented by a directed acyclic graph (DAG) denoted as  $G = (T, E)$ . The subtasks in the workflow exhibit dependencies, where  $T$  represents a subtask and  $E$  represents the dependency relationship between subtasks. Some subtasks are determined to be locally executable on the mobile device if they do not require offloading, while others are deemed eligible for offloading. For the latter case, once the preceding tasks (if any) are completed, the mobile device transfers the output data of the preceding tasks to the designated edge server for offloading. The edge server receives the data and executes the task, subsequently transmitting the output data back to the mobile device before proceeding to the next task.

Let  $N = |T|$  represent the number of tasks within the DAG  $G$ . Additionally, let  $d_j$  denote the size of the task  $t_j$ , and  $q_j$  represents the size of the output data generated upon the completion of task  $t_j$ . Regarding task offloading decisions, our primary concern lies in minimizing both the time and energy consumption, as these factors determine whether the tasks should be executed on the mobile device or dispatched to an edge server for execution.

## 2.3 Latency and Energy Consumption Model

Let us assume that  $\varphi_j \in \{0, 1, \dots, M\}$ ,  $j \in [1, N]$  represents the offloading decision for the subtasks  $t_j$  on the mobile device and  $\delta_j$  serves as the offloading indicator.

$$\delta_j = \begin{cases} 0, & \varphi_j = 0 \\ 1, & \varphi_j \neq 0 \end{cases}, \quad (1)$$

when  $\delta_j = 0$ , it signifies that the current task  $t_j$  is executed locally on the MD; otherwise, it is sent to an edge server for execution.

The system's latency encompasses the time required for task execution and data transmission. Firstly, the time taken for device  $x_i$  to execute task  $t_j$  is

denoted as  $T_j^s = \frac{d_j}{F_i^s}$ , where  $F_i^s$  represents the computational capability of the device  $x_i$ .  $S_i$  denotes the transmission rate between MD  $x_0$  and edge server  $x_i$ . Therefore, we can express the latency for the task  $t_j$  to be transmitted from MD  $x_0$  to the edge server  $x_i$  as  $T_j^t = \frac{d_j}{S_i}$ . Moreover, for the subtasks that need to be offloaded to an edge server, the edge server receives the data and executes the task, followed by transmitting the output data back to the mobile device. Hence, there is an additional delay as the mobile device receives the output data after task  $t_j$  is completed on edge server  $x_i$ , denoted as  $T_j^r = \frac{q_j}{S_i}$ . Finally, the system latency can be expressed as follows:

$$T(G) = \sum_{j=1}^N \left[ (T_j^s)^* (1 - \delta_j) + (T_j^t + T_j^r + T_j^s)^* \delta_j \right] \quad (2)$$

Formally, the system's energy consumption arises from task execution on the edge server and the local device. We assume that the energy consumption of the server is proportional to the computational load. Consequently, the system's energy cost for executing task  $t_j$  in the local MD can be calculated as  $E_j^l = k \times d_j \times (F_j^s)^2$ , where  $k$  represents the effective capacitance coefficient of the chip architecture. The energy consumption resulting from task execution on the edge server includes the energy expended when the MD transfers the task to the edge server and the energy consumed when the MD receives the output data from the edge server.  $E_j^t$  denotes the energy consumption for transmitting the task  $t_j$  from the mobile device to the edge server  $x_i$  and is defined as  $E_j^t = P_i \times T_j^t$ , where  $P_i$  represents the receiving power of the edge server.  $E_j^r$  signifies the energy consumption for the mobile device to receive the output data of task  $t_j$  after its execution on edge server  $x_i$  and is given by  $E_j^r = P_i \times T_j^r$ . Hence, the system's energy consumption can be expressed as follows:

$$E(G) = \sum_{j=1}^N \left[ (E_j^l)^* (1 - \delta_j) + (E_j^t + E_j^r)^* \delta_j \right]. \quad (3)$$

## 2.4 Problem Formulation

Therefore, in order to minimize system latency and energy consumption, we formulate the optimization problem as follows:

$$\underset{\varphi_j}{\text{Minimize}} \quad (T(G), E(G)) \quad (4)$$

$$s.t. \quad \text{C1: } \varphi_j \in \{0, 1, \dots, M\}, \forall j \in \{1, \dots, N\},$$

$$\text{C2: } \sum_{j=1}^k \left[ (T_j^s)^* (1 - \delta_j) + (T_j^t + T_j^r + T_j^s)^* \delta_j \right] \leq T_j^{\text{start}}, t_k \in \text{pre}(t_j),$$

$$\text{C3: } T_j^t + \sum_{j=1}^k \left[ (T_j^s)^* (1 - \delta_j) + (T_j^t + T_j^r + T_j^s)^* \delta_j \right] \leq T_j^{\text{start}}, t_k \in \text{pre}(t_j). \quad (5)$$

Constraint C1 defines the constraint on the task execution location, specifying whether task  $t_j$  should be executed on the mobile device (MD) or on a specific edge server. If  $t_j$  is to be executed on the MD, constraint C2 applies; otherwise, constraint C3 applies. Constraint C2 states that  $t_j$  can only start after all its preceding nodes have completed execution on the MD, while for nodes executed on an edge server, their output data must be fully returned to the MD. If  $t_j$  is to be executed on an edge server, constraint C3 specifies that the input data must be transferred to the edge server  $x_i$ , and all its preceding tasks must have been executed before the execution of task  $t_j$  can commence.

### 3 Multi-objective Reinforcement Learning Algorithm Based on Pareto Optimization

This paper proposes an effective algorithm called the Multi-objective Reinforcement Learning Algorithm based on Pareto Optimization (MORLBP) to compute the Pareto policy set, offering a more efficient and advanced approach to solving multi-objective optimization problems. The MORLBP algorithm consists of three main stages: the warm-up stage, the evolution stage, and the Pareto analysis stage, as shown in Fig. 2.

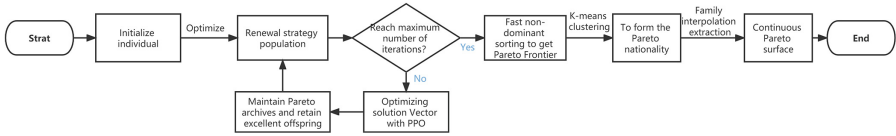


Fig. 2. The flow chart of the proposed algorithm.

**Warm-up stage:** In this stage,  $n$  individuals are randomly initialized, where each individual represents a different solution to the problem model. The Multi-Objective Policy Gradient (MOPG) algorithm is employed to optimize each policy, using  $n$  uniformly distributed non-negative weights  $\{\omega_i\}$  ( $\sum_i \omega_{i,j} = 1, 1 \leq i \leq n$ ) to specify the number of iterations. The policies generated in this stage form the first generation of the policy population. This stage is crucial in helping the initial policies escape low-performance regions characterized by high noise and unpredictability.

**Evolution stage:** In each generation of the evolution stage, the analytical model of each policy is learned from the reinforcement learning data of the population's past iterations. This model is used to predict the expected improvement of each optimization weight. The predicted model is then utilized to guide the selection of  $n$  pairs of policy weights using an optimization algorithm, maximizing the quality of the Pareto set. Finally, the selected tasks are optimized using the Proximal Policy Optimization (PPO) algorithm with a fixed number of iterations, generating new offspring policies to update the population.

**Pareto analysis stage:** Once a discrete set of Pareto policies is found, the MORLBP algorithm performs Pareto analysis on the computed policies to identify different policy families. Then, a continuous representation of the Pareto set is derived by interpolating within each family. The policies are embedded into a lower-dimensional parameter space using t-SNE for better observation. After obtaining the embedding in the lower-dimensional space, the simplified policies are clustered into several classes using the k-means clustering method. The entire Pareto optimal set consists of several disjoint policy families, with each family responsible for a different continuous segment on the Pareto frontier.

Since this algorithm uses the model-free reinforcement learning algorithm, we need to specify the action, state and reward. Next, we will build a multi-objective Markov decision process (MOMDP) based on the problem model mentioned in the previous section.

(1) State: The state space represents a collection of parameters such as computing capabilities and the number of executed tasks for each entity.  $S = \{S_t \mid S_t = (\lambda, t_j, s_t), t = 1, 2, 3, \dots\}$  represents the state of the MEC system environment at time  $t$ . In state  $S_t$ ,  $\lambda = j - 1$  indicates the number of tasks already executed so far,  $t_j$  represents the  $j$ -th task to be executed in the execution order vector  $O$ , and  $s_t = (s_t^0, s_t^1, \dots, s_t^M)$  represents the remaining executable task capacities for the mobile devices and  $M$  edge servers at time  $t$ .

(2) Action: The action space is the set of actions taken by the mobile device, denoted as  $A = \{a_t \mid a_t \in \{\varphi_1, \varphi_2, \dots, \varphi_N\}, t = 1, 2, 3, \dots\}$ .  $a_t$  represents the action taken by the mobile device in state  $S_t$ , i.e., the execution location of task  $t_j$ . If  $a_t = 0$ , it indicates that the task is executed on the mobile device, otherwise, it is offloaded and executed on an edge server.

(3) Reward: The objective is to minimize both the completion time  $T(G)$  of the application and the energy consumption  $E(G)$  of the mobile device. Therefore, after taking action  $a_t$  in state  $S_t$ , the received reward is defined as a vector value  $r_t = (r_t^T, r_t^E)$ . Let  $G_j$  represent the subgraph consisting of the first  $j$  tasks in the execution order vector  $O$ . We compute the completion time  $T(G_j)$  of  $G_j$ . To minimize  $T(G)$ , we set  $r_t^T = -T_j$ , which represents the negative increment of the reward based on action  $a_t$  for executing  $t_j$ .  $T(G_0) = 0$  indicates no task is executed. For the reward  $r_t^E$ , we first calculate the energy consumption  $E_j$  incurred by executing  $t_j$ , and set  $r_t^E = -E_j$ , which again represents the negative increment of the reward after completing action  $a_t$ . Therefore, the accumulated reward over time is  $R_t = (R_t^T, R_t^E)$ .  $R_t^T$  and  $R_t^E$  represent the return values of  $r_t^T$  and  $r_t^E$  within the time step  $t$ , defined as follows, where  $\alpha$  is the discount factor:

$$R_t^T = - \sum_{k=t}^N \alpha^{k-t} T_j, \quad R_t^E = - \sum_{k=t}^N \alpha^{k-t} E_j \quad (6)$$

To simultaneously minimize  $T(G)$  and  $E(G)$ , it is equivalent to maximizing the expected return  $R_t$ .

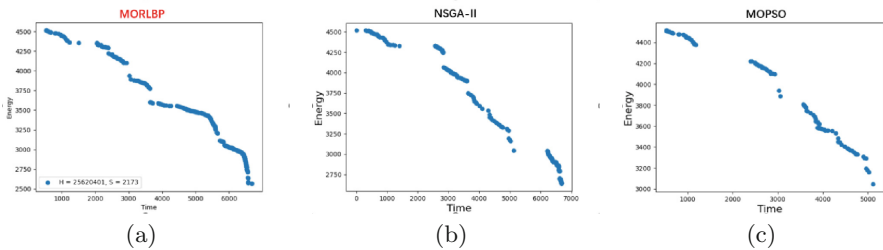
## 4 Simulation and Analysis

To benchmark the proposed algorithm, a simulated MEC system with three edge servers is constructed in this study. All code implementations are carried out on Windows 10 using Python 3.7. Various experimental parameters used in the simulation experiments are presented in the following Table 1. To validate the effectiveness and superiority of the proposed algorithm in terms of overall completion time of the workflow and energy consumption of mobile devices within the constructed problem model, the following simulation experiments were conducted. A comparison was made with the NSGA-II and particle swarm optimization (MOPSO) algorithm while ensuring the consistency of the model parameters throughout the process. Detailed analysis was performed on the results obtained from each experimental group, along with the underlying reasons behind them.

**Table 1.** Parameter setting.

Parameter	Value	Parameter	Value
M	3	$d_j$	[100, 1024]MB
N	5	$S_i$	[5, 15]MB/s
$F_0^s$	2MB/s	k	1
$F_i^s$	[10, 40]MB/s	$P_i$	{100, 300, 500, 200}Hz

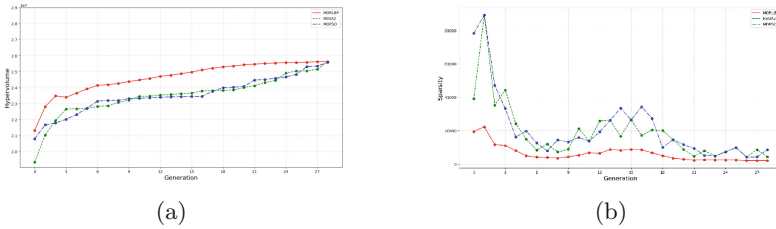
The continuous Pareto representation constructed by the proposed algorithm, along with the Pareto frontiers of the two baseline algorithms, is shown in Fig. 3. To test the accuracy of our continuous representation, observation points were sampled on the continuous Pareto frontier, and the relative error between the expected objectives and interpolation policy objectives was evaluated. The relative error for the majority of points was below 1%, further demonstrating the effectiveness of constructing the continuous Pareto surface.



**Fig. 3.** Strategic populations determined by different algorithms. **a** MORLBP **b** NSGA-II **c** MOPSO.

Furthermore, this study demonstrates the quality of the approximated Pareto set through the hypervolume indicator and sparsity metric. Figure 4 provides

an intuitive comparison of the results. The proposed algorithm outperforms the other two algorithms significantly in terms of the hypervolume indicator (larger values are better). Moreover, the proposed algorithm also exhibits superior performance in the sparsity metric (smaller values are better). Thus, it can be concluded that the proposed algorithm is capable of selecting important reinforcement learning tasks, leading to a more effective improvement in Pareto quality compared to the baseline methods. By utilizing the policy-improvement prediction model, the proposed algorithm can identify which regions on the Pareto frontier are approaching optimality and which regions can still be improved. Consequently, optimal task offloading decisions can be selected, and high-quality Pareto frontiers can be efficiently generated.



**Fig. 4.** Comparison of hypervolume and sparsity. **a** Hypervolume **b** Sparsity.

## 5 Conclusion

This paper focuses on the task offloading problem for energy-constrained mobile devices in 5G mobile edge computing scenarios, considering the minimization of both latency and energy consumption. A multi-objective optimization problem model is constructed for task dependency workflows in mobile edge networks. The paper proposes a predictive-guided multi-objective reinforcement learning algorithm called MORLBP, which combines multi-objective optimization, Pareto optimality theory, and deep reinforcement learning algorithms. By balancing the optimization of multiple objectives with different preferences and aiming at lower energy consumption and latency, the algorithm determines the action decisions for the execution location of workflow subtasks. Comparative experiments demonstrate that the MORLBP algorithm achieves a higher Pareto frontier quality and exhibits good stability and adaptability in optimizing both energy consumption and latency. These results provide evidence of the effectiveness and feasibility of the proposed optimization method.

**Acknowledgment.** This work is supported by the State Grid Henan Electric Power Company Science and Technology Project (no.SGHAXT00GCJS2250197).

## References

1. Hemanand, D., Jayalakshmi, D., Ghosh, U., Balasundaram, A., Vijayakumar, P., Sharma, P.K.: Enabling sustainable energy for smart environment using 5g wireless communication and internet of things. *IEEE Wirel. Commun.* **28**(6), 56–61 (2021)
2. Kishor, A., Chakarbarty, C.: Task offloading in fog computing for using smart ant colony optimization. *Wirel. Personal Commun.* 1–22 (2021)
3. Liu, J., Wang, S., Wang, J., Liu, C., Yan, Y.: A task oriented computation offloading algorithm for intelligent vehicle network with mobile edge computing. *IEEE Access* **7**, 180491–180502 (2019)
4. Luo, Q., Li, C., Luan, T.H., Shi, W.: Minimizing the delay and cost of computation offloading for vehicular edge computing. *IEEE Trans. Serv. Comput.* **15**(5), 2897–2909 (2022)
5. Movahedi, Z., Defude, B., et al.: An efficient population-based multi-objective task scheduling approach in fog computing systems. *J. Cloud Comput.* **10**(1), 1–31 (2021)
6. Saemi, B., Sadeghilalimi, M., Hosseinabadi, A.A.R., Mouhoub, M., Sadaoui, S.: A new optimization approach for task scheduling problem using water cycle algorithm in mobile cloud computing. In: 2021 IEEE Congress on Evolutionary Computation (CEC), pp. 530–539. IEEE (2021)
7. Shakarami, A., Ghobaei-Arani, M., Shahidinejad, A.: A survey on the computation offloading approaches in mobile edge computing: a machine learning-based perspective. *Comput. Netw.* **182**, 107496 (2020)
8. Spinelli, F., Mancuso, V.: Toward enabled industrial verticals in 5g: a survey on MEC-based approaches to provisioning and flexibility. *IEEE Commun. Surv. Tutor.* **23**(1), 596–630 (2020)
9. Wang, J., Hu, J., Min, G., Zhan, W., Ni, Q., Georgalas, N.: Computation offloading in multi-access edge computing using a deep sequential model based on reinforcement learning. *IEEE Commun. Mag.* **57**(5), 64–69 (2019)
10. Wang, W., Qu, R., Liao, H., Wang, Z., Zhou, Z., Wang, Z., Mumtaz, S., Guizani, M.: 5g MEC-based intelligent computation offloading in power robotic inspection. *IEEE Wirel. Commun.* **30**(2), 66–74 (2023)
11. Yan, J., Bi, S., Zhang, Y.J.A.: Offloading and resource allocation with general task graph in mobile edge computing: a deep reinforcement learning approach. *IEEE Trans. Wirel. Commun.* **19**(8), 5404–5419 (2020)
12. Yu, Y.: Mobile edge computing towards 5g: vision, recent progress, and open challenges. *China Commun.* **13**(Supplement2), 89–99 (2016)
13. Zhang, K., Mao, Y., Leng, S., Zhao, Q., Li, L., Peng, X., Pan, L., Maharjan, S., Zhang, Y.: Energy-efficient offloading for mobile edge computing in 5g heterogeneous networks. *IEEE Access* **4**, 5896–5907 (2016)





# Distributed Core Network Traffic Prediction Architecture Based on Vertical Federated Learning

Pengyu Li<sup>1</sup>, Chengwei Guo<sup>2</sup>, Yanxia Xing<sup>1</sup>, Yingji Shi<sup>2</sup>, Lei Feng<sup>2</sup>(✉),  
and Fanqin Zhou<sup>2</sup>

<sup>1</sup> 6G Research Center, China Telecom Research Institute, Beijing 102209, China

<sup>2</sup> State Key Laboratory of Networking and Switching Technology, Beijing University of Posts  
and Telecommunications, Beijing 100876, China  
fenglei@bupt.edu.cn

**Abstract.** Network traffic prediction has always been an important research topic, frequently employed in intelligent network operations for load awareness, resource management, and predictive control. Most existing methods adopt a centralized training and deployment approach, neglecting the involvement of multiple parties in the prediction process and the potential for training prediction models using distributed methods. This study introduces a novel wireless traffic prediction framework based on split learning, addressing the limitations of existing centralized methods. The proposed framework enables multiple edge clients to collaboratively train high-quality prediction models without transmitting large amounts of data, thus mitigating latency and privacy concerns. Each participant trains a dimension-specific prediction model using its local data, which are then aggregated through a collaborative interaction process. A partially global model is trained and shared among clients to tackle statistical heterogeneity challenges. Experimental results on real-world wireless traffic datasets demonstrate that our approach outperforms state-of-the-art methods, showing its potential and accuracy in Internet traffic prediction.

**Keywords:** Traffic prediction · Core network · Federated learning · Split learning

## 1 Introduction

The recent advancements in network paradigms (5G/6G, IoT, Industrial Internet) and the popularity of Internet applications (live streaming, video sharing, virtual reality) have caused substantial growth in Internet traffic. Accurate traffic prediction is critical for intelligent network management and planning, optimizing network services and content delivery. Traffic prediction enables proactive allocation of communication and computing resources to meet QoS requirements, making it a vital research area.

In Internet traffic prediction, real-world scenarios involve multiple parties with vested interests, such as university network management departments, Internet service

providers, and Internet content providers, acting as intelligent agents. Despite the effectiveness of distributed machine learning over single-server training, its superiority for Internet traffic prediction remains unexplored [1].

Federated Learning (FL) is a successful approach for privacy-preserving prediction tasks. Multiple clients collaborate to train models under a central server's coordination. Only intermediate gradients or parameters are sent, keeping raw data secure. FL offers advantages for next-gen communications [2], leveraging edge computing, reducing latency [3], and enabling large-scale data collection and flexible model training. Clients actively collect data and update the global model for improved efficiency and accuracy.

In Federated Learning (FL) for network traffic prediction, there are notable re-search challenges due to user mobility leading to complex spatio-temporal couplings in wireless traffic. Moreover, different base stations (BSs) exhibit distinct traffic patterns, creating highly heterogeneous traffic data, which poses a significant challenge for accurate prediction.

In Vertical Federated Learning, data sharing among participants is done through encryption and secure computation. Encryption protocols protect sensitive feature data, allowing joint computation of gradient updates and model parameter transmission while ensuring data privacy. This enables collaborative training of high-performing models without revealing specific data contents.

Vertical Federated Learning and Split Learning can be combined for improved privacy protection and performance. Split Learning assigns different model parts to different devices, facilitating joint learning without compromising privacy. This approach has great potential in handling privacy-sensitive tasks effectively.

Our main goal is to utilize both computation-rich and computation-limited subnets in the training process to develop high-performing deep learning models for traffic prediction. This approach improves the efficiency of traffic prediction by leveraging collaborative intelligence and ensuring privacy protection. The main contributions of this paper are as follows:

- (1) We conducted experiments on a real network dataset to verify the feasibility of the above approach. The experimental results show that the framework achieves significant results in improving the prediction accuracy and reducing the training over-head, thus significantly improving the traffic prediction efficiency.
- (2) We propose a longitudinal federated learning framework incorporating split learning that aims to improve efficiency in traffic prediction tasks by using feature-based models trained collaboratively by nodes with stronger as well as weaker arithmetic power. The framework improves the efficiency of traffic prediction.

The rest of the paper is organized as follows. Section 2 further discusses the different types of prediction models. We describe the prior knowledge in detail in Sect. 3. Section 4 presents the traffic prediction problem, as well as the modeling framework to solve the problem and a specific algorithmic scheme based on the framework. Experimental results and discussion are given in Sects. 5, and 6 concludes the paper.

## 2 Related Work

Recently, accurate traffic modeling and prediction have become crucial for network communications tasks, leading to increased attention towards network traffic prediction. It involves time series prediction and can be categorized into three main types: simple, parametric, and non-parametric methods. These methods aim to offer effective prediction strategies for managing traffic variations in wireless communications.

The historical averaging method is a representative among the first type of methods [4]. It uses the average of historical data or the last observation as a future forecast. While simple and easy to implement, it lacks accuracy in capturing underlying patterns in wireless communications, making it less suitable for accurate traffic modeling and prediction.

The second type of methods are parametric methods, Parametric methods, like ARIMA [5], use statistical tools for wireless traffic prediction, but struggle with stochastic components. Researchers also explore  $\alpha$ -stability models, entropy theory, and covariance functions for better capturing complexity. Nonparametric methods, especially deep neural networks [6], show promise in wireless traffic prediction. Studies propose wireless mesh network prediction using deep belief networks and a hybrid deep learning framework [7] for spatiotemporal dependencies.

In this study, we use longitudinal federated learning and split learning for improved inter-domain model migration. This approach handles traffic variations better, leading to more accurate and optimized predictions.

Our research focuses on network traffic prediction and differs from existing work. We propose a new framework that uses a distributed architecture and a federated learning approach to address this problem. In this way, we provide a more efficient solution.

## 3 Preliminary Knowledge

In vertical federated learning (VFL), multiple parties collaboratively train machine learning models using the same set of users but different features, while preserving data privacy and model parameters. VFL enables each participant to maintain its data and model locally, exchanging intermediate computational results without sharing raw data or model information during the inference process. This collaborative inference approach promotes the utilization of data resources, benefitting companies or organizations with limited and fragmented data seeking data partners.

The specific definitions are as follows:

Assume that there are  $K$  data holders collaborate to train a machine learning model and they hold the local privacy data  $\{D_1, \dots, D_k\}$ .  $D = \bigcup_{i=1}^K D_i$  denotes the data that all can be aligned. The feature space is represented as  $X$ , and the label space is expressed as  $Y$ . The sample ID space is represented as  $I$ , and  $D_k \triangleq (X_k, Y_k, I_k)$ . The VFL system assumes  $N$  alignable samples  $D$ ,  $D \triangleq \{(x_i, y_i)\}_{i=1}^N$ . Training a joint machine learning model, the label information of the  $K$ -th party is  $y_i = y_{i,K}$ . Each feature vector  $x_i \in R^{1 \times d}$ . Distributed among  $K$  participants  $\{x_{i,k} \in R^{1 \times d_k}\}_{k=1}^K$ ,  $d_k$  is the dimension of the data characteristics of the participant with ID  $k$ . The goal is to use dataset  $D$  to

collaboratively train machine learning models while preserving the privacy of local data and models. The loss function is defined as follows:

$$\min_{\Theta} l(\Theta; D) \triangleq \frac{1}{N} \sum_{i=1}^N f(\Theta; x_i, y_i) + \lambda \sum_{k=1}^K \gamma(\Theta). \quad (1)$$

## 4 Problem Formulation and Proposed Framework

Given  $K$  base stations, each base station has its own local network traffic data, denoted as  $d_k = \{d_{k1}, d_{k2}, \dots, d_{kz}\}$ , where  $Z$  is the total number of time intervals. Let  $d_{kz}$  be the target to predict, and the wireless traffic prediction problem can be expressed as  $d_{kz} = f(\Theta; d_{k1}, d_{k2}, \dots, d_{kz-1})$ , where  $f$  defines the specific form of the model,  $\Theta$  represents the model parameters. This equation indicates the prediction of target flow  $d_{kz}$  is based on historical traffic data from time intervals  $d_{k1}, d_{k2}, \dots, d_{kz-1}$  along with the model parameters  $\Theta$ . As for the complexity, we take advantage of a sliding window scheme to generate a set of input-output pairs  $\{x_i, y_i\}$  by using part of the historical traffic data as input features, among which  $x_i$  denotes the historical flow data associated with  $y_i$ . Here, we focus only on the problem of one-step ahead prediction.

$\Theta$  represents the shared machine learning model. The co-model can be partitioned into  $\theta_k$  with parameter  $\vartheta_k, k \in \{1, \dots, K\}$ . These individual models act only locally, and the global model is represented as  $F_k$  with  $\psi_k$  as a parameter. The  $k$ th participant who has the label is called the active party and the loss function can be redefined as:

$$f(\Theta; x_i, y_i) = L(F_K(\psi_K; \vartheta_1(x_{i,1}, \theta_1), \dots, \vartheta_K(x_{i,K}, \theta_K)), y_i, K) \quad (2)$$

Global Model  $F_k$  can be the one that needs to be updated using the back propagation method. The VFL scene is consistent with splitNN, where the whole model is divided vertically into different parts.

Our objective is to minimize prediction errors for all  $K$  base stations, achieved by solving for the parameter  $\Theta$ . Actually, we utilize the input-output pairs  $\{x_i, y_i\}$  in the training dataset to train the model and determine the parameter values that minimize prediction errors. By fine-tuning the parameters  $\Theta$ , the model achieves optimal prediction performance on the training data, typically achieved by minimizing the loss function associated with prediction errors. Once the model training is completed, the parameter  $\Theta$  can be utilized for making predictions when provided with new input features. Hence, through the solution for parameter  $\Theta$ , we accomplish the goal of minimizing prediction errors for all base stations and enhance the accuracy of network traffic prediction.

Due to functional variations in urban areas, base station traffic patterns differ significantly from one region to another. Moreover, variations in users' mobility and communication behaviors further contribute to the diversity of wireless service patterns. Consequently, wireless service data originating from different base stations exhibit a high degree of heterogeneity and possess a non-independently and identically distributed (non-iid) nature, which is the most difference from the conventional federation learning algorithms. Nevertheless, through the utilization of our proposed methods and techniques, these obstacles can be surmounted, enabling the attainment of accurate and interpretable models.

The participating training base stations are divided into active and passive sides, the global model is trainable, and the passive-side local model, after training intermediate results, collaborates with the active-side local model to form the global model  $F$  and uses the active-side labels for the next training together.

The first step for the VFL system to start co-training is to align the data from the base stations. After alignment, the participants can use the aligned samples to start training the VFL model and sends the local output to the base station of the active party holding the labels. After obtaining the intermediate result for each participant, the active party  $K$  uses stochastic gradient descent method to update the global model with  $\psi_K^{j+1} = \psi_K^j - \eta_1 \frac{\partial l}{\partial \psi_K}$ , and subsequently, the active party  $K$  computes  $\frac{\partial l}{\partial H_K}$ , and sends it to the other base stations. After receiving the information from the proactive party, the other participants calculate and update of its own local model.

Through the VFL training process, we eventually get the parameters  $\theta_1, \theta_2, \dots, \theta_k$  for the local model and  $\psi_K$  for the global model through a certain number of rounds of iterations.

## 5 Experimental Results and Discussions

We used in our experiments the cellular traffic datasets provided by Telecom Italia. These two datasets record the call details of Milan (MI) in the last two months of 2013. They are among the most commonly used datasets in the field of cellular traffic forecasting. In our experiments, we focus on voice call traffic and Internet service traffic, which are the most common types of cellular traffic in existing networks. Our task is to predict the traffic in week 7 based on the traffic in the first six weeks. In addition, we normalize the traffic data so that we can eliminate scale differences between grids to ensure that the model treats the data fairly across grids.

To ensure generality and reduce computational complexity, we randomly selected 100 base stations in each dataset and conducted experiments on three types of wireless traffic from these base stations. In the experiments, we used the traffic from the first seven weeks to train the prediction model, while the traffic from the last week was used to test the performance of the model. By randomly selecting 100 base stations, we can reduce the complexity of computation and processing while retaining data diversity. Such a sampling method can represent the characteristics of the entire dataset and provide reliable results in the experiments. The training model uses the first seven weeks of traffic data so that the model can learn the patterns and trends of the historical data. We then use the trained model to make predictions for the last week of traffic to evaluate the performance of the model on future data. With such an experimental design, we can verify the accuracy and reliability of the prediction model and provide meaningful results for further analysis and decision making. Also, since we randomly selected 100 base stations, our experimental results can be generalized and can be generalized over the entire dataset.

We use two evaluation metrics, MAE and MSE, to evaluate the effectiveness of the above method.

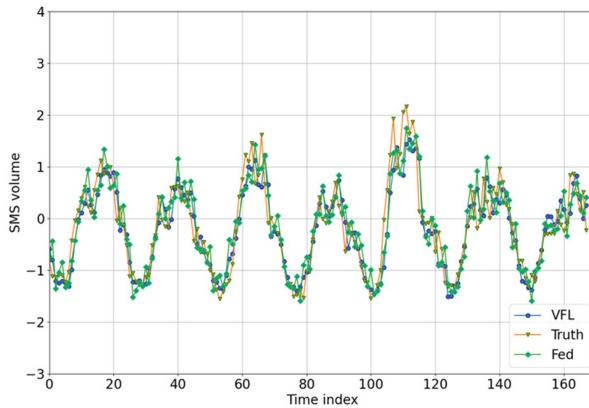
The results from Table 1 and Figs. 1, 2, 3 show that our method has the best prediction results. Compared with only SVR and LSTM, our method captures both spatial and

**Table 1.** Comparison of MSE prediction performance of different methods on Milano dataset.

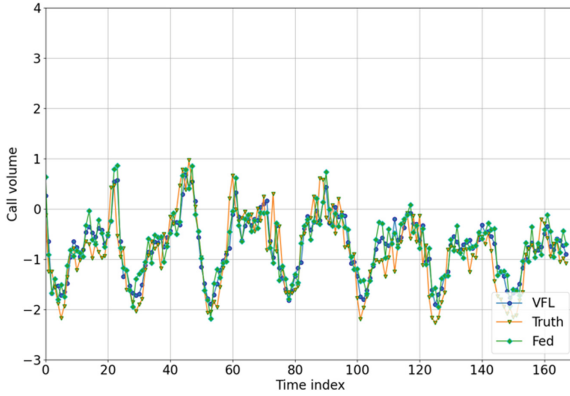
Methods	Milano		
	MSE		
	SMS	Call	Internet
SVR	0.5294	0.1211	0.1252
Lasso	0.8411	0.3215	0.4621
LSTM	0.5922	0.1545	0.1874
FedAvg	0.4853	0.1466	0.1168
VFL	<b>0.3479</b>	<b>0.1023</b>	<b>0.1132</b>

**Table 2.** Comparison of MAE prediction performance of different methods on Milano dataset.

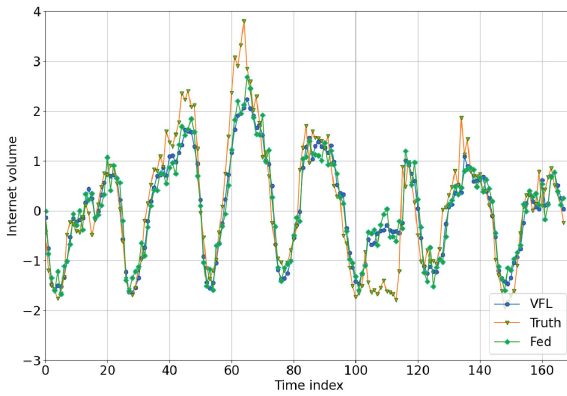
Methods	Milano		
	MAE		
	SMS	Call	Internet
SVR	0.3981	0.2134	0.3120
Lasso	0.7214	0.5162	0.6122
LSTM	0.4721	0.3134	0.3122
FedAvg	0.4176	0.2045	0.3109
VFL	<b>0.3742</b>	<b>0.2101</b>	<b>0.2976</b>

**Fig. 1.** Comparison of predicted and actual values of SMS

temporal dependence through model fusion; our scheme solution greatly reduces the heterogeneity of the data compared with the traditional FL algorithm. As a result, our



**Fig. 2.** Comparison of predicted and actual values of Call



**Fig. 3.** Comparison of predicted and actual values of Internet

method has a high generalization capability and can balance between data from the base station as well as training, thus having more accurate predictions (Table 2).

## 6 Conclusion

Compared with fully distributed algorithms that consider only the temporal dependence of network traffic operations (e.g., SVR and LSTM), our approach can capture both spatial and temporal dependence through model fusion, resulting in greater robustness. Compared to traditional FL algorithms, our approach allows the learning process to be tuned for specific cases. In addition, the application of longitudinal federation greatly reduces the impact of heterogeneity of data. As a result, our method has a high generalization capability and can better adapt to the differences and characteristics among different base stations. Our approach is able to strike a balance between capturing the unique characteristics of base station clusters and the macro traffic patterns shared among different clusters. This allows our method to provide more accurate prediction results

while balancing the specificity of individual base stations with the shared nature of the overall traffic patterns.

**Acknowledgment.** This work was supported by the National Key R&D Program of China (No. 2020YFB1806700).

## References

1. Ke, S., Liu, W.: Distributed multi-agent learning is more effectively than single-agent. (2021). <https://europepmc.org/article/ppr/ppr419060>. Accessed 1 Nov 2022
2. Tran, H., Bao, W., Zomaya, A., Nguyen, H., Hong, S.: Federated learning over wireless networks: optimization model design and analysis. In: 2019 IEEE Conference on Computer Communications (INFOCOM), pp. 1387–1395 (2019)
3. Liu, H., Liu, B., Zhang, H., Li, L., Qin, X., Zhang, G.: Crowd evacuation simulation approach based on navigation knowledge and two-layer control mechanism. *Inf. Sci.* **436–437**, 247–267 (2018)
4. Hyndman, J., Athanasopoulos, G.: *Forecasting: Principles and Practice*. OTexts (2018)
5. Hamilton, J.M.: *Time Series Analysis*, vol. 2. Princeton New Jersey (1994)
6. Nie, L., Jiang, D., Yu, S., Song, H.: Network traffic prediction based on deep belief network in wireless mesh backbone networks. In: 2017 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–5 (2017)
7. Wang, J., Tang, J., Xu, Z., Wang, Y., Xue, G., Zhang, X., Yang, D.: Spatiotemporal modeling and prediction in cellular networks: a big data enabled deep learning approach. In: 2017 IEEE Conference on Computer Communications (INFOCOM), pp. 1–9 (2017)
8. Harvard, D. Italia, T.: Telecommunications-SMS, Call, Internet-MI (2015). <https://doi.org/10.7910/DVN/EGZHFV>. Accessed 5 Nov 2022
9. Jiang, W.: Cellular traffic prediction with machine learning: a survey. *Expert Syst. Appl.* **201**, 117163 (2022)





# Design and Implementation of SRv6 Routing Module in Computing and Network Convergence Environment

Jing Gao, Wenkuo Dong, Lei Feng, and Wenjing Li

Beijing University of Posts and Telecommunications, Beijing 100876, China  
wjli@bupt.edu.cn

**Abstract.** In the computing network convergence environment, the deployment and scheduling of the service function chain put forward high requirements for network flexibility, and the traditional network architecture is difficult to support highly flexible network scheduling functions. SRv6 has become an important way to implement service function chain technology because of its segment routing function and protocol expansion ability. This paper first introduced the technologies such as SRv6 and P4 and many tools used in the implementation process. Then, the detailed design of SRv6 routing module based on P4 is introduced in detail, including the key technologies such as using P4 Match-Action abstraction to identify and parse SRv6 messages, add and delete SRv6 header, segment routing forwarding behavior based on SRH, as well as the automation and parameterization design of SRv6 segment routing to facilitate deployment and verification experiments, and the tracking packet path analysis method in virtual environment based on the secondary encapsulation of Mininet log function. Finally, the function of the designed SRv6 routing module is demonstrated by simulation experiments.

**Keywords:** SDN · SRv6 · Segment routing

## 1 Introduction

With the continuous development of computer network technology, the continuous improvement of computer computing power, and the increasing demand for flexibility in network functions in modern industry, traditional network architectures are struggling to support existing requirements. In addition, in the context of computing network integration, the scheduling of computing power in the network requires high network flexibility [1]. Therefore, the scheduling problem of computing power highly relies on flexible and programmable network scheduling strategies. How to build a highly flexible network has become an urgent issue for both academia and industry to explore. To solve these problems, new generation network technologies such as SDN, NFV, and data plane programmable technology have emerged [2]. These technologies greatly improve the flexibility of the network, allowing traditional network functions to break free from the constraints of network hardware and gain new vitality.

Service Function Chain (SFC) is a technology that provides orderly services to the application layer. SFC is used to logically connect services on network devices, forming an orderly service composition. SFC adds business chain path information to the original message to enable the message to pass through the service device in sequence according to the specified path [3]. Due to the limitations of traditional network devices, the deployment of service function chains highly relies on network devices. However, with the rise of network programmable technology, SFC technology can place network functions or services on general-purpose programmable networks or computing devices, thus preliminarily solving the problem of tight coupling with network hardware [4].

SRv6 (Segment Routing IPv6) utilizes the large address space of IPv6 addresses, combined with segment routing ideas, to conveniently plan routing routes for network packets [5]. By using SRv6's segment routing technology, control packets sequentially flow through various network functional nodes to achieve SFC, becoming an important way to achieve SFC. Through this, SFC has achieved further development, not only breaking free from hardware limitations but also further improving its flexibility in scheduling function chains [6].

In programmable network technology, an important implementation method is to use the protocol-independent programming language P4 (Programming Protocol independent Packet Processors) to define data plane behavior. It uses the Match Action model to highly abstract network functions, allowing network functions to be defined using a unified programming model. The PISA (Protocol Independent Switch Architecture) architecture that supports the P4 definition can achieve high throughput due to its high-speed pipeline design. If we consider implementing SRv6 and network functions on the PISA data plane, it will greatly improve the performance of packet processing [7].

This article first explores the technical support related to the design and simulation of routing modules. Afterward, this article introduced the requirement analysis, functional design, and implementation of the SRv6 routing module in a computing network integration environment, and finally demonstrated the system.

## 2 System Functional Requirement Analysis

### 2.1 Functional Requirements Analysis of IPv6 Routing Submodule

SRv6 implements segment routing based on the IPv6 forwarding plane, which means that the routing module should have basic IPv6 forwarding capabilities. The module needs to ensure that for any segment route within the network, the corresponding routing capability should be available on each router node. In this way, packets can be transmitted smoothly through the network, thus realizing efficient and reliable communication.

To support large-scale and scalable routing table definitions, the routing table design should consider using exact matching as much as possible to streamline the design of routing table construction. At the same time, to better support different application scenarios in the network, the routing definition should be as uniform as possible, with strong regularity of route forwarding behavior.

## 2.2 Functional Requirements Analysis of SRH Submodules Added or Deleted in SRv6

SRv6 TE emphasizes the operation of adding or deleting SRH on the port, which means that the router needs to have corresponding functions to support this operation. The core requirements of this submodule include the following.

The router needs to be able to determine whether the route supports adding or deleting SRH functions by configuring an SRH flow table for the route. In this way, the router can decide whether to add or delete SRH operations to the data packets based on the actual situation. If the router supports the SRH addition and deletion function, the router can generate SRH of different lengths for packets based on the data in the flow table. In this way, the data packet can carry SRH information of different lengths according to actual needs. If a packet has an SRH but no SID, it needs to be deleted to expose the original IPv6 packet. In this way, data packets can continue to be transmitted in the network without being affected by SRH. When assembling SRH, it is necessary to retain the original destination address in the package. In this way, when deleting SRH, the data packet can be restored to its original state and continue to be transmitted in the network.

## 2.3 SRv6 Segment Route Forwarding Submodule Functional Analysis

SRv6 Segment Route Forwarding emphasizes the act of checking SIDs and performing the appropriate network functions on routes that support SRv6 functionality. This means that the router needs to have the appropriate functionality to support this operation. The core requirements for this sub-module include the following.

The router needs to be able to determine whether the route supports segment route forwarding and network functions on the chain by being able to check its own SID. In this way, the router will be able to decide whether or not to segment route forward packets and perform the appropriate network functions, depending on the actual situation. If the router supports the ability to check its own SID, the route should be able to support segment route forwarding behavior. In this way, packets can be transmitted smoothly in the network, thus realizing efficient and reliable communication. If the router supports the ability to check its own SID, the route should be able to support checking the SID to perform the corresponding network functions. In this way, packets can perform the corresponding network functions according to the actual needs, thus satisfying the needs of the functional chain. SRv6 segment route forwarding emphasizes the behavior of checking SIDs and performing the corresponding network functions on the routes that support the SRv6 function. This requires the router to have the appropriate functions to support this operation. These features include determining whether a route supports segment route forwarding and the network functions on the chain, support for segment route forwarding behavior, and support for checking SIDs to perform the corresponding network functions.

Auxiliary functions mainly include message parsing, Layer 2 forwarding function, and southbound interface support. The message parsing part needs to design an efficient and reliable state machine to parse Ethernet, IPv6, and SRv6 packet headers; the Layer 2 forwarding support part needs to realize the function of checking the Mac address and blocking the interference of other packets that have nothing to do with the routing of

SRv6 segments; and the southbound interface mainly interacts with the control plane to receive configuration information.

### 3 Design and Implementation of Main Functions of the System

The main functions of the system include two main parts: the definition of routing behavior and the construction of automatic flow table.

#### 3.1 Routing Behavior

Because the technical implementation of SRv6 depends on traditional IPv6 forwarding, all routing behaviors also include two parts, namely, conventional IPv6 forwarding logic and support for SRv6 segment routing. This section makes a theoretical analysis and overall design of the two kinds of routes respectively.

##### (1) Parser Design

The core of the design of Parser is to use self-loop to parse Segment List. If the parsed SID is found to be the last, the Optional TLV will be parsed down, otherwise, the SID will continue to be parsed. Figure 1 presents the Parser parsing packet header state machine.

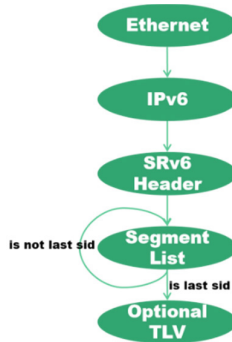


Fig. 1. Parser parsing packet header state machine.

##### (2) IPv6 forwarding logic

IPv6 forwarding logic is the traditional route lookup strategy of the Longest prefix match. Use IPv6 Destination Address to find the key, and use the next hop's Degree Port as the value to construct the Routing table. When forwarding, the Mac address will be updated and the forwarding exit will be recorded, and each hop will cause the TTL (which should be the hop limit field in IPv6) to decrease by one. Extract the Match Action logic from this.

Use IPv6 dest address as the Match Key for lpm, and use the dest Mac Address and Egress Port as values to construct a Match Table. If the query is successful, perform the corresponding update operation. The Match Action abstraction is shown in Fig. 2.

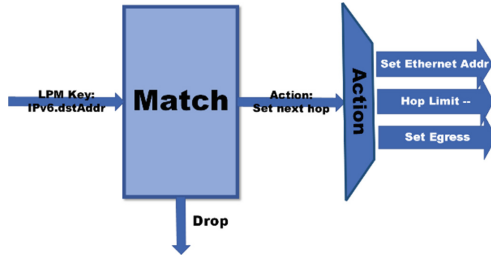


Fig. 2. Abstract principle of IPv6 routing forwarding match action.

For the convenience of debugging design, Default route forwarding is not configured. If there is no suitable match in the Routing table, it should be discarded directly to reduce unnecessary traffic.

**(3) Assemble and delete the Segment List**

The data plane will assign a segment list to packages without a segment list. There are many ways to define the content of a specific segment list. Here, we select the IP destination address as the identifier to obtain the segment list. Afterward, multiple Actions are used to divide different segment list assembly lengths. Figure 3 shows the Match-Action abstract principle for assembling the SRH part of SRv6.

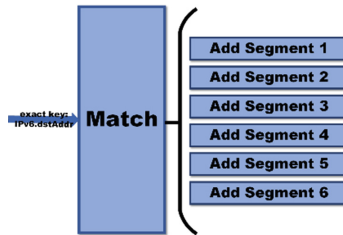


Fig. 3. Abstract Principle of Match Action for Assembly of SRH Part in SRv6.

**(4) Mac address matching**

Routers need to provide a MAC address detection mechanism for each node, and each router will only process packets with the destination MAC address identified as its own. If it matches, execute NoAction.

**(5) Overall behavior**

The overall behavior refers to integrating the functions of all network functional modules, connecting the behavior of several modules in series, and providing a control mechanism to control different routes to execute different network functions in the same configuration. Figure 4 is the routing behavior design flowchart.

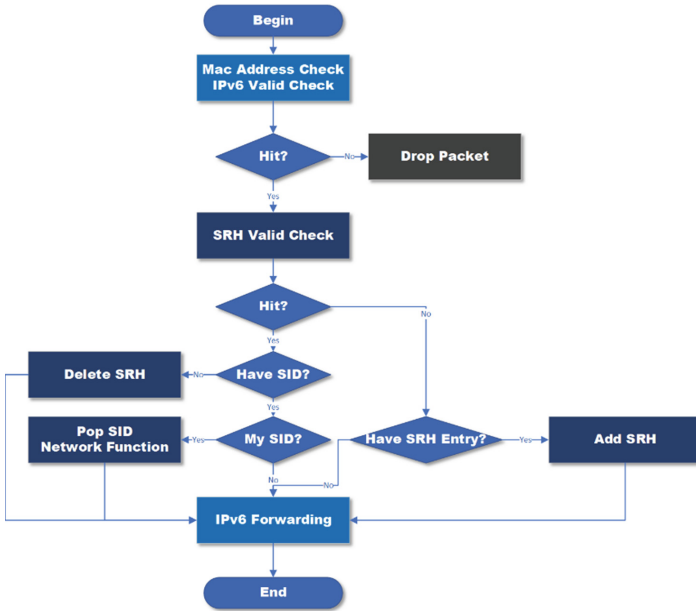


Fig. 4. Routing behavior design flow chart.

### 3.2 Flow Meter Design

#### (1) Topological structure of flow table reference

This section defines a unified topology consisting of 25 routers. All routers support IPv6 forwarding. Four of them provide the function of checking SID, called intermediate nodes. These four switches not only check SID but also provide the function of adding segment lists, known as boundary routers. In the design, one host is connected to each boundary router for testing. Figure 5 shows the network topology structure.



Fig. 5. Network topology structure.

#### (2) IPv6 flow table design

The Routing table of IPv6 mainly has two aspects: one is the Routing table between routers to realize segment routing, and the other is the Routing table from router to host.

First is the Routing table between routers. In a square topology, the mapping relationship between port numbers and directions is shown in Fig. 6.

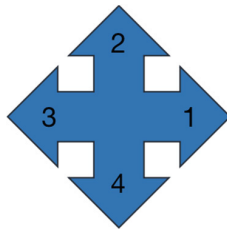


Fig. 6. Mapping relationship between port number and direction.

When there are multiple routes to choose from, define the forwarding priority for the forwarding port. If the target address is below the current address, the router will prioritize sending to the router below, followed by the right, then the top, and finally the left. In short, teleport as far down as possible to the right. Define all routing information between routers through this method.

Subsequently, the router-to-host routing is defined, and the host's routing comes from the routing information between routers. On the one hand, if the router is not connected to the host, the router to which the host is connected should be found, and the route to the connected router should be directly configured to that router; On the other hand, if the router is connected to a host, it is necessary to find the corresponding port that connects to the host and configure the route to that router. After configuring all necessary routes, integrate them into JSON and send them to each router, and all the basic IPv6 routing configuration work is completed.

### (3) SRv6 Flow Table Design

Number the routers that need to support the addition and deletion of SRH and segment routing intermediate nodes in sequence. Figure 7 shows the relationship between SRv6 routing numbers and overall routing.



Fig. 7. Relationship between SRv6 route number and overall route.

These numbers can describe the segment routing behavior between boundary routers. Define segment routing between each boundary router using a simple data structure. Subsequently, the developer parsed the path data structure into a router-readable configuration table JSON format.

### (1) Configuration distribution

All routers support the same routing behavior and IPv6 forwarding behavior, and the behavior configuration and IPv6 routing need to be distributed to all routing nodes. Use a flow table to control whether the router supports SRH assembly and segment routing forwarding functions. The target for issuing SID check flow table items supports SRv6 segment routing forwarding operations, represented in dark blue and black; The distribution target of SRH flow table items supports the SRH assembly deletion function, represented in dark blue. A detailed schematic diagram is shown in Fig. 8.

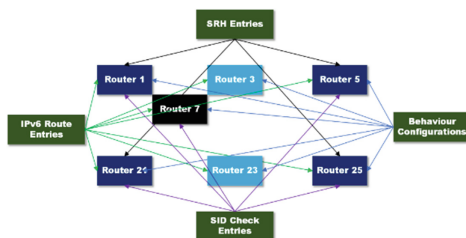


Fig. 8. Configuration and flow table distribution target

## 4 System Function Display

### 4.1 Automated Script Construction

The core idea of the automated build script is to use Python's loop and lists to concisely describe the repeated json structure.

#### (1) Topology building script design

The topology building script is named `gen_topo.py`, which is mainly used for the automated construction of predefined json format topo definition files in the environment. Firstly, construct four hosts and define their Mac addresses for each of them. The Mac address of the host and the Mac address of each router are described in Python language.

The same applies to the construction of routers. The main task of topology construction is to build the connection relationship between routers and routers, as well as between routers and hosts.

#### (2) Design of script for automated flow table construction

Automated flow table construction includes json format definition and address definition. The json format definition and address definition sections are located in the `entry_The` format.py file is mainly used to mask the parts related to json format and address format conversion, providing a concise calling interface for the high-level flow table design part. The code is as follows:



```

for switch in ipv6_routes:
  for route in ipv6_routes[switch]:
    dst_switch = route[0]
    interface = route[1]
    next_hop_switch = route[2]
    add_entry(switch,
      e.ipv6_routing_table_entry(
        ipv6_switch(dst_switch, interface),
        mac_router(next_hop_switch, dst_interface_dict[interface]),
        interface
      )
    )
  )
)

```

### 4.2 System Demonstration

#### (1) Detailed effects of individual use cases

Select the segment route from h1 to h4 and select it in gen\_ The route from h1 to h4 is defined as follows in entry.py:

(1, 8): [3, 4, 6, 8]		
----------------------	--	--

Here, 3, 4, 6, and 8 represent SRv6 segment routing markers, corresponding to router IDs 7, 9, 19, and 25.

Open Mininet, enter the following command to start Mininet’s simulation system, and determine which routers its routes have passed through. This path should be drawn in Fig. 9 as follows: red represents the segment routing path, and blue represents the actual path.

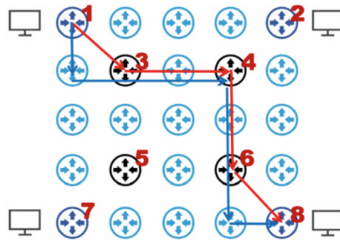


Fig. 9. Path diagram of this use case.

At this point, the system has successfully implemented the segment routing function from h1 to h4. It passed through SRv6 routers 3, 4, 6, and 8 in sequence.

#### (2) Detailed test results

Analyze the detailed test results in a Table 1.

The following two important features can be seen in the experimental results (Table 2):

**Table 1.** Correspondence between SRv6 router IDs and global router IDs.

1	2	3	4	5	6	7	8
1	5	7	9	17	19	21	25

**Table 2.** Detailed experimental results.

Source and destination	Segment routing	Actual path through the router
1, 2	5, 4, 2	<b>1, 6, 11, 16, 17, 18, 19, 14, 9, 10, 5</b>
1, 3	3, 5, 7	<b>1, 6, 7, 12, 17, 22, 21</b>
1, 4	3, 4, 6, 8	<b>1, 6, 7, 8, 9, 14, 19, 24, 25</b>
2, 1	4, 5, 1	<b>5, 10, 9, 14, 19, 18, 17, 12, 7, 2, 1</b>
2, 3	3, 5, 7	<b>5, 10, 9, 8, 7, 12, 17, 22, 21</b>
2, 4	3, 4, 8	<b>5, 10, 9, 8, 7, 8, 9, 14, 19, 24, 25</b>
3, 1	3, 4, 1	<b>21, 22, 17, 12, 7, 8, 9, 4, 3, 2, 1</b>
3, 2	6, 4, 2	<b>21, 22, 23, 24, 19, 14, 9, 10, 5</b>
3, 4	6, 8	<b>21, 22, 23, 24, 19, 24, 25</b>
4, 1	5, 1	<b>25, 20, 19, 18, 17, 12, 7, 2, 1</b>
4, 2	5, 2	<b>25, 20, 19, 18, 17, 18, 19, 20, 15, 10, 5</b>

- (a) The serial number always changes in the direction of increasing as much as possible. For example, when routing from 1 to 17, 1 will prioritize routing to 6 instead of 2.
- (b) The route will pass through the configured segment routing nodes in sequence, rather than directly routing to the destination address.

These two features successfully reflect the design of IPv6 routing priority and segment routing in the flow table design.

## 5 Conclusion

This paper researched how to use P4 and its supporting environment to simulate the entire data plane to realize the routing function of SRv6 segment. The interconnection scheme between routers is clearly described by constructing a checkerboard topology. The forwarding behavior of SRv6 is defined using the Match Action abstraction of P4. Then we use the Python script to automate the construction of the flow table for each router. Finally, the debugging is started by sending packets between hosts, and the complete debugging information presents the final segment routing effect.

**Acknowledgement.** This work is supported by National Natural Science Foundation of China (U22B2031).

## References

1. McKeown, N., Anderson, T.: OpenFlow: enabling innovation in campus networks. *ACM SIGCOMM Comput. Commun. Rev.* **2018**(38), 69–74 (2018)
2. Bosshart, P., Gibb, G., Varghese, G.: Forwarding metamorphosis: fast programmable match-action processing in hardware for SDN. *ACM SIGCOMM Comput. Commun. Rev.* **2013**(43), 99–110 (2013)
3. Giesen, H., Shi, L., Sonchack, J.: In-network computing to the rescue of faulty links. In: *Proceedings of the 2018 Morning Workshop on In-Network Computing* (2018)
4. Sun, Z., Mo, Y., Yu, C.: Graph reinforcement learning based task offloading for multi-access edge computing. *IEEE Internet of Things J.* (2021)
5. Xie, Y.: Virtualized network function forwarding graph placing in SDN and NFV-enabled IoT networks: a graph neural network assisted deep reinforcement learning method. *IEEE Trans. Netw. Serv. Manag.* **19**(1), 524–537 (2022)
6. Sadeeq, M., Abdulkareem, N.: IoT and Cloud computing issues, challenges and opportunities: a review. *Qubahan Acad. J.* **1**(2), 1–7 (2021)
7. Baykara, M.: A centralized honeypot-based security approach using software-defined switching for secure management of VLAN networks. *Turk. J. Electric. Eng. Comput.* **27**, 3309–3325 (2019)



# Reliable and Efficient Routing Management Mechanism for Power Communication Network Based on Multi-party Cooperation

Zhongmiao Kang<sup>1</sup>, Donghai Huang<sup>1</sup>, Yuben Bao<sup>1</sup>, Peiming Zhang<sup>1</sup>,  
and Jiewei Chen<sup>2</sup>✉

<sup>1</sup> Electric Power Dispatching Control Center of Guangdong, Power Grid Co., Ltd.,  
Guangzhou 510600, China

<sup>2</sup> State Key Laboratory of Networking and Switching Technology, Beijing University of Posts  
and Telecommunications, Beijing 100876, China  
chenjiewei@bupt.edu.cn

**Abstract.** SDN technology brings the advantages of improving resource utilization and management efficiency to the network, and at the same time, it poses new challenges to the reliable operation of the network. In order to solve the problem of data forwarding error caused by network equipment attack, this paper proposes a multi-party cooperative routing management mechanism for power communication network. In order to achieve a reliable and efficient routing mechanism, a routing management platform architecture is designed according to the characteristics of the network. The architecture includes four types of devices: blockchain, centralized management center, SDN controller and repeater. In the routing table generation stage, a blockchain-based routing table audit mechanism is proposed. In the routing table execution phase, a routing table detection mechanism based on active detection is proposed. In the performance analysis, from the two dimensions of blockchain management routing table, centralized management center and SDN controller collaboration, it is verified that the mechanism in this paper has good performance in improving routing reliability and efficiency.

**Keywords:** Power communication network · Route management · SDN controller · Blockchain

## 1 Introduction

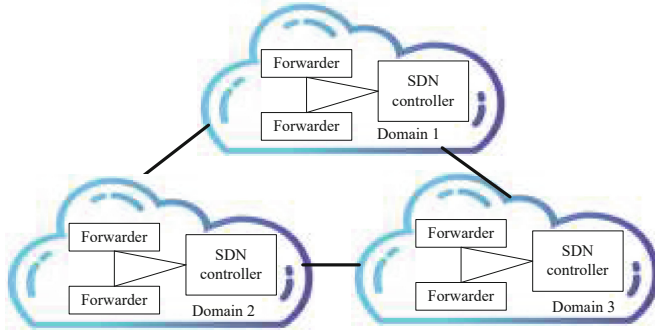
With the maturity and development of virtualization technology, software definition network (SDN) technology has been supported and recognized by equipment manufacturers and network operators [1]. At present, most power companies have adopted SDN technology to build power communication network. After the adoption of SDN technology, the network equipment has changed from the original single hardware equipment resource to SDN controller and forwarder [2]. The SDN forwarder is responsible for the data forwarding function, and the SDN controller is responsible for the data control function. Since network reliability is an important indicator of user satisfaction,

the current network reliability mechanism has become a research focus. Literature [3] adopts the route segmentation strategy and proposes the network application-aware segmented routing strategy, which solves the problem of low routing performance of SDN networks in large-scale environments. Literature [4] adopts blockchain technology to reduce the negative impact of DDoS attacks on SDN network performance. Literature [5] takes network routing performance as a parameter to evaluate cloud service providers and proposes optimization objectives for routing management. Literature [6] adopts a routing conversion strategy to solve the problem of routing interoperability between traditional networks and SDN networks. Literature [7] uses convolution neural network theory to monitor network traffic, improving the monitoring efficiency of abnormal traffic. Literature [8] proposes a real-time computing model to monitor network data frames, effectively solving the problem of low reliability of time-sensitive networks.

Through the analysis of existing research, researchers have accumulated a variety of research results to improve network reliability. However, in the SDN environment, the routing generation and routing execution devices are separated and executed by the controller and the forwarder respectively, posing new challenges to the reliability of the network. In order to solve the problems of path transmission interruption or flow rule tampering caused by network device denial of service, this paper proposes a reliable and efficient routing management mechanism for power communication network based on multi-party cooperation. In the performance analysis, it is verified that this mechanism can achieve the reliability and efficiency of routing.

## 2 Problem Description

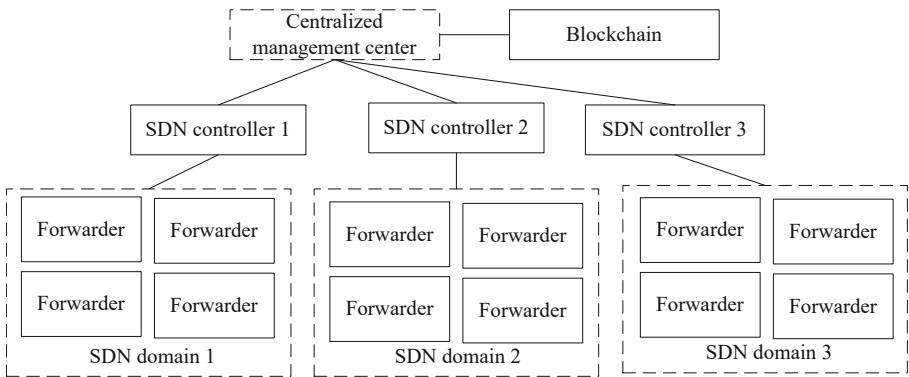
The power communication network architecture is shown in Fig. 1. This architecture is a power communication network built with SDN technology. As the type and quantity of services carried by the power communication network are increasing, the coverage of SDN network is also increasing. In order to meet the efficient management of SDN network equipment in a large range, the multi-domain management mechanism has become a common technology in SDN network management. Figure 1 is a schematic diagram of power communication network composed of three SDN domains. From the figure, each SDN domain includes one SDN controller and multiple forwarders. The function of SDN controller is to realize the generation of data forwarding flow table and the summary and analysis of the execution results of the forwarder. It undertakes the function of data forwarding control. The function of the forwarder is to forward the data according to the flow table issued by the SDN controller. It undertakes the function of data forwarding. Therefore, in the SDN network environment, the network control and data forwarding functions of the power communication network are divided into two types of devices, which significantly improves the efficiency of network management and reduces the investment of network resources.



**Fig. 1.** Power communication network architecture

### 3 Routing Management Platform Architecture

In order to achieve a reliable and efficient routing mechanism, a routing management platform needs to be designed according to the characteristics of the network. The platform needs to meet the two basic requirements of SDN network characteristics and support for routing management. To meet these two requirements, this paper designs a routing management platform architecture as shown in Fig. 2. The architecture includes four types of devices: blockchain, centralized management center, SDN controller and repeater. It can be seen from the figure that the SDN controller and transponder adopt the strategy of sub-domain management. This sub-domain management strategy can meet the needs of the reality of the growing network size. Each module is described in detail below.



**Fig. 2.** Architecture of routing management platform

The centralized management center is responsible for the centralized management of routing tables. The blockchain node is responsible for auditing and saving the routing table. The centralized management center is connected with the blockchain node and SDN controller. In terms of the interaction between the centralized management center

and the blockchain nodes, it mainly completes the submission of the routing table and the query of the routing table. In terms of routing table submission, the centralized management center obtains the routing table from the SDN controller and submits it to the blockchain node for consensus and storage. In the aspect of routing table query, the centralized management center obtains reliable routing tables from the blockchain nodes, so as to analyze the routing information and forwarding actions reported by the forwarder, and determine the consistency of the routing table and forwarding actions. In terms of the interaction between the centralized management center and the SDN controller, it mainly includes two functions: the aggregation of the initial routing table and the aggregation of the routing table execution results. In terms of initial routing table aggregation, the main function is to collect SDN routing tables. In the aspect of routing table execution result aggregation, the main function is to achieve the aggregation of repeater execution results.

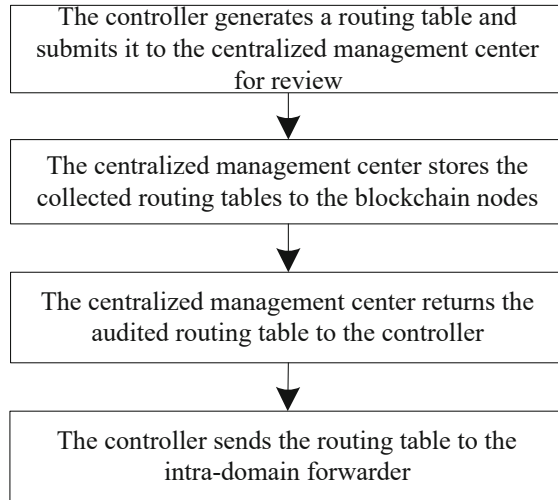
## 4 Routing Management Mechanism

In terms of the life cycle of the routing table, it generally includes three steps: generation, optimization and deletion of the routing table. When network equipment is attacked by virus or fails, unreliable or inefficient problems will occur at all stages of the routing table life cycle. In order to solve this problem, the routing management mechanism proposed in this paper is divided into two parts: routing table generation phase management and routing table execution phase management. Among them, the management of route table generation phase is mainly related to the route management of route table generation. The route table execution phase management mainly corresponds to the route management work of route table optimization and deletion. The two mechanisms are described in detail below.

### (1) Mechanism of route table generation stage

In the generation stage of routing table, the main strategy to achieve the reliability and efficiency of routing is the audit of routing table. In the generation stage of routing table, the common routing problems are routing loop and duplicate routing. To achieve the reliability and efficiency of routing tables, this paper proposes a blockchain-based routing table audit mechanism. The blockchain-based routing table audit mechanism is shown in Fig. 3. The mechanism includes four steps: the controller generates the routing table and reports it to the centralized management center for audit, the centralized management center stores the collected routing table to the blockchain node, the centralized management center returns the audited routing table to the controller, and the controller sends the routing table to the intra-domain forwarder. The mechanism is described in detail below.

The steps of generating a routing table in the controller and reporting it to the centralized management center for review mainly include the following three sub-processes. First, the controller formulates a new routing strategy according to the network request. Secondly, the controller generates a new routing table according to the new routing strategy. Finally, the controller reports the generated routing table to the centralized management center for review.



**Fig. 3.** Routing table audit mechanism based on blockchain

The steps of storing the collected routing tables to the blockchain nodes in the centralized management center mainly include the following four sub-processes. First, the centralized management center formats the relevant attribute information of the collected flow table, generates a transaction information, and packages it to the blockchain system. Secondly, the blockchain system uses the consensus mechanism of voting to invite each blockchain node to verify the consensus of the transaction. Thirdly, each blockchain node performs consensus verification. First, the blockchain identifies duplicate routing tables. If duplicate routing tables are found, delete them. Secondly, identify the routing table of the loop. If a routing loop is found, a pruning algorithm is used to remove the routing loop. Finally, the blockchain node saves the verification results and returns them to the centralized management center.

In the centralized management center, the audited routing table is returned to the controller step. The centralized management center updates the routing data of the controller according to the latest routing table data, so as to feed back the latest routing table for the controller.

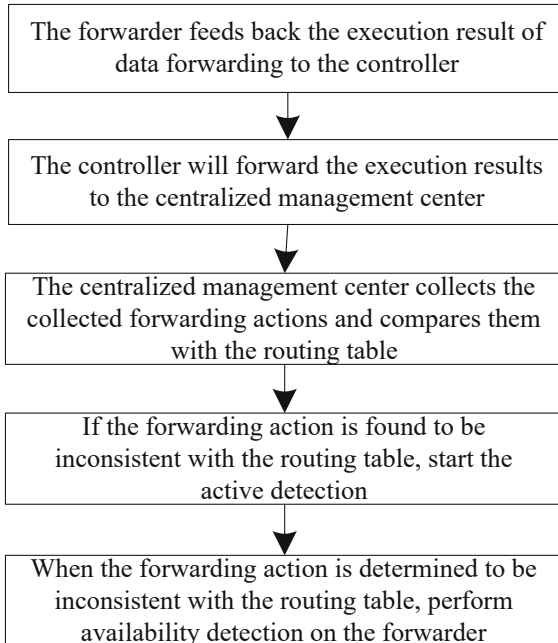
The controller sends the routing table to the intra-domain forwarder, mainly including the following two sub-processes. First, when the controller sends the routing table to the intra-domain repeater, the forwarding rule of “feedback forwarding action to the controller” is added. Secondly, the forwarder forwards the data according to the routing table, and forwards the data to the controller according to the feedback requirements.

## (2) The mechanism of routing table execution stage

In the execution stage of routing table, the main strategy to achieve the reliability and efficiency of routing is the detection of routing table. In the execution stage of the routing table, the common routing problems are that the controller or forwarder is attacked and the routing is wrong. To achieve the reliability and efficiency of the routing table, this paper proposes a routing table detection mechanism based on active detection, as shown



in Fig. 4. This mechanism includes five steps: the forwarder feeds back the execution results of data forwarding to the controller, the controller feeds back the execution results of data forwarding to the centralized management center, the centralized management center collects the collected forwarding actions and compares them with the routing table, starts the active detection when the forwarding actions are found to be inconsistent with the routing table, and performs the availability detection on the forwarder when the forwarding actions are determined to be inconsistent with the routing table. The mechanism is described in detail below.



**Fig. 4.** Routing table detection mechanism based on active detection

The execution result step of feedback data forwarding from the forwarder to the controller mainly includes the following two sub-processes. First, the transponder organizes and reports data content, including business attribute information, route association information, and data attribute information. Secondly, the forwarder feeds back the data forwarding results to the controller, including whether the data is compressed, encrypted, forwarding delay, forwarding quantity and other information. After the controller feeds the execution results of forwarder back to the centralized management center, which collects the data of the controller, it uses the data preprocessing strategy to analyze and gather the data. The analyzed and processed data mainly includes the identification of the controller, the identification of the transponder it contains, and the routing table of the region. In the centralized management center, collect the forwarding actions and compare them with the routing table, which mainly includes the following three sub-processes. First, the centralized management center uses the data aggregation strategy

to analyze and process the data reported by multiple controllers. The strategy of data aggregation can sort the forwarding actions according to the relationship before and after the routing, and improve the efficiency of data processing. Secondly, the centralized management center downloads the routing table from the blockchain and compares it with the routing table uploaded by the controller. If the same, the controller is normal. Otherwise, the controller has been attacked or failed. Finally, compare the data aggregation results with the routing table. The string-matching algorithm can be used. When the forwarding action is found to be inconsistent with the routing table, the active detection step is started, and the active detection technology is mainly used to obtain the uncertain data. During active detection, it is necessary to determine the source node and destination node according to the uncertain data content, and use the shortest path detection technology to detect. When the forwarding action is determined to be inconsistent with the routing table, the availability detection step is performed for the forwarder, which mainly includes the following two sub-processes. First of all, determine the transponder information that is suspected to have a problem according to the location where the forwarding action is inconsistent with the routing table. Secondly, perform availability detection on the suspected transponder to confirm whether the transponder is attacked by virus and whether it is available.

## 5 Performance Analysis

When analyzing the performance of improving the reliability and efficiency of routing, we analyze it from two dimensions: blockchain management routing table, the collaboration of centralized management center and SDN controller.

Using blockchain to manage routing tables can improve routing reliability and efficiency. The blockchain manages the routing table and realizes the generation, optimization and saving of the routing table. In the generation and optimization stage of the routing table, adopting the consensus mechanism of the blockchain can effectively avoid the occurrence of repeated routing and routing loops, and improve the quality and reliability of the routing table. In the saving stage of the routing table, using blockchain to save the routing table can prevent the routing table from being tampered with. Based on the routing table saved in the blockchain, the centralized management center can compare the routing table of the controller with the routing table in the blockchain, quickly understand the authenticity of the routing table, and improve the efficiency of routing table management.

The use of the collaboration of centralized management center and SDN controller can improve the reliability and efficiency of routing. During the generation of routing tables, the centralized management center and SDN controllers can work together to gather and check the routing tables generated by multiple SDN controllers to find duplicate routes and routing loops, thus improving the quality of routing tables. In the process of routing table execution, the centralized management center cooperates with the SDN controller to efficiently manage the routing table execution process from four aspects: routing table distribution, routing table execution result feedback, routing execution result aggregation, and routing execution result verification, ensuring the quality and safety of routing table execution.

Therefore, the routing management mechanism in this paper improves the efficiency and reliability of routing management from two dimensions: blockchain management routing table, centralized management center and SDN controller collaboration. To sum up, from the analysis of the mechanism of the route table generation stage, we can see that this mechanism uses the centralized management center to implement centralized management, and takes effective measures to remove routing loops and duplicate routes, thus improving the routing execution efficiency. From the analysis of the routing table execution stage mechanism, we can see that this mechanism adopts effective measures such as blockchain, active detection and passive feedback to remove routing loops and duplicate routes and improve the reliability of routing.

## 6 Conclusion

In the SDN environment, the route generation and route execution equipment are separated and executed by the controller and the forwarder respectively, posing a new challenge to the reliability of the network. In order to solve the problems of data forwarding error or route tampering, this paper proposes a reliable and efficient route management mechanism for power communication network based on multi-party cooperation. In the routing table generation stage, the mechanism achieves the reliability and efficiency of routing through the routing table audit policy. In the routing table execution stage, the routing table detection technology is used to achieve the reliability and efficiency of routing. The performance analysis shows that the reliability and efficiency of the mechanism in this paper depend on the accuracy and efficiency of the active detection technology. In the next step, based on the research results of this paper, we will study the detection technology suitable for routing execution strategy, so as to further improve the application value of this mechanism.

**Acknowledgment.** This research was supported by Guangdong power grid project (No.: 036000KK58200002).

## References

1. Dai, B., Xu, G., Huang, B., et al.: Enabling network innovation in data center networks with software defined networking: a survey. *J. Netw. Comput. Appl.* **94**, 33–49 (2017)
2. Sarmiento, D.E., Lebre, A., Nussbaum, L., et al.: Decentralized SDN control plane for a distributed cloud-edge infrastructure: a survey. *IEEE Commun. Surv. Tutor.* **23**(1), 256–281 (2021)
3. Tong, V., Souihi, S., Tran, H.A., et al.: SDN-based application-aware segment routing for large-scale network. *IEEE Syst. J.* **16**(3), 4401–4410 (2021)
4. Sanyal, S., Barai, M.K., Goplani, A.: A novel blockchain based software defined network (sdn) architecture to curb the impact of dos/ddos. **6**(5), 12–24 (2021)
5. Rădulescu, C.Z., Rădulescu, I.C.: An extended TOPSIS approach for ranking cloud service providers. *Stud. Inf. Control* **26**(2), 183–192 (2017)
6. Csikor, L., Szalay, M., Rétvári, G., et al.: Transition to SDN is HARMLESS: hybrid architecture for migrating legacy ethernet switches to SDN. *IEEE/ACM Trans. Netw.* **28**(1), 275–288 (2020)

7. Haider, S., Akhunzada, A., Mustafa, I., et al.: A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks. *IEEE Access* **8**, 53972–53983 (2020)
8. Zhang, P., Liu, Y., Shi, J., et al.: A feasibility analysis framework of time-sensitive networking using real-time calculus. *IEEE Access* **7**, 90069–90081 (2019)



# Blockchain-Based Searchable Encryption Access Control Mechanism for the Internet of Things

Mengyuan Li<sup>1</sup>(✉), Shaoyong Guo<sup>1</sup>, Wengjing Li<sup>1</sup>, Ao Xiong<sup>1</sup>, Dong Wang<sup>2</sup>, Da Li<sup>2</sup>, and Feng Qi<sup>1</sup>

<sup>1</sup> State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, CN, China

{mengyuanli, qifeng}@bupt.edu.cn

<sup>2</sup> State Grid Digital Technology Holding Co., LTD, Beijing 100053, CN, China

**Abstract.** With the rapid development of the Internet of Things, numerous security and trust risks, including a single point of failure for authorities, data tampering, unauthorized users decrypting data, and challenges with searching encrypted data, have emerged on the centralized Internet of Things data sharing platform. As a novel technology, blockchain offers the benefits of decentralization, tamper-proofing, and trusted data sharing. Therefore, this article suggests a blockchain-based searchable encryption access control method. Users can simply search the necessary data using keywords provided they comply with the access rules. To ensure the privacy of the data, the cloud will not get any privacy-related information. The simulation demonstrate that our study has a lower time overhead than the current investigations. Data encryption takes 33% less time than standard access control methods, decryption takes 5% less time, and searching takes 75% less time.

**Keywords:** Blockchain · Searchable encryption · Attribute access control · Privacy protection · Data sharing · Keyword search

## 1 Introduction

The Internet of Things has been widely used in smart cities, smart grids, smart industries, smart homes, smart transportation, and other domains due to its rapid development. The amount of data that Internet of Things terminals produce is increasing, and this data needs to be shared with other Internet of Things terminals and uploaded to the cloud. Technology for cloud storage is also developing, such Tencent Micro Cloud in China and Amazon storage. The integrity of cloud servers, users, and management organizations is the only foundation that traditional data sharing methods can rely on. When these entities have malicious intentions, they cannot protect the security of cloud data. Because users' data may contain sensitive information of users, after users upload their data to the cloud, the cloud may be semi-trustworthy or untrustworthy, [1, 2], and any device can access users' data, resulting in internal storage of third-party service providers can use private data or information for profit [3, 4]. It brings great challenges to users' privacy and

security. In addition, the data uploaded by users to the cloud is often encrypted, which brings great challenges to data search. Therefore, the searchable access control of cloud ciphertext data sharing has become a hot topic.

In order to solve the problem of ciphertext retrieval of access control, searchable encryption can be combined with attribute-based access control methods [5], but there are still many problems to be solved in the current searchable access control scheme. First, the traditional attribute-based searchable encryption method is only applicable when the cloud server and the attribute management agency are honest. In the actual attribute-based access control, users are not sure that the cloud server and the attribute management agency will protect the privacy of users' information and data. Given the threat of malicious attribute management, existing verifiable search schemes do not take effective countermeasures (such as punishing cheaters). For example, the user pays only after verifying the results returned by the cloud server, and the cloud server performs the search operation only after the user pays the service fee. In cases where the server is likely to be malicious, it returns only incorrect or partial results after receiving a fee. At the same time, the data user may be malicious, not paying the service fee, claiming that the returned results are incomplete or incorrect when the returned results are indeed correct. Second, the existing attribute-based searchable encryption scheme consumes a lot of computing resources and energy in the process of data retrieval, which is not low-carbon and environmentally friendly [6].

Blockchain is gaining popularity in many fields due to its advantages such as distributed storage, information transparency, tamper-resistance and effective credit sharing [7]. While blockchain technology can provide an effective and efficient solution to the Internet of Things, there are many challenges to the various aspects of integrating these technologies together. First, data security cannot be guaranteed. After users upload their data, the blockchain will make redundant backup to ensure data availability, but this will increase the risk of user privacy information disclosure. Although the consortium blockchain and private chain introduce the user access mechanism and the data access operation needs authorization, compared with the traditional centralized implementation scheme, the security intensity of blockchain data privacy still restricts the promotion of blockchain in the Internet of things. Therefore, how to protect the data privacy security on the chain is an important issue that needs to be solved. Second, it is the anonymity of users. Pseudo-anonymity is one of the main features of blockchain, which can protect users' identity information to a certain extent. However, the anonymity design of blockchain is not perfect. Most of the current blockchain systems directly associate the user's identity with the public key or other data that can represent the identity, which is prone to privacy disclosure [8]. In addition, blockchain faces integration challenges with security-related system components, smart contracts, storage capacity and scalability, resource utilization, predictability, and legal issues [9]. Therefore, how to solve these problems in the existing Internet of things, so that blockchain can be safely applied in the industrial Internet of things, is a field worth studying.

Aiming at the problems of how to efficiently search cloud ciphertext data, whether cloud, attribute management institutions and users are safe and trustworthy, and how to securely apply blockchain in the access control of the Internet of Things, this paper uses blockchain to record data stored in the cloud related information and data keyword trap.

The ciphertext searching process is transferred from the untrusted cloud to the trusted blockchain, and the searchable encryption method is combined with the attribute-based encryption scheme. When the user's attributes meet the access policy, the data required by the user can be quickly found without revealing any information, and the data privacy is protected while the fine-grained data access control is achieved. This paper focuses on combining searchable encryption and access control in the scenario of Internet of Things data sharing with blockchain technology to evaluate their applicability and efficiency from the perspective of privacy security and response time.

The main contributions of this paper are as follows:

1. Based on blockchain technology, this paper realizes ciphertext data searching based on attribute encryption in the Internet of Things scenario, without exposing any information related to users' identity information and data keywords, so as to protect the privacy of Internet of Things users. By assigning keywords to data, the data owners can realize data confidentiality and fine-grained access control so that users can find the data they need more accurately when searching. At the same time, because the keywords given by the data owners is encrypted, other users do not know the content of the keywords.

2. In order to reduce the computing cost, this paper transfers the computing load of the search to the blockchain network. The keyword of the data is stored on the federated chain, and the users search through the smart contract. This enables the search process to get rid of the constraints of untrusted authorities, realizes the decentralized storage of keywords, and solves the problem of single point of failure. Compared with the existing access control schemes, the simulation results show that the proposed searchable access control scheme takes less time in the encryption, decryption and search phases, and improves the efficiency of access control and information search.

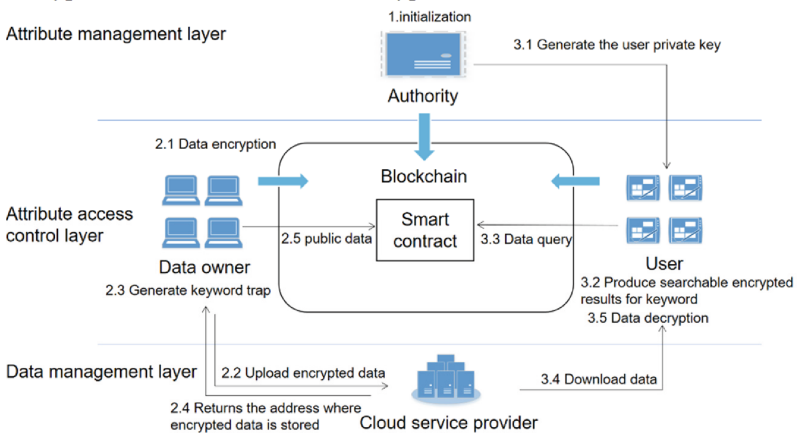
## 2 System Model

As shown in the Fig. 1, the architecture designed in this paper is composed of four logical entities, namely, data owner, user, authority, cloud service provider. Among them, authority is the full node of blockchain, data owner and user is the light node of blockchain. In order to solve data leakage and improve the efficiency of the system, we divided the architecture into three layers: attribute management layer, attribute access control layer and data management layer.

The attribute management layer consists of the authority. The authority manages users' attributes in this way: generate a private key for each user based on the user attributes, and send it to the users in secure transmission mode.

The access control layer is implemented through the blockchain, whose nodes are operated by the authority, data owners and users. Blockchain provides service to users and data owners by publishing smart contract. Users and data owners can query information through the blockchain, such as the encrypted ciphertext of the content secret key, the address of the data stored in the cloud, the access policy of the data, the hash value of the data, and the key of the data.

The data management layer is implemented by the cloud service provider. When the attributes of the user match the access policy and the user's search keyword matches the keyword given by the data owner, the user can obtain the encryption key and obtain the encrypted data from the cloud for decryption.



**Fig. 1.** Architecture of searchable access control system.

The access control process can be divided into the following stages:

### 1. Initialization phase

The authority negotiates public parameters, generates public attribute keys, and builds the blockchain based on these parameters. Authority provides data upload and data acquisition services for data owners and users by publishing smart contracts on the chain.

### 2. Data upload phase

The data owner first hashes the original data to obtain the hash value of the data and assigns a keyword to the data for later query. The data owner generates symmetric encryption keys, encrypts his data using symmetric encryption methods, and also generates his own searchable public and private key pairs and information keyword trap. Then the encrypted data is uploaded to the cloud service provider, and the cloud returns the address that data stored in the cloud. After that, the content secret key is encrypted by the content secret key encryption algorithm, and the encryption results of the encrypted content secret key, the address stored in the cloud, the data access policy, the data hash value, and the data key are recorded on the blockchain. In this way we implement trusted sharing of data.

### 3. Data acquisition phase

After the user registers with the authority, the authority sends the user's private key to the user in a secure transmission channel. The user, as a light node, interacts with the blockchain through the smart contract. The user encrypts keywords and submits query requests to the smart contract. The smart contract compares the encryption result of the user's keywords with the trap of the data owner. Only when the attributes meet the access control policy can the user decrypt the content secret key, and then decrypt the original



data. At the same time, users can verify that the hash value of their data is the same as the hash value of the original data recorded in the blockchain, and thus know whether their data has been tampered with.

In our scenario, data owner and user are only logical concepts, and an internet of thing device can be either a data owner or a user.

### 3 Design and Implementation of Algorithm

This section describes the initialization, data upload, and data acquisition phases of data access control in detail.

#### 3.1 Initialize the System

##### (1) Initialization of public information

Firstly, we input  $U$  attributes into the system, and then the nodes of the authority negotiate to select a bilinear group  $\mathbb{G}$  of generator  $g$  order  $p$  which based on the bilinear group, a bilinear pair  $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ , and  $U$  random group elements  $h_1, \dots, h_U \in \mathbb{G}$  related to  $U$  attributes in the system, and select random index  $\alpha$ , and  $a \in \mathbb{Z}_p$ . The common parameters of the system are  $PK = \{g, e(g, g)^\alpha, g^a, h_1, \dots, h_U\}$ , and the main private key is  $MSK = g^\alpha$ .

##### (2) The data owner generates searchable public and private key pairs

The data owner first generates a security parameter  $para$ , which determines the size of groups  $G_1$  and  $G_2$ . Data owner randomly selected from a number of  $\beta \in \mathbb{Z}_p^*$ , and the generator of  $G_1$ , then calculate  $A_{pub} = [g, h = g^\beta]$ ,  $A_{priv} = \beta$ .

##### (3) Data owner generates trap

The data owner uses his own search private key,  $A_{priv}$ , and the keyword it gives to the data  $m$ , to calculate a trap

$$T_W = H_1(W)^\beta \in G_1$$

The trap is then sent to the blockchain node to be packaged into a transaction.

##### (4) Blockchain initialization

There are two types of nodes in the blockchain. One is the full node that can initiate or receive transactions, participate in consensus, and retain all the blockchain content. The other is light nodes that are connected to the full node and accessed through the full node. In our paper, the authority is the full node, and other facilities that have access to the authority node such as users and data owners are the light nodes.

In the initialization process of blockchain, the Genesis block is first constructed, and the Genesis block needs to specify how the blockchain is run. When all authority nodes agree, the Genesis block officially takes effect through consensus.

### 3.2 Data Upload Phase

#### (1) Content key encryption

The data owner first encrypts its own information  $m$  using the content secret key  $\kappa \in \mathbb{Z}$ .  $\kappa$  is randomly generated by each data owner through symmetric encryption method. At the same time, a hash value  $hash = HASH(m)$  is generated for each data to be stored in the blockchain, thus verifying that the encrypted data has not been tampered with after decryption. The data owner then encrypts its own content secret key  $\kappa$  using the content secret key encryption algorithm. Input system parameter  $PK$ , content key  $\kappa$ , access structure  $(M, \rho)$ , where  $M$  is a matrix with  $l$  rows and  $n$  columns,  $l$  is the number of attributes in all encryption processes, and the function  $\rho$  associates  $M$ 's row with the attributes.

Content encryption algorithm firstly selects a random encryption index  $s \in \mathbb{Z}_p$ , and randomly selects a vector  $v = (s, y_2, \dots, y_n)$ ,  $y_2, \dots, y_n$  is used to share the encryption exponent  $s$ , calculating  $\lambda_i = v \cdot M_i (1 \leq i \leq l)$ , where  $M_i$  is the vector corresponding to row  $i$  of  $M$ . Then, randomly select  $r_1, r_2, \dots, r_l \in \mathbb{Z}_p$  and calculate the ciphertext as  $CT$ .

$$CT = \{C = \kappa \cdot e(g, g)^{\alpha s}, Ct = g^s, \\ C_i = g^{a\lambda_i} h_{\rho(i)}^{r_i}, D_i = g^{r_i}, i = 1, \dots, l, \rho(i) \in S_j\}$$

#### (2) The data owner generates searchable public and private key pairs

The data owner generates a security parameter  $para$ , which determines the size of groups  $G_1$  and  $G_2$ . Data owner randomly selected a  $\beta \in \mathbb{Z}_p^*$ , and a generator  $g$  of  $G_1$ . Thus it can be calculated that  $A_{pub} = [g, h = g^\beta]$ ,  $A_{priv} = \beta$ .

#### (3) The data owner generates the trap for data

The data owner uses his own search private key,  $A_{priv}$ , and the keywords belong to the data  $m$ , calculate a trap

$$T_W = H_1(W)^\beta \in G_1$$

After completion, the keyword trap, encrypted information  $CT$ , data address in the cloud, data access policy, content key ciphertext, and original data hash value are sent to the blockchain nodes to package into a transaction.

When the data  $m$  needs to be updated, the data owner encrypts the updated information after taking a hash value, and uploads the new encrypted data to the address where the original data is stored. The new hash value is recorded in the blockchain.

### 3.3 Data Acquisition Phase

(1) Generation of user  $U_j$ 's private key

When a user is added to the system, the authority first generates a series of attributes  $S_j$  for the user based on the user's role and identity, and uses the following private key generation algorithm to generate a private key for each user: the master private key  $MSK$ , a series of attributes  $S_j$  describing the user, and then randomly selected from a random number  $t_j \in \mathbb{Z}_p$ . Thus, produce the user's private key  $SK_j = \{K = g^\alpha g^{at_j}, L = g^{t_j}, \forall x \in S_j K_x = h_x^{-t_j}\}$ . The authority then sends the  $SK_j$  to user  $U_j$  through a secure channel.

(2) Searchable encryption of keywords generated by users

Users first randomly selected from a number  $\gamma \in \mathbb{Z}_p^*$ , at the same time input the keyword  $W'$ , and then calculate the  $y = e(H_1(W'), h^\gamma) \in G_2$ , and then output the user's keyword encryption result  $[g^\gamma, H_2(z)]$ .

(3) Query information

The user sends a query request to the smart contract, and the blockchain verifies whether  $H_2(e(T_W, g^\gamma)) = H_2(z)$  is established through the smart contract. If it is true, it indicates that the keyword searched by the user matches the keyword of the information, and the user can obtain the location of the encrypted data of the original data stored in the cloud. And get the encrypted raw data from the cloud. Otherwise, the cloud will not send encrypted information to the user.

Prove: For  $H_2(e(T_W, g^\gamma))$  and  $H_2(z)$ , which include  $z$  and  $T_W$ , then

$$H_2(e(T_W, g^\gamma)) = H_2(e(H_1(W')^\beta, g^\gamma)) = H_2(e(H_1(W), g))^{\gamma \cdot \beta}$$

$$H_2(z) = H_2(e(H_1(W'), h^\gamma)) = H_2(e(H_1(W'), g^{\beta \cdot \gamma})) = H_2(e(H_1(W), g))^{\gamma \cdot \beta}$$

The equation is valid when the user's keyword  $W'$  is the same as the data owner's keyword  $W$ .

(4) User decryption content key

When the user's attributes  $S_j$  satisfy the access control structure  $M$ , and the keyword searched by the user matches the keyword of the data owner information  $m$ , user  $U_j$  queries the blockchain to get the ciphertext  $CT$  of content secret key  $\kappa$ . At this time, input ciphertext  $CT$  and the user's private key  $SK_j$ , user  $U_j$  executes the decryption algorithm. When the user's attribute  $S_j$  satisfies the access control structure, we let  $I = \{i : \rho(i) \in S_j\}, I \subset \{1, 2, \dots, l\}$ , and  $\{w_i \in \mathbb{Z}_p\}_{i \in I}$  is a set of constants. When  $\{\lambda_i\}$  is effective share based on  $M$ 's secret  $s$ , then  $\sum_{i \in I} w_i \lambda_i = s$ .

$$e(CT, K) / (\prod_{i \in I} (e(C_i, L) e(D_i, K_{\rho(i)}))^{w_i}) = e(g, g)^{\alpha s}$$

The decryption algorithm can then obtain the content secret key  $\kappa$  through the following formula:

$$\kappa = \frac{C}{e(g, g)^{\alpha s}}$$

We can hash the decrypted  $m'$  and get  $hash' = HASH(m')$ . We comparing  $hash'$  and  $hash$ , if they are equal, then our data has not been tampered with.

## 4 Simulations

The simulation environment for this article was run on ubuntu18.04 system and gcc version 7.5.0. We used the charm-crypto 0.50 [11] of python 2.7.17 to simulate our CP-ABE scheme. In pursuit of more accurate results, we run each experiment 10 times and averaged it.

We reflect the efficiency of our proposed scheme by comparing the time of encryption, decryption and secret key generation phase when the number of attributes changes from 2 to 10 in [10, 12–14] and the search time when the total search keywords are different.

In the data encryption stage, the encryption time of our scheme is reduced by about 48, 33 and 55% respectively compared with [12–14], which reduces the time cost in the data upload stage, as shown in Fig. 2.

In the data decryption stage, the decryption time of our scheme is reduced by 66, 5 and 27% respectively compared with [12–14], which reduces the time cost in the data acquisition stage, as shown in Fig. 3.

In the generation stage of the secret key, as shown in Fig. 4, although the generation time of the secret key [13] is 40% less than our time, the time in the encryption and decryption period [13] is longer than our scheme. Considering that the secret key is only generated once in the initialization stage of public information, but the stage of data encryption and data decryption will be executed several times in the stage of data owner's data upload and user data acquisition. Through comprehensive analysis and comparison, we believe that our method is more efficient in these schemes.

In the stage of data search, we compare this scheme with [15]. As can be seen from Fig. 5, the search time and the number of keywords of this scheme and [15] are linearly correlated. When the number of keywords changes from 10 to 50, our search time increases by 75% compared with [15], which greatly reduces the time required for search and improves search efficiency.

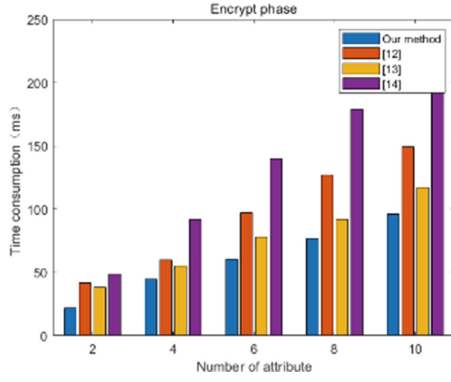


Fig. 2. Data owner encryption time.

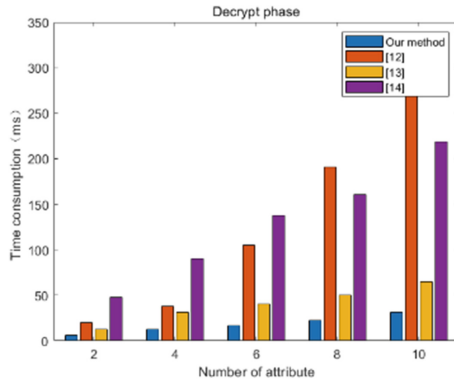


Fig. 3. User decryption time.

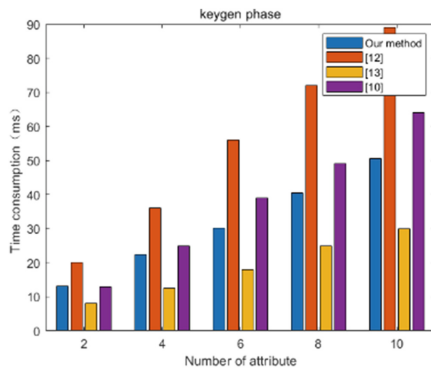


Fig. 4. Key generation time.

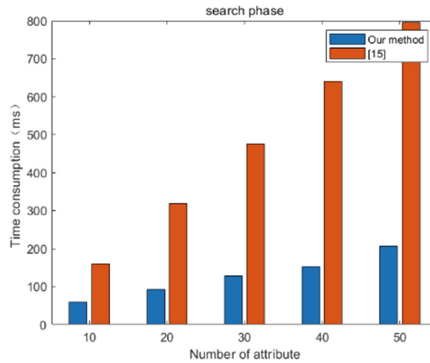


Fig. 5. Keyword search time.

## 5 Conclusion

This paper proposes an architecture of data sharing in Internet of Things based on consortium blockchain. Blockchain provides a multicentralized trusted environment for IOT data sharing, which ensures that the data stored in won't be tampered with, while also avoiding the single point of failure problem. Different from traditional blockchain-based access control solutions, this paper designs a searchable method of data with invisible keywords. In this way, users who conform to the access control policy can search for the required data in a faster time without disclosing the privacy of data to the cloud. At the same time, the permission of consortium blockchain to record data, cloud storage address and keyword information can be used to protect the information stored in the consortium blockchain from tampering. The scheme in this paper can reduce the time cost. Simulation results show that the proposed scheme is feasible. Compared with other attribute encryption schemes and searchable schemes, the proposed solution can reduce the computing time cost of Internet of Things devices without reducing the system efficiency.

**Acknowledgement.** This work was supported by the National Key R&D Program of China(2022YFB2703400).

## References

1. D'orazio, C.J., Choo, K.-K.R.: Circumventing iOS security mechanisms for APT forensic investigations: A security taxonomy for cloud apps. *Futur. Gener. Comput. Syst.* **79**, 247–261 (2018)
2. Brown, A.J., Glisson, W.B., Andel, T.R., et al.: Cloud forecasting: Legal visibility issues in saturated environments. *Comput. Law Secur. Rev.* **34**(6), 1278–1290 (2018)
3. Li, H., Jing, T.: A lightweight fine-grained searchable encryption scheme in fog-based healthcare IoT networks. *Wirel. Commun. Mob. Comput.* **2019**, 1–15 (2019)
4. Ahsan, M.A.M., Ali, I., Imran, M., et al.: A fog-centric secure cloud storage scheme. *IEEE Trans. Sustain. Comput.* **7**(2), 250–262 (2022)

5. Yin, H., Zhang, J., Xiong, Y., et al.: CP-ABSE: a ciphertext-policy attribute-based searchable encryption scheme. *IEEE Access* **7**, 5682–5694 (2019)
6. Mamta, Gupta, B.B., Li, K.-C., et al.: Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system. *IEEE/CAA J. Autom. Sin.* **8**(12), 1877–1890 (2021)
7. Wang, H., Li, Y., Susilo, W., et al.: A fast and flexible attribute-based searchable encryption scheme supporting multi-search mechanism in cloud computing. *Comput. Stand. Interfaces* **82** (2022)
8. Wang, L.P., Guan, Z., Li, Q.S., Chen, Z., Hu, M.S.: Survey on blockchainbased security services. *Ruan Jian Xue Bao/J Softw.* **34**(1), 1–32 (2023) (in Chinese). <http://www.jos.org.cn/1000-9825/6402.htm>
9. Zubaydi, H.D., Varga, P., Molnar, S.: Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: a systematic literature review. *Sensors (Basel)* **23**(2) (2023)
10. Wei, X., Yan, Y., Guo, S., et al.: Secure data sharing: blockchain-enabled data access control framework for IoT. *IEEE Internet Things J.* **9**(11), 8143–8153 (2022)
11. Charm-crypto <https://jhuisi.github.io/charm/index.html>
12. Zhang, L., Ye, Y., Mu, Y.: Multiauthority access control with anonymous authentication for personal health record. *IEEE Internet Things J.* **8**(1), 156–167 (2021)
13. De, S.J., Ruj, S.: Efficient decentralized attribute based access control for mobile clouds. *IEEE Trans. Cloud Comput.* **8**(1), 124–137 (2020)
14. Rouselakis, Y., Waters, B.: Efficient statically-secure large-universe multi-authority attribute-based encryption. In: *International Conference on Financial Cryptography and Data Security*, pp. 315–332. Springer, Berlin (2015)
15. Chen, R., Mu, Y., Yang, G., et al.: Server-aided public key encryption with keyword search. *IEEE Trans. Inf. Forensics Secur.* **11**(12), 2833–2842 (2016)



# TSN Traffic Scheduling and Route Planning Mechanism Based on Hybrid Genetic Algorithm

Zelin Zheng<sup>1</sup>, Qian Wu<sup>1</sup>, Wei Lv<sup>1</sup>, Qiang Gao<sup>1</sup>, Junhong Weng<sup>1</sup>, and Peng Lin<sup>2</sup>(✉)

<sup>1</sup> Shenzhen Power Supply Co., Ltd., Shenzhen 518000, China

<sup>2</sup> Beijing Vectinfo TECHNOLOGIES Co., Ltd., Beijing 100088, China  
linpeng@Vectinfo.com

**Abstract.** In order to solve the problems of the uncertainty of end-to-end delay caused by the separation of scheduling and routing in the existing scheduling strategies in time-sensitive networks and the poor convergence of traditional genetic algorithms, a traffic scheduling method based on particle swarm optimization algorithm (PSO) combined with genetic algorithm and route planning was proposed. The method combines the inherent characteristics of time sensitive traffic and allows for flexible allocation of traffic routing. On this basis, a scheduling constraint model with no-wait constraints and risk balanced routing is established to guarantee low latency requirements for time sensitive traffic scheduling in both temporal and spatial dimensions. The experimental results show that the proposed method shows good convergence in different topology scenarios. By using the route planning strategy and the improved genetic algorithm, the total transmission time of the time-triggered flow is reduced by about 7.92% compared with the traditional genetic algorithm.

**Keywords:** Time sensitive network · Heuristic algorithm · Route planning · Time-triggered flow

## 1 Introduction

As a new network data transmission technology, time sensitive network (TSN) can support multiple types of traffic, such as time sensitive (TT) traffic and best-effort traffic, globally plan and schedule different types of traffic, and eliminate conflicts on outgoing ports for sequential transmission. Ensure the deterministic transmission requirements of TT traffic in terms of delay, jitter and reliability. As the core mechanism of TSN, traffic scheduling is the key to ensure data transmission of TSN. The current TSN traffic scheduling mechanism uses protection tape. Although protection tape protects high-priority traffic, it has the problem of bandwidth loss. In recent years, no-wait scheduling mechanism has attracted wide attention in academia and industry.

At present, there have been a lot of researches on TSN traffic scheduling [1–6]. In [1], Durr et al. introduced the no-wait model of TSN scheduling without queuing delay on the switch. In addition, they propose a heuristic algorithm for computing scheduling and a scheduling compression technique to reduce bandwidth waste. Reference [3]



describes the traffic scheduling problem as a combinatorial optimization problem, and sets the optimization objective as minimizing the number of queues occupied by real-time traffic and the weighting of end-to-end delay, which is solved through the traffic scheduling mechanism based on integer linear programming. In [4], a new integer linear programming model is proposed based on software defined network (SDN), and zero frame loss is successfully achieved by offline scheduling and online scheduling. Reference [5] improved the protection belt problem concerned with TSN, described the traffic scheduling problem as a binary knapsack problem, and proposed a dynamic programming solution algorithm under ideal conditions and a fast solution algorithm based on greedy algorithm under the premise of protection belt constraints, so as to reduce the waste of protection belt. In [3], scheduling is conducted in sequence according to the cut-off time of streams, and an early transmission strategy is designed to minimize the number of occupied queues and reduce the total transmission time as much as possible, thus greatly reducing the solution time.

Furthermore, the schedule ability of traffic not only depends on the configuration of TSN gating and time slot mapping, but also can be improved with a good routing policy. Researchers have extensively explored traffic routing in TSN [7–11]. For example, in [10], constraints jointly generated by routing and scheduling are used along with a heuristic algorithm based on genetic algorithms to solve the global scheduling table, which significantly improves link utilization, schedule ability, and transmission efficiency. In [5], the traffic scheduling problem is transformed into a binary knapsack problem by improving the simulated annealing and genetic algorithms. This incorporates route selection into the constraint conditions thus enabling synchronous planning of routing and scheduling. In [11], Voica et al. adopted the GCL synthesis method, which considers AVB traffic when scheduling TT traffic. Additionally, a time-sensitive software-defined network (TSSDN) solves the routing and scheduling combination problem of TT traffic using different ILP formulas.

The existing research has the following deficiencies. Firstly, the current scheduling scheme does not consider the routing conflicts and dependencies between the TT traffic deployed in the network, which leads to the limitation of the global communication scheduling capability of the TSN. Secondly, in the study of joint route scheduling, the characteristics of the traffic itself are not fully considered, but the traffic path is simply defined according to the routing index, which makes the delay performance of traffic scheduling difficult to be guaranteed. To solve the above problems, this paper proposes a joint routing scheduling strategy with no-wait constraints. The specific contributions are as follows:

- 1) Establishing a scheduling model that incorporates no-wait constraints, utilizing both time and space TDMA for scheduled traffic, can eliminate queuing delay and ensure high-quality delay performance.
- 2) By constructing a risk-balanced link load model and proposing a corresponding routing strategy, traffic transport can be selectively distributed to different paths to minimize contentions along the same route. Load balancing of the links can be achieved for optimal performance.

- 3) Design a hybrid genetic algorithm based on particle swarm optimization (PSO) algorithm, in order to reduce the total TT flow transmission time as the goal, on the premise of no-wait for the constraint in the acceptable time find out the optimal solution.

## 2 System Model

### 2.1 Network Model

The data plane’s network topology can be expressed as a directed graph  $G = (V, E)$ , where  $V$  denotes the nodes that make up the network, including switches (SW) and end systems (ES). Figure 1 provides an example.  $E \subseteq V \times V$  represents an edge set in which each element represents a one-way link between two nodes. To represent the routing path between two end nodes, an ordered list of links that it passes through can be utilized. For instance,  $r = \{ES1, SW1, SW3, ES4\}$  refers to a valid route between the end devices  $ES1$  and  $ES4$ .

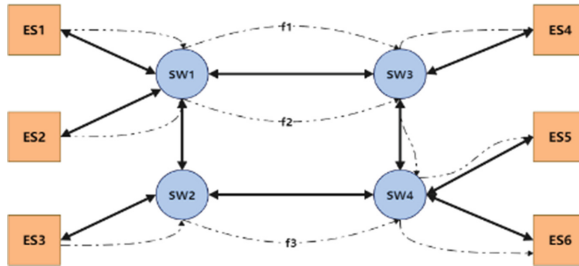


Fig. 1. Example of a TSN model.

Each TT flow can be defined by a quadruple  $\langle src, dst, T, L \rangle$ , which represents the sender and receiver of the TT flow, its period, and data size. The flows have different periods, thus the least common multiple of all flow periods denotes the super cycle can be expressed as:

$$T_{sched} = LCM(F, \text{persiods}) \tag{1}$$

The number of times each TT flow is transmitted within a super-period is:

$$Tnum = \frac{T_{sched}}{f_i \cdot T} \tag{2}$$

All flows in TSN are transmitted in frames, and Ethernet specifies that the payload of each frame should not exceed its maximum transmission unit (MTU) of 1500 bytes. If the size of a flow exceeds MTU, it needs to be split into multiple frames for transmission.

## 2.2 No-Wait Scheduling Model

In a TSN network, the end-to-end delay includes propagation delay on the network link, processing delay on switches, queuing delay caused by congestion, and transmission delay. Here, we assume that all switches have the same processing delay, and we represent the propagation delay of all links as  $d_{prop}$ . Let  $d_{i,j}^{trans}$ ,  $d_{i,j}^{queu}$  represent the transmission delay and the queuing delay of the flow  $f_i$  on the switch  $sw_j$ .

To minimize end-to-end delay, we eliminate the queuing delay in switches and enable TT flows to be transmitted without waiting. Because there is no queuing delay, the remaining components of the end-to-end delay are deterministic. This means that given the known transmission paths, it is only necessary to determine when a TT flow enters the network in order to calculate the time it passes through each switch. By adjusting the injection time of packets at the source, conflicts with other flows in the network can be avoided, thereby eliminating queuing delay.

If flow  $f_i$  travels  $n$  hops from device  $v1$  to device  $v2$ , its end-to-end delay can be expressed as:

$$delay_i^{(v1,v2)} = n * (d_{prop} + d_{proc}) + \sum_{k=1}^n d_{i,k}^{trans} \quad (3)$$

Let the duration from when the first bit of the first flow is sent from the source system to when the last bit of the last flow is processed at the destination system be represented as *FlowSpan*.

## 2.3 Core Constraints in No-Wait Scheduling

Under the environment defined in this article, the constraint conditions defined below can ensure the effective operation of our no-wait scheduling model.

- Time Slot Constraint:  $T = \{t0, t1, t2, \dots, tn - 1\}$  representation of time slot set. The length of each time slot is the sum of transmission delay, propagation delay and switching delay of an MTU, which can be represented as:

$$solt\_len = d_{trans}^{MTU} + d_{proc} + d_{prop} \quad (4)$$

- Flow Offset Constraint: In TSN, the frame offset of the flow being transmitted cannot be earlier than the global timing start time. In addition, to meet the periodic characteristic of TT streams, each TT stream must be transmitted within its own period, which can be expressed as follows:

$$\forall f_i \in F, (f_{i,1}.offset \geq 0) \cap (f_{i,1}.offset < f_i.T - delay_i^{(src,dst)}) \quad (5)$$

- *FlowSpan* Constraint: If the flow of the previous cycle is still in transmission at the beginning of the next cycle, the flow of the next cycle will be queued. To avoid this situation, the constraint is as follows:

$$FlowSpan \leq T_{sched} \quad (6)$$

- **No Conflict Constraint:** The constraint of links is the core constraint under the condition of conflict-free transmission. It requires that any two data frames passing through the same link must not pass at the same time to ensure no temporal. A function can be defined as shown as follows:

$$FTL = \{X(f, t, l)\}, \forall f \in F, \forall t \in T, \forall l \in L \quad (7)$$

If flow  $f$  occupies the link  $l$  in the time slot  $t$ , the value of Eq. (7) is 1; otherwise, it is 0. The constraint of link conflict can be uniformly described in the following form.

$$\forall l \in E, \forall t \in T \sum_{\forall f \in F} X(f, t, l) \leq 1 \quad (8)$$

## 2.4 Problem Formulation

The protection band is derived from the gate driver program events, which control the opening and closing of queue gates for predetermined streams. Reasonable scheduling of TT flows can reduce these events, thereby reducing the number of protection bands, saving more network throughput, and providing more transmission resources for BE traffic. To achieve this goal, a more intuitive optimization objective is to minimize the total transmission time of all TT flows.

Minimizing *FlowSpan* means that the transmission of TT flows is compressed at the beginning of scheduling, reducing the number of protection bands. According to our no-wait model, as long as the transmission interval between data streams is large enough, it can be ensured that there will be no queuing in the network. However, blindly increasing the interval may result in failure to meet the transmission constraints. To avoid the above problems, the TT flow should enter the network as early as possible. Equation (9) defines the completion time of a flow:

$$C_i = t_i + delay_i + Tnum_i * f.T \quad (9)$$

The latest completion time for all flows is:

$$C_{\max} = \max\{C_i | i \in \{1, 2, \dots, n\}\} \quad (10)$$

The optimization goal of minimizing the total transmission time can be described as:

$$\begin{aligned} & \min C_{\max} \\ & s.t. (4) - (8) \end{aligned} \quad (11)$$

## 3 Algorithm Design

### 3.1 Risk-Balanced Routing Planning Algorithm

In the context of no-wait constraints, we use an incremental scheduling algorithm that gives priority to link load factors, optimizes the overall quality of route selection, and improves the success rate of scheduling. Each TT flow will cause a load on the links it

passes through. By coordinating the route selection of TT flows, the load on each link in the network can be relatively balanced. If flow  $f_i$  is transmitted through link  $l_j$ , its load on link  $l_j$  can be represented as.

$$l_{i,j} = \frac{\frac{f_i \cdot L}{\max(f \cdot L)}}{|P_i| * \frac{f_i \cdot T}{\min(f \cdot T)}} \quad (12)$$

$\min(f \cdot T)$  and  $\max(f \cdot L)$  represent the maximum concentrated load of the traffic set for this scheduling and the minimum value of the propagation period. When the traffic set for this scheduling is determined, the total load on each link can be obtained by summing up the loads generated by each flow on that specific link.

$$l_j = \sum_i l_{i,j} \quad (13)$$

Each TT flow will only select one path from the shortest path set for transmission. The evaluation of the load on a path can be obtained by summing up the loads of the links included in that path. Then, the candidate path with the minimum cost is selected as the result.

$$P_i = \sum_j l_j \quad (14)$$

In order to balance the load in the network, it is necessary to distribute the load of the links occupied by transmission as evenly as possible. Equation (15) describes an overall evaluation index for the comprehensive load of the network.

$$LBD = \sqrt{\frac{\sum_{i=1}^{|E|} (l_i - \bar{l})^2}{|E|}} \quad (15)$$

A load-balancing routing method based on a greedy algorithm is now proposed. This approach takes into consideration the network topology and data flow information as inputs and generates the routing for all flows as output.

The proposed greedy-based load-balancing routing method follows a series of steps. Firstly, the breadth-first algorithm is used to compute the candidate path set for each flow. Subsequently, Eqs. (12) and (13) are utilized to calculate the load value of all links. The candidate path set is then sorted in an ascending order of size to establish the solving order of the routing algorithm. Then, the first candidate flow in this sequence is selected, and a greedy approach is employed to select the path with the minimum risk from the available paths. This path is subsequently considered as the final result, and the link load in the network is recalculated. These steps are repeated until all flows have been successfully routed.

### 3.2 Design of Traffic Scheduling Algorithm

**Fixed-Priority Traffic Scheduling Algorithm.** When a series of data streams and their transmission order is known, the entry time for each stream into the network can be

selected accordingly. The timing of transmission for each stream is influenced by the streams preceding it, and the quality of the solution obtained in this iteration is determined by the transmission order.

During the scheduling process, the link is considered as a spatial resource unit while the time slice is viewed as a temporal unit. The transmission of a data stream on the link is taken as an indicator to determine conflicts. In this regard, the scheduling variable pertains to the time when the data stream enters the network. The objective of the algorithm is to minimize the total transmission time by ensuring that all streams enter the network as early as possible to reduce completion time. The pseudocode for the algorithm is presented below:

```

begin
(1)  FSTime← {}, Span←0, UseLinkPeriod← {},slove=True
(2)  for each flow in F:
(3)    while starTime<flow.T-FlowSpan:
(4)      scheduled flow on each timeslot of each link in flow path
(5)      if no conflict in all link:
(6)        FSTime[flow]←starTime
(7)        break
(8)    end while
(9)    if flow cannot scheduling:
(10)     slove=FALSE
(11)     break
(12)    for each link in flow path:
(13)     for each timeslot in cluser period:
(14)       UseLinkPeriod[link]←flowUsedPeriod
(15)     end for
(16)     span ← max(Span,link.lastUsedTime)
(17)    end for
(18)  end for
(19)  if slove=TRUE:
(20)    return (FSTime,Span,UsedLinkPeriod)
(21)  else return infeasible
end

```

**PSO-GA Scheduling Algorithm.** In conclusion, the scheduling sequence of flows has a great influence on the results. To achieve the most optimal solution, it is necessary to examine all possible sequence combinations, but given that there are  $n!$  permutations for ordering  $n$  flows, the complexity of such traversal becomes too high. Consequently, we propose a mixed genetic algorithm which comprises the following parts.

- Definition of individuals: As the purpose of this algorithm is to explore different TT flow sequences, the genome is an ordered arrangement of the treatment scheduling flow collections, and different sequences represent different individuals.
- Fitness evaluation function: To better select parents, a reasonable fitness function is needed. We can directly use the optimization objective defined in Chap. 2 and add an additional term to it as follows:

$$f(x) = \min C_{\max} + a * \sum_{\forall f \in F} f.offset \tag{16}$$

where  $a$  is a coefficient multiplied by the sum of the start transmission time for all TT flows.

- Initialization of the population: Generate a list of flows with sequential order randomly, specifying the number of flows to be scheduled as the initial solution. Evaluate all individuals within this initial solution, keep track of the best individual in history, and determine the global optimum.
- Natural selection: During the phase of natural selection, beginning with the first individual, other individuals are chosen through the roulette wheel method to mate with it and generate offspring. The three constants  $w$ ,  $c1$ , and  $c2$  are defined as inertia weight, self-awareness factor, and social awareness factor. They respectively represent the probabilities of selecting parent as self-reverse, personal best ( $pBest$ ) historical position, and global best ( $gBest$ ) position.

$$parent2 = \begin{cases} self.reverse, & 0 \leq random < \frac{w}{w+c1+c2} \\ pBest, & \frac{w}{w+c1+c2} \leq random < \frac{w+c1}{w+c1+c2} \\ gBest, & \frac{w+c1}{w+c1+c2} \leq random < 1 \end{cases} \tag{17}$$

- Crossover and mutation: The crossover operation can be implemented using the following steps: randomly select a segment of sequence from one parent, place it in the corresponding position of the offspring, and fill the remaining positions with sequences from the other parent which have not yet appeared in the current offspring (see Fig. 2). The mutation operation is relatively simple, directly select any two positions of the genes at random, and exchange their positions.

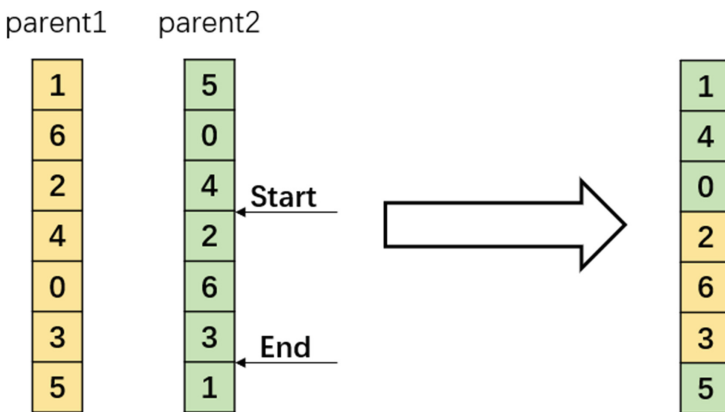


Fig. 2. Cross-reference example.

- Evaluation iteration: After each iteration produces children, the current particle swarm is reevaluated. For each particle, if its current cost is less than its historical best estimate, the historical best is updated to the current sequence. If the minimum cost of an individual in this generation is less than or equal to the historical global optimal, then the historical global optimal will be updated to the minimum value of this generation.

```

begin
(1)   Initialize w,c1,c2,iterMax,gBest,pBest,gLine,pLine
(2)   Poplist←RandomInitPop(F)
(3)   for each pop in Poplist:
(4)       PopScore←FixOrderScheduling(pop)
(5)       Upgrade pBest,pLine
(6)       if PopScore>gBest:
(7)           upgrade gBest,gLine
(8)   end for
(9)   while iter<iterMax:
(10)      for each pop in Poplist:
(11)          parent2=selectParent(random,w,c1.c2)
(12)          poplist[pop]=crossover(pop,parent2)
(13)          popScore= FixOrderScheduling(poplist[pop])
(14)          if popScore<pBest:
(15)              upgrade pLine,pBest
(16)          if popScore<gBest:
(17)              upgrade gLine,gBest
(18)      end for
(19)  end while
end

```

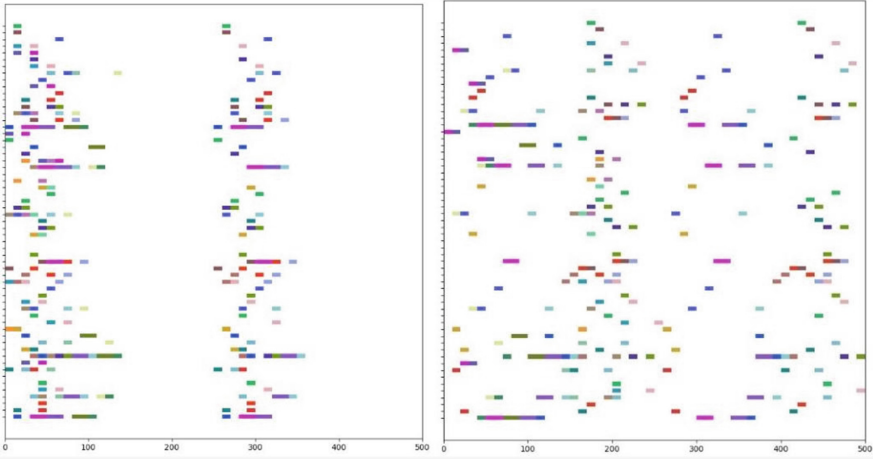
## 4 Evaluation and Result

We primarily validate the performance of the algorithm proposed in this work. The simulation mainly focuses on algorithm optimization under different network topologies and data flow sizes, and uses traditional genetic algorithms as a comparison. In our simulation, the experimental environment is Python3.7 and networkx2.8, running on a machine equipped with an Intel Core i5-9300 processor and 8 GB of RAM.

Since there is currently no official dataset on traffic scheduling for TSN, the TT flow collection in this experiment will be randomly generated based on actual scenarios. The sender and receiver are selected randomly, and the data size is chosen to be between 1 and 3 MTUs, assuming that the devices in the network have the same transmission rate and processing delay.

To verify the final effect of the traffic scheduling algorithm designed in this paper on the optimization objective, simulation was carried out in a network environment with 30 data flows, 20 switches and 10 terminal devices. The algorithm parameters were set





**Fig. 3.** Comparison between the initial solution and the better solution.

as follows: 30 particles, an inertia factor of 0.4, a self-knowledge factor of 0.6, a social knowledge factor of 0.6, and 200 iterations. After 200 iterations, the global optimal solution obtained and the randomly generated initial solution were compared, and the Gantt chart for the two schedules is shown in Fig. 3.

Following optimization, we have observed a significant decrease in the earliest completion time. Notably, the transmission efficiency of each TT flow has improved, which helps mitigate bandwidth waste caused by protection bands. In addition, the periodic transmission of TT flows has become even more apparent.

In addition to algorithm effectiveness, the calculation time required by the algorithm is also a significant evaluation metric. The network topology complexity and the number of scheduled flows is the main factors that affect scheduling algorithm execution time. To examine the algorithm’s runtime performance under differing conditions, we designed three distinct network environments with varying scales and verified the time it took for the algorithm to schedule data flows of different sizes in each network environment, as demonstrated in Fig. 4.

It can be seen from the comparison results that, for the same algorithm parameter configuration, the algorithm running time is positively correlated with the network topology scale and the number of streams to be scheduled, and the number of streams to be scheduled plays a major role. The time complexity of the algorithm is obviously less than  $n!$ ,  $n$  is the amount left for scheduling, which can converge within an acceptable time.

In order to demonstrate the efficiency of the routing planning algorithm proposed in this paper, along with the improved genetic particle swarm algorithm, comparative experiments were conducted to validate their enhanced performance under identical network environments and data flow sets. Four comparative experiments were carried out, utilizing both genetic particle swarm algorithms and traditional algorithms, either

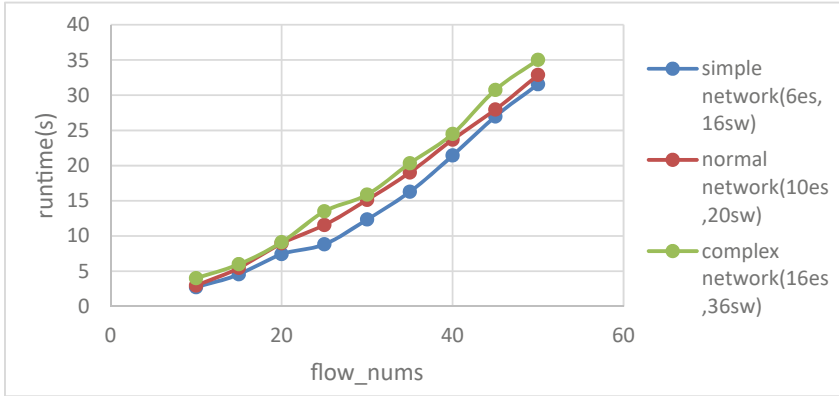


Fig. 4. Algorithm execution time.

with or without the use of route planning strategies. These experiments were intentionally designed to achieve controlled variable contrast. The operational results have been illustrated in Fig. 5.

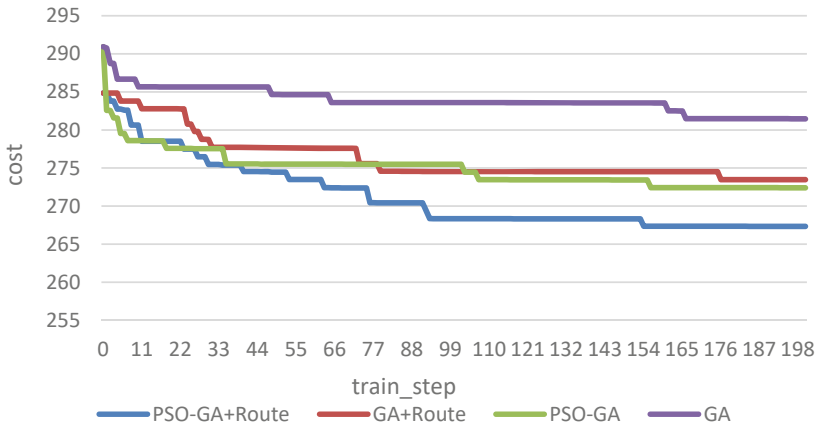


Fig. 5. Comparison between route planning and traditional genetic algorithms.

Under the same network environment and scheduling flow set, after using the route planning algorithm, Eq. 14 indicates that the risk assessment in the network is reduced by about 14%, which is shown in the figure above as the cost of the initial solution is directly reduced. Compared with the traditional genetic algorithm, although the traditional genetic algorithm converges earlier, it is easy to fall into the local optimal solution. Under the same parameter configuration and network environment, the cost of the PSO-GA algorithm is reduced by about 7.92%.

## 5 Conclusion

Aiming at the problem of scheduling and routing separation of TT traffic in TSN, this paper proposes a route planning algorithm and scheduling algorithm of risk balance, which provides a new solution for joint route planning and scheduling of TSN. Experimental results show that the proposed scheduling method can adapt to different types of TSN topology scenarios. There are still many shortcomings in the work done in this paper. For example, when the size of time-triggered stream is less than one MTU, certain broadband waste will be caused, and the network environment is considered static. In future work, we will consider more comprehensive TT flow scheduling.

**Acknowledgement.** This work was supported by the Science and Technology Project of China Southern Power Grid (No.090000KK52210155).

## References

1. Dürr, F., Nayak, N.G.: No-wait packet scheduling for IEEE time-sensitive networks (TSN)[C/OL]. In: Proceedings of the 24th international conference on real-time networks and systems 203–212 (2016)
2. Schweissguth, E., Danielis, P., Timmermann, D.: ILP-based joint routing and scheduling for time-triggered networks[C/OL]. In: Proceedings of the 25th International Conference on Real-Time Networks and Systems (2017)
3. Raagaard, M.L., Pop, P.: Optimization algorithms for the scheduling of IEEE802.1 time sensitive networking (TSN)[OL]
4. Pang, Z., Huang, X., Li, Z.: Flow scheduling for conflict-free network updates in time-sensitive software-defined networks[J/OL]. *IEEE Trans. Industr. Inf.* **17**(3), 1668–1678 (2020)
5. Zhang, C., Wang, Y., Yao, R.: Packet-size aware scheduling algorithms in guard band for time sensitive networking[J/OL]. *CCF Trans. Netw.* **3**(1), 4–20 (2020)
6. Wang, Y., Chen, J., Ning, W.: A time-sensitive network scheduling algorithm based on improved ant colony optimization[J/OL]. *Alex. Eng. J.* **60**(1), 107–114 (2020)
7. Arestova, A., Hielscher, K.S.J., German, R.: Design of a hybrid genetic algorithm for time-sensitive networking [M/OL]. In: Lecture Notes in Computer Science, Measurement, Modelling and Evaluation of Computing Systems, pp. 99–117 (2020)
8. Bingqian, L., Yong, W.: Hybrid-GA based static schedule generation for time-triggered ethernet[C/OL]. In: 2016 8th IEEE International Conference on Communication Software and Networks (ICCSN). Beijing (2016)
9. Vlk, M., Hanzálek, Z., Tang, S.: Constraint programming approaches to joint routing and scheduling in time-sensitive networks[J/OL]. *Comput. Ind. Eng.* **157**, 107317 (2021)
10. Pahlevan, M., Obermaisser, R.: Genetic algorithm for scheduling time-triggered traffic in time-sensitive networks[C/OL]. In: 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA). Turin (2018)
11. Gavrilut, V., Pop, P.: Scheduling in time sensitive networks (TSN) for mixed-criticality industrial applications[C/OL]. In: 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS). Imperia, Italy (2018)



# An DAG-Based Resource Allocation Mechanism of Federated Learning for New Power Systems

Jiakai Hao<sup>1</sup>, Guanghuai Zhao<sup>1</sup>, Ming Jin<sup>1</sup>, Yitao Xiao<sup>2</sup>(✉), Yuting Li<sup>1</sup>, and Jiewei Chen<sup>2</sup>

<sup>1</sup> State Grid Beijing Electric Power Company, Beijing 100031, China

<sup>2</sup> Beijing University of Posts and Telecommunications, Beijing 100088, China  
850612068@qq.com

**Abstract.** The traditional federated learning framework heavily relies on a single central server, which leads to problems such as single-point failures and malicious attacks. The new-type power system brings diverse collaborative business needs of “generation-transmission-distribution-storage”. With the significant increase of sensing terminals of new-type power devices, the security protection of data generalization becomes more and more crucial, and the energy consumption of devices has become a critical bottleneck for current federated learning tasks. The DAG structure has inherent decentralization and asynchronous characteristics, which can greatly accelerate the speed of global aggregation in federated learning, and the complexity of the DAG network can ensure the security and reliability of the model. In this paper, we propose a DAG-based federated learning framework for energy-constrained new-type power systems. In order to solve the problems of energy loss and training delay in DAG-based federated learning, a resource allocation algorithm based on multi-objective differential evolution is proposed. The algorithm aims to consider the impact of device energy consumption on federated learning performance, so as to minimize the completion time and energy loss of federated learning tasks under the constraint of expected learning accuracy of edge devices in the smart grid.

**Keywords:** Directed Acyclic Graph (DAG) · Federated learning · New power systems · Resource allocation

## 1 Introduction

With the proposal of the dual carbon goals, artificial intelligence (AI) and digital grid are further integrated, and the large-scale new-type power system dominated by new energy sources accelerates the evolution towards the energy internet [1]. The new-type power system brings diverse collaborative business needs of “generation-transmission-distribution-storage”, while the expansion of security boundaries has led to a significant escalation in the risk of novel network attacks. How to ensure secure cross-domain data communication while achieving efficient training of a massive number of distributed terminals has become a key constraint for the new-type power system [2].

To this end, it is urgently needed to break through the data security sharing technology of the power industry and develop a privacy-preserving computing framework for power industry data. This will support the security and protection system architecture of information and communication services in the new power system. Federated learning (FL) [3], as one of the most advanced trusted distributed machine learning frameworks, has gained popularity among scholars due to its ability to achieve secure data sharing through model sharing and aggregation, without requiring data to be moved to other participating nodes.

Decentralized blockchain can ensure the privacy and trustworthiness of the calculation process and data and aggregate model parameters through consensus algorithms. However, the traditional blockchain consensus mechanism and architecture suffer from problems such as slow transaction speed, limited resources and throughput, scalability, and high energy consumption, leading to significant delays in parameter convergence in blockchain networks. Based on the aforementioned issues, Cao et al. [4] proposed an asynchronous DAG blockchain-enhanced federated learning (DAG-FL) that accelerated the transaction speed of the blockchain and achieved complete decentralization through P2P communication between nodes for exchanging models or gradients. However, the drawback is that this architecture did not consider the energy consumption of devices in new power system scenarios. To address this problem, this paper analyzes the device energy consumption in DAG-FL and designs a resource scheduling strategy based on differential evolution algorithm optimization. The main contributions of this paper are as follows:

1. We propose a DAG-based federated learning framework for energy-limited new power system scenarios, which achieves complete decentralization and asynchronous learning.
2. We analyze the energy consumption of the system and design an energy optimization objective by modeling the communication and computing resources. A multi-objective differential evolution algorithm is adopted to optimize energy consumption and total training time.

## 2 Related Work

### 2.1 Federated Learning Framework Based on DAG

In the past two years, the DAG-based federated learning (DAG-FL) framework has shown its advantages in achieving complete decentralization and asynchronous learning. The DAG-FL system developed by Cao et al. consists of three layers: the FL layer, DAG layer, and Application layer. The Application layer provides an interface for deploying DAG-FL conveniently to external agents, while the DAG layer and FL layer provide an asynchronous platform for federated learning. Each participating node constructs a global model from its local DAG, thereby solving the problem of asynchronous and abnormal nodes in wireless networks. Based on DAG-FL, Beilharz et al. [5] implemented biased random walks by integrating the performance of the model on local data as a bias for the tip selection algorithm, achieving personalized implicit clustering of client nodes. A compromise can be made between reaching consensus on a common model and personalizing the model to local data.

## 2.2 Federated Learning Resource Allocation

In the context of smart grid, the training accuracy and time of federated learning are affected by the limitations of various resources such as communication, computation, and devices. To address the low training efficiency caused by stragglers, Cui et al. [6] propose a heterogeneous-aware client scheduling strategy based on ISODATA and explore a resource block allocation strategy based on MIP to accelerate the training efficiency, taking into account the heterogeneity of participating IoT devices. Lim et al. [7] considered the node failure and device disconnection, and designed a two-level resource allocation and incentive mechanism design problem. They adopted an auction mechanism based on deep learning to obtain the service value of each cluster head.

## 2.3 Application of Federated Learning in New Power Systems

In the context of smart grids, federated learning has wide application prospects. Jithish [8] et al. proposed a federated learning-based anomaly detection scheme for smart grids, where local machine learning training is conducted in smart meters and SSL/TLS protocols are employed to secure the model parameter updates. Singh [9] et al. introduced a serverless cloud-based federated learning model for privacy-preserving smart grid data. The model takes into account dew servers supporting blockchain in each HAN, and utilizes advanced perturbation and normalization techniques to reduce the adverse impact of irregular workloads on training results.

# 3 System Model

## 3.1 System Framework Structure

In order to construct a secure and privacy-preserving data environment for electric power big data, this paper proposes a new energy-limited DAG-based federated learning framework for the new type of power system. This framework can be used for various business scenarios of the information and communication security service platform of the new power system, such as electricity prediction, distributed power device fault detection and parameter setting, electricity fee recovery, user profiling of power metering systems, etc. Participants can conduct trusted computing for intelligent computing business of the new power system under the premise of data privacy protection, breaking down energy data barriers and efficiently realizing data analysis.

The framework is a fully asynchronous and decentralized federated learning framework, which uses distributed edge devices for data collection and computation, and any node can choose the latest local reference model when it is idle, and is subject to less bandwidth constraints.

The system model, as shown in the Fig. 1, includes two types of entities: distributed edge nodes (EN) and multi-access edge computing servers (MEC), which communicate with each other through point-to-point network communication. The specific roles of each entity are as follows:

(1) EN

Each edge node has hardware capacity limitations, and only stores local data to construct a sub-DAG that is visible only locally. Local aggregation is performed by selecting and verifying the accuracy of the tip nodes to update the local model. Then, the local device attaches the new transaction containing the updated local model to the peer-to-peer DAG network.

(2) MEC

The MEC server has high computing and storage capacity and serves as a full node, storing all transactions and constructing the global DAG from the genesis transaction via point-to-point network communication. MEC enables the DAG network to reach consensus on the global model.

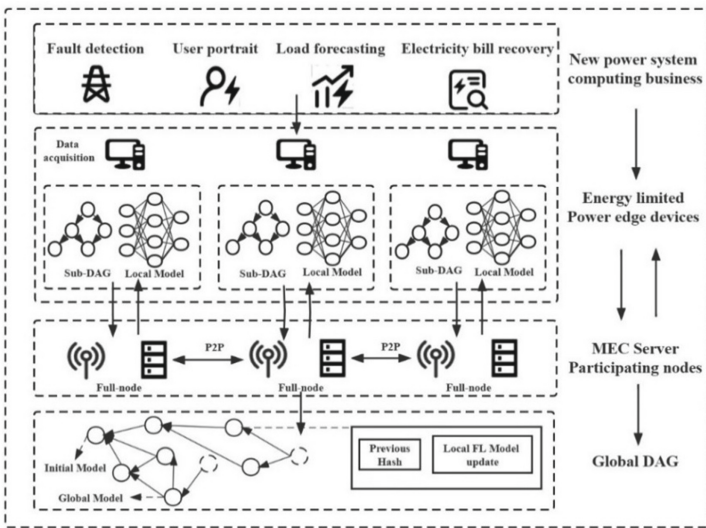


Fig. 1. Frame diagram of a new power system federated learning system based on DAG

3.2 System Workflow

As shown in Fig. 2, due to the unique asynchronous nature of DAG, there is no need to stop and wait for the central server to update the global model. Local models can be freely uploaded. Therefore, each edge node needs to first create a local sub-DAG, composed of Transactions and their Approvals, and the updating process can be divided into seven steps.

(1) Random Tips Selection

Tips refer to unapproved transactions, and the local edge node needs to randomly select  $\Upsilon$  Tips from multiple unapproved transactions to minimize the computational pressure

on the edge device. If the number of Tips on the local DAG is too large, it indicates that there may be significant differences between the constructed global models. This will greatly reduce the efficiency of early models, and even co-constructed machine learning models may never converge. For different federated learning tasks, keeping the number of Tips around a constant value  $L_0$  ( $L_0 > 0$ ) at any time is the key to ensuring the stable and efficient operation of system. To simplify the analysis, we represent the setting of  $L_0$  as follows:

$$L_0 = \frac{k\lambda(T_{cmp} + T_{val} + T_{com})}{(k - 1)f} \quad (1)$$

In the above formula,  $\lambda$  represents the arrival rate of the Poisson process and can be considered a constant.  $k$  serves as a dynamic weight to maintain the constancy of  $L_0$ .  $f$  represents the CPU frequency during device training, and  $T_{cmp}$ ,  $T_{val}$ ,  $T_{com}$  represent the node computation delay, validation delay, and propagation delay, respectively.

### (2) Local Accuracy Testing

In the second step, the local edge node selects  $\Upsilon$  tips and conducts precision testing using its own local privacy testing set to obtain the testing accuracy of each selected tip.

### (3) Authentication

In the third step, the local edge node performs transaction verification to verify the transaction hash information before the integrity of the DAG network to achieve authentication.

### (4) Tips Selection Again

In the fourth step, local edge nodes will sort the accuracy of the Tips tested on their local sensitive dataset, and select another  $\nu$  ( $\nu < \Upsilon$ ) highest accuracy Tips in descending order.

### (5) Local Aggregation

In the fifth step, the local edge node uses the FedAvg algorithm to locally aggregate the  $\nu$  ( $\nu < \Upsilon$ ) highest precision tips to obtain the local reference model.

### (6) Local Updates

In the sixth step, the local edge node trains the local model update on its local private training dataset using the local reference model.

### (7) Publish Transactions

In the seventh step, the local edge node publishes a new transaction to the peer DAG nodes through the P2P network. The new transaction contains authentication information, the updated local model after training, and the approval information of the selected  $\nu$  Tips.

For the global DAG, the model needs to be initialized first, with the genesis transaction and pre-defined expected learning accuracy published. The MEC server regularly updates the global DAG. The accuracy of the latest approved tips is sorted from high



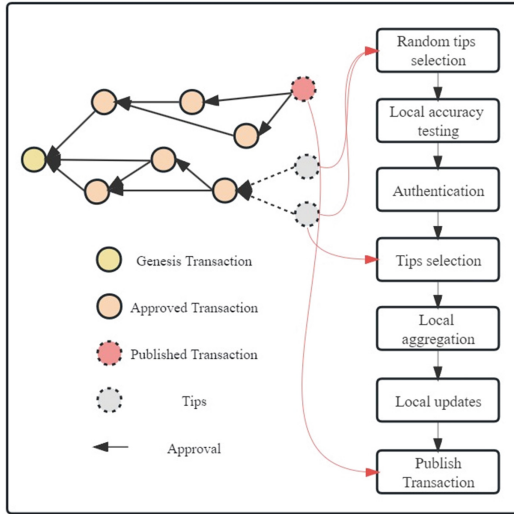


Fig. 2. Local DAG update process

to low, and the top  $v$  tips with the highest accuracy are selected for global aggregation using the FedAvg algorithm. The accuracy of the global model is validated, and once the accuracy exceeds the predefined learning accuracy, the federated learning task ends.

### 3.3 Analysis of Resource Allocation Problems

In the new power IoT scenario, with the requirements of scalability and flexibility and considering the complexity of wiring, battery power supply is often used. However, the energy consumption of devices becomes a critical bottleneck for current federated learning tasks. In view of the resource optimization and management problems such as battery energy and communication resource allocation of heterogeneous devices in low-resource available environments, this paper aims to consider the impact of device energy consumption on federated learning performance, in order to solve the optimization problem of minimizing federated learning task completion time and energy loss of edge perception devices in the new power system under the constraint of expected learning accuracy.

### 3.4 Modeling Resource Allocation

In this study, each device has performance differences (such as CPU). If each device can freely train and upload local models, resources will be wasted. Therefore, it is expected to use a local controller for each device to balance its local training time and energy consumption.

We define a device set  $D = \{1, 2, 3, \dots, M\}$ , where each device participates in the federated learning process. The local data of each device can be divided into a training set and a validation set, where the size of the local dataset is  $S_i$ , the size of the training

set is  $S_i^{train}$ , the size of the validation set is  $S_i^{val}$ , and the size of the model parameter is  $B$ .

### (1) Communication Model

In this framework, the local models are transmitted between devices using the P2P method. The propagation rate is defined as  $V_{com}$ , and the propagation delay is  $T_{com}$ . The energy loss during propagation can be defined as  $E_i^{com} = T_{com}P_{i,t}$ , where  $P_{i,t}$  represents the transmission power of the device.

### (2) Computation Model

For the local selection and aggregation process performed by each participating node in federated learning, the local training process can be divided into local tips validation and local model computation.

Due to the elimination of the central server in DAG-based federated learning, a local reference model formed by local aggregation replaces the global model, and the local model is temporarily constructed by Tips on the DAG. The number of selected Tips is defined as  $\Upsilon$  ( $\Upsilon \geq 1$ ).

Device  $i$  uses its local computing resources to verify the accuracy of Tips models. The validation latency of device  $i$  is:

$$T_{val} = \frac{\varpi_i S_i^{val} \alpha_i \Upsilon}{f_i} \quad (2)$$

In the above equations,  $\alpha_i$  and  $\varpi_i$  represent the size of one sample data and the number of CPU cycles needed to process each bit of data for device  $i$ , respectively.  $f_i$  is the CPU frequency of device  $i$  during training.

The CPU energy consumption when device  $i$  verification completes multiple tips can be expressed as:

$$E_i^{cmp} = \Upsilon \sum_{x=1}^{\varpi_i S_i^{val} \alpha_i} \beta f_i^2 = \Upsilon \beta \varpi_i S_i^{val} f_i^2 \quad (3)$$

In this equation,  $\beta$  calculates the effective capacitance factor of the chipset for device  $i$ .

The calculation delay of the device updating the model locally is:

$$T_{cmp} = \frac{\varpi_i S_i^{cmp} \alpha_i}{f_i} \quad (4)$$

Given the model, the CPU energy consumption of device  $i$  during a local training can be expressed as:

$$E_i^{cmp} = \sum_{x=1}^{\varpi_i S_i^{cmp} \alpha_i} \beta f_i^2 = \beta \varpi_i S_i^{cmp} f_i^2 \quad (5)$$

Combining the above three delays, the comprehensive training delay and comprehensive energy loss of device  $i$  can be expressed as:

$$T_i = T_{cmp} + T_{val} + T_{com} \quad (6)$$

$$E_i = E_i^{cmp} + E_i^{val} + E_i^{com} \quad (7)$$

The goal of this article is to minimize latency and energy consumption. However, the latency of the device can be reduced by using the highest frequency at any time, but this will increase power consumption, meaning that minimizing energy consumption and latency represents a conflict. Therefore, we need to find a balance between energy cost and learning time to achieve optimization.

$$\text{Minimize}(T_i, E_i) \quad (8)$$

## 4 Resource Allocation Algorithm

Combining the above analysis, we abstract the problem as a multi-objective optimization problem of minimizing both latency and energy consumption, and propose a solution based on a Bezier mutation strategy in a multi-objective differential evolution algorithm. We compare our method with particle swarm optimization (PSO) [10], genetic algorithm (GA) [11], and ant colony optimization (ACO) [12] to analyze the most suitable solution for this problem.

The evolution process of the differential evolution algorithm is similar to that of the genetic algorithm, and is divided into mutation, crossover, and selection steps. The difference is that the DE algorithm uses a differential strategy in the mutation operation [13]. The specific process is as follows:

**Initialization of population:** A population  $X$  consisting of  $NP$  individuals is randomly generated uniformly within the solution space range,  $X_i = (x_{i,1}, x_{i,2}, \dots, x_{i,D}), i \in [1, NP]$ , where each individual  $X_i$  is represented as a  $D$ -dimensional vector.

**Mutation operation:** In each iteration, three individuals are randomly selected from the population, denoted as  $X_{i1}, X_{i2}, X_{i3}$ , and let  $i1 \neq i2 \neq i3$ . Let  $g$  denote the current generation. Based on the  $DE/rand/1$  strategy, the mutation vector is generated as shown in Eq. (9).

$$V_i(g) = X_{i1}(g) + F \cdot (X_{i2}(g) - X_{i3}(g)) \quad (9)$$

where the scaling factor  $F \in [0, 1]$ . Traditional mutation strategies cannot clearly identify local search trajectories nor control the diversity of search trajectories. To address these issues, we introduce the Bezier mutation strategy, which crosses the current best and worst points, allowing for a wider local exploration in the limited space, enhancing the algorithm's search ability and accelerating its convergence rate. The Bezier mutation strategy can balance the complexity of search trajectories and the exploration of space.

Differences in the curvature of different individuals lead to diversity in search trajectories and drive the population to converge in different directions. The Bezier mutation strategy is formulated as follows:

$$V_i(t) = (1 - t)^2 x_{worst} + 2t(1 - t)x_i + t^2 x_{best} \quad (10)$$

where  $x_{best}$  denotes the global optimal individual,  $x_{worst}$  denotes the global worst individual,  $t$  is a parameter that controls the mutation mechanism,  $t \in [0, 1]$ .

The crossover operation combines the mutated individual  $V_i$  with the target individual  $X_i$  to generate a trial individual  $U_i$ , as shown in Eq. (11):

$$u_{i,j}(g) = \begin{cases} v_{i,j}(g) \text{ rand}_{i,j}[0, 1]cr \text{ or } i = i_{rand} \\ x_{i,j}(g) \text{ else} \end{cases} \quad (11)$$

where the crossover rate  $cr \in [0, 1]$ ,  $i_{rand} \in [1, D]$ . If  $\text{rand}_{i,j} \in [0, 1]$  is less than or equal to  $cr$  or  $i = i_{rand}$ , The mutated genes will be included in the trial individual, otherwise the original genes will be included in the trial individual.

Selection operation: For each individual  $U_i$ , compare it with its parent individual. If the fitness of the mutated individual is smaller than that of its parent, then replace it.

$$X_i(g + 1) = \begin{cases} U_i(g) f(U_i(g)) < f(X_i(g)) \\ X_i(g) \text{ else} \end{cases} \quad (12)$$

Our approach to solving the problem is to first determine the objective functions for the multi-objective optimization problem, then determine the range of variable values and the method for generating initial solutions. We then use the differential evolution algorithm based on the Bezier strategy for mutation. It is important to note that the solution to a multi-objective optimization problem is a set of Pareto optimal solutions, which cannot be obtained through single optimization. Therefore, in the differential evolution algorithm, techniques from multi-objective optimization algorithms, such as non-dominated sorting and crowding distance operator, are needed to handle the selection and maintenance of the Pareto optimal solution set.

## 5 Simulation and Experiments

### 5.1 Simulation Parameter Settings

To simulate and verify the effectiveness of the proposed multi-objective differential evolution algorithm based on the Bezier mutation strategy in solving resource scheduling problems, we use Pycharm to model and simulate a new power system environment related to resource scheduling problems. The experiment simulates the process of federated learning training in the new power system environment and sets the CPU frequency and transmission power of the federated learning devices according to the available computing resources. The specific experimental parameters are shown in Table 1.

To solve  $\text{Minimize}(T_i, E_i)$ , 1000 iterations were performed with a population size of 50, and the scaling factor and crossover probability were set to 0.8 and 0.5, respectively. Through experiments, we obtained a set of Pareto optimal solutions for each algorithm.

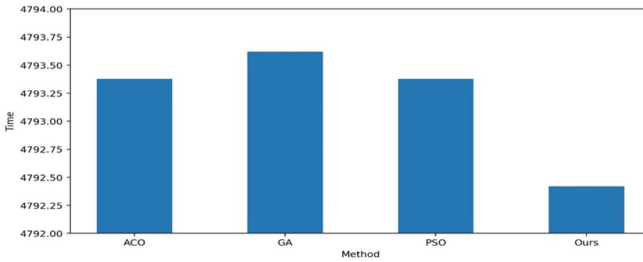
**Table 1.** The specific experimental parameters settings.

Parameter	Meaning	Value
$\alpha_i$	Sample size/bit	24.576
$\varpi_i$	The number of CPU cycles required to process each bit of data/ $cycle \cdot bit^{-1}$	30
$P_{max}$	Maximum transmit power/w	0.2
$f_{max}$	Maximum CPU frequency/ghz	1~2
$f_{min}$	Minimum CPU frequency/ghz	0.1

However, to find the optimal solution from these non-dominated solutions, a specific optimization objective needs to be defined. Here, we use a weighted sum approach to assign different weights to each objective function, and then sort all non-dominated solutions based on a comprehensive index. The top-ranked solution is selected as the optimal solution. Since energy consumption and time are equally important for the experimental results, we set the weights of these two objective functions to 0.5, and the optimization function is transformed into  $Minimize(0.5T_i + 0.5E_i)$ .

**5.2 Experiment and Analysis**

Based on the above steps, the optimal solutions for ACO, GA, PSO, and our method are [2, 3.16E-05], [1.9995, 2.24E-05], [1.9996, 1.66E-05], and [1.9996, 4.77E-05]. The specific comparison charts for latency and energy consumption are shown above (Figs. 3 and 4).



**Fig. 3.** Training time comparison graph

It seems that the our algorithm outperformed the other three algorithms in terms of minimizing the time delay and achieving a good trade-off between energy consumption and time delay. Thus achieving effective resource allocation in the context of a new type of power system based on DAG for federated learning.

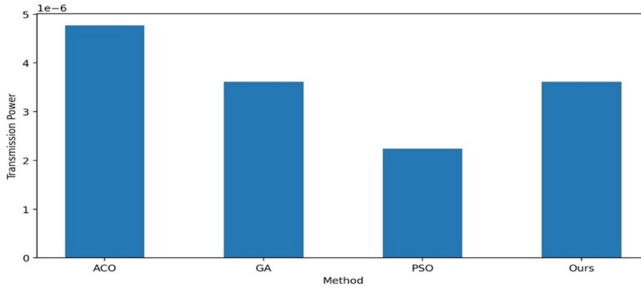


Fig. 4. Comparison chart of equipment energy consumption

## 6 Conclusion

As an important branch of distributed machine learning, federated learning has been widely applied in various intelligent grid businesses such as load forecasting, distributed power equipment fault detection and electricity bill recovery. In this paper, we propose a DAG-based federated learning framework for the new power system scenario. By utilizing the completely decentralized and asynchronous characteristics of DAG structure, this framework accelerates the global aggregation and training speed of federated learning while ensuring data privacy and security. Communication and computation modeling are conducted for the system, and a multi-objective optimization problem is designed for energy consumption and time, based on the expected learning accuracy constraints. A resource allocation algorithm based on differential evolution is proposed to solve this optimization problem of minimizing the completion time and energy consumption loss of the federated learning task. Experimental results show that this strategy balances well between latency and energy consumption. In the future, we will explore the relationship between the learning efficiency and topology structure of DAG federated learning and integrate reinforcement learning into the resource allocation mechanism.

**Acknowledgement.** This work is supported by the science and technology project of State Grid Corporation of China “Research on Key Technologies of New Power System Information Communication Service Infrastructure” (No. 520230220006).

## References

1. Impram, S., Nese, S.V., Oral, B.: Challenges of renewable energy penetration on power system flexibility: a survey. *Energy Strat. Rev.* **31**, 100539 (2020)
2. Bevrani, H., Golpira, H., Messina, A.R., et al.: Power system frequency control: an updated review of current solutions and new challenges. *Electr. Power Syst. Res.* **194**, 107114 (2021)
3. Feng, L., Zhao, Y., Guo, S., et al.: BAFL: a blockchain-based asynchronous federated learning framework. *IEEE Trans. Comput.* **71**(5), 1092–1103 (2021)
4. Cao, M., Zhang, L., Cao, B.: Toward on-device federated learning: a direct acyclic graph-based blockchain approach. *IEEE Trans. Neural Netw. Learn. Syst.* (2021)

5. Beilharz, J., Pfitzner, B., Schmid, R., et al.: Implicit model specialization through dag-based decentralized federated learning. In: Proceedings of the 22nd International Middleware Conference, pp. 310–322 (2021)
6. Cui, Y., Cao, K., Cao, G., et al.: Client scheduling and resource management for efficient training in heterogeneous IoT-edge federated learning. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* **41**(8), 2407–2420 (2021)
7. Lim, W.Y.B., Ng, J.S., Xiong, Z., et al.: Decentralized edge intelligence: a dynamic resource allocation framework for hierarchical federated learning. *IEEE Trans. Parallel Distrib. Syst.* **33**(3), 536–550 (2021)
8. Jithish, J., Alangot, B., Mahalingam, N., et al.: Distributed anomaly detection in smart grids: a federated learning-based approach. *IEEE Access* (2023)
9. Singh, P., Masud, M., Hossain, M.S., et al.: Privacy-preserving serverless computing using federated learning for smart grids. *IEEE Trans. Industr. Inf.* **18**(11), 7843–7852 (2021)
10. Eberhart, R., Kennedy, J.: Particle swarm optimization. In: Proceedings of the IEEE International Conference on Neural Networks, vol. 4, pp. 1942–1948 (1995)
11. Mirjalili, S., Mirjalili, S.: Genetic algorithm. In: Evolutionary Algorithms and Neural Networks: Theory and Applications, pp. 43–55 (2019)
12. Dorigo, M., Birattari, M., Stutzle, T.: Ant colony optimization. *IEEE Comput. Intell. Mag.* **1**(4), 28–39 (2006)
13. Storn, R.: On the usage of differential evolution for function optimization. In: Proceedings of North American Fuzzy Information Processing, pp. 519–523. *IEEE* (1996)



# Reliable Data Interaction Scheme Based on Oblivious Transfer Technology in Smart Grid

Pengzhan Sun<sup>(✉)</sup>, Feng Qi, Xingyu Chen, Xuesong Qiu, and Yinlin Ren

Beijing University of Posts and Telecommunications, Beijing 100876, China  
sunpengzhan2021@163.com

**Abstract.** With the accelerated transformation of the development of new power systems, the data interaction between the data center and the edge of the business system is increasingly frequent, which challenges the reliability and privacy security of the data in the interaction process. The existing data interaction schemes based on data anonymity usually rely on the trusted third party (TTP). However, the TTP has the risk of a single point of failure and internal leakage. At the same time, the terminal can easily be hijacked and become a medium to disrupt system decisions maliciously due to the lack of security protection of edge networks. To solve these problems, this paper proposes a reliable data exchange scheme based on the oblivious transfer (OT) technology in the smart grid. Experiments show that this scheme can achieve the protection of user privacy without excessive overhead while getting rid of the dependence on the TTP.

**Keywords:** Smart grid · Oblivious transfer · Elliptic curve encryption · Intelligent terminal

## 1 Introduction

With the construction of the new power system, the data interaction between smart meters (SM) and data centers (DC) has become increasingly frequent. Such terminals are widely distributed on the edge side, showing the characteristics of a wide range of data collection and a short interaction cycle. Traditional data interaction schemes have unreliable problems, leading the power grid to make wrong decisions and risk endangering user privacy.

There are three main types of existing user privacy protection schemes for billing purposes [1], based on trusted platform module (TPM), cryptographic protocol, and TTP. TTP is more suitable for data security interaction in the power grid in terms of performance and scalability considering the resource limitation. The common methods of TTP include data obfuscation, data aggregation, data anonymity. Compared with the other two methods, the data anonymization method has more advantages in cost and data effectiveness. Many researchers and institutions have proposed anonymous user privacy protection schemes. Ambrosin et al. [2] proposed an anonymous fine-grained data collection scheme with a verification center like TTP to ensure the normal operation of the smart meter. Zhang et al. [3] proposed a certificateless ring signcryption scheme.



Afrin and Mishra [4] proposed an anonymous authentication framework based on an entity named Anonymizer. Xia et al. [5] proposed a privacy protection scheme based on a virtual ring. These schemes usually rely on the third-party entity to realize their security, and the third-party entity must be honest and trusted. However, it is difficult to guarantee this in practice. According to the ENISA report in 2017, insider threats account for more than 20% of the threats in the past six years [6]. At the same time, this centralized approach suffers from a single point of failure. If the trusted third party suddenly fails to provide services, the data interaction between the cloud and the edge will be affected. Therefore, this kind of scheme has the problem of untrusted transmission. At the same time, most of these schemes assume that the SM is safe and do not consider the problem of SM hijacking. The SM are easily hijacked by attackers, pretending to be normal SM and uploading false data to perform various malicious activities against the power system, such as botnets. The data source may be not trusted.

In response to the above problems, this paper proposes a reliable data interaction scheme based on OT protocol, in which the intelligent terminal in the station area is used as the security agent between the terminal and the power system to participate in the data interaction process, and a trusted evaluation module is deployed on it to conduct trusted detection of subordinate terminals to ensure the security and credibility of edge side terminals. At the same time, the intelligent terminal in the station is used to manage the generation and maintenance of anonymous identity. The intelligent terminal in the station is combined with the Oblivious Transfer technology (OT) to complete the conversion process of anonymous identity and real identity without relying on TTP to protect the privacy and security of user data.

## 2 Reliable Data Exchange Scheme Based on OT Technology

This section introduces the reliable data exchange scheme based on OT technology proposed in this paper. Figure 1 shows three interactive entities in the proposed scheme: data center (DC), Intelligent Terminal (IT)  $ITs = \{IT_1, \dots, IT_m\}$ , and smart meters (SM)  $SMs = \{SM_1, \dots, SM_n\}$ . The IT in the station area is responsible for generating anonymous identities and collecting user data of subordinate SM. The set of SM affiliated with the IT in each station area is defined as a delegation domain.

### 2.1 Source Reliability Based on Trust Evaluation

In order to solve the problem of untrusted sources, this scheme deployed the trust evaluation module based on artificial intelligence on IT to evaluate the SM. In this scheme, the time dimension of the system is divided into several time slots, and  $Ts = \{1, \dots, t, \dots, T\}$  is the set of time slots.  $T_d$  is the duration of each time slot  $t$ . The module collects subordinate SM's multi-source activity data on a cycle of  $T_d$ , including traffic and log data. For time slot  $t$ , IT will collect the activity data  $D_t^i$  (including traffic and log data) of the smart meter  $SM_i$  in the period of  $T_d$ . After preprocessing,  $D_t^i$  will be submitted to the trust evaluation model for scoring. The scoring result represents the reliability degree of  $SM_i$  in time slot  $t$ , and it will be combined with the historical score

to generate the trust score  $S_t^i$  representing the current state of  $SM_i$ . The higher the risk, the calculation is as follows:

$$S_t^i = (1 - \alpha)S_{t-1}^i + \alpha Model(D_t^i), S_t^i \in [0, 1] \quad (1)$$

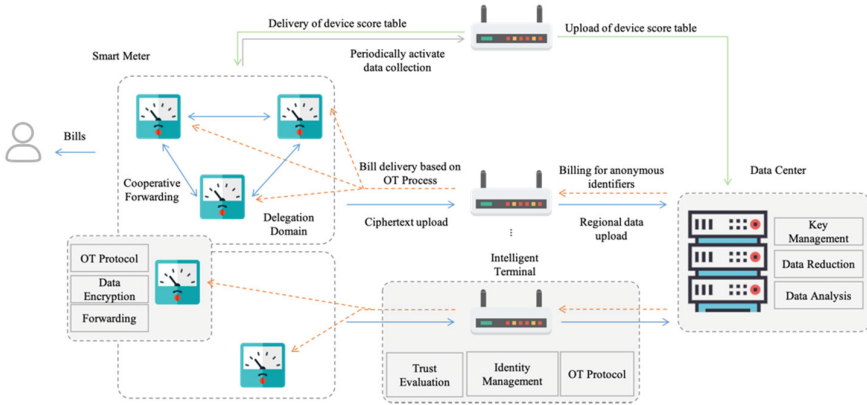
where  $D_t^i$  represents the activity data of  $SM_i$  in time slot  $t$ ,  $S_{t-1}^i$  represents the historical score of  $SM_i$  in the last time slot,  $S_t^i$  represents the latest trust score of  $SM_i$  after combining the behavior score in time slot  $t$ ,  $\alpha$  represents the influence of the behavior score in time slot  $t$  on the overall score, as a reference for subsequent data interaction.  $Model()$  is a neural network model that outputs the behavior score of the  $SM_i$  within time slot  $t$ .

After the score  $S_t^i$  corresponding to  $SM_i$  is obtained,  $S_t^i$  and  $SM_i$  identification information  $ID_{sm}^i$  will form a key-value pair  $(ID_{sm}^i, S_t^i)$ , which will be saved in the local IT to generate the device score table  $Tab_{trust} = \{(ID_{sm}^i, S_t^i) | i = 1, \dots, n\}$ .  $Tab_{trust}$  can reflect the overall security situation of the SM subordinate to the IT and will be shared with SM and DC, as shown in Fig. 1. In the system initialization phase, it is necessary to set the parameters such as cycle  $T_d$ , start time, and collection data type. When the new  $SM_i$  is registered, it will be verified for security, and the default value will be set to 1.

## 2.2 Trusted Transmission Based on Intelligent Terminal

In order to solve the problem of untrusted transmission, this paper adopts a non-aggregated data anonymization scheme, which uses IT to replace fog nodes or TTP to realize data collection and anonymization processing. In the initialization phase of the system, the DC generates the key used for data transmission and distributes the public key to each IT. The public key and the anonymous identity used in data transmission are obtained from the IT through the registration operation. During the data interaction, the anonymous identity is used to identify the user, and the user data is encrypted with the public key and sent to the IT. After receiving the ciphertext data, the IT verifies the validity of the data and forwards it to the data center. After receiving the anonymous user bill, the IT will assign the bill to the SM according to the anonymous identity, and the SM will deliver the bill to the corresponding user, as shown in Fig. 1.

Different from the TTP, which is an independent third party involved in the data transmission process, the IT is an important part of the smart grid, which undertakes important functions such as data collection, status monitoring, and indicator analysis. If the IT is directly used to replace the TTP to complete the data collection and anonymous processing tasks, there will be a situation in that IT and DC conspire to obtain user privacy, so it is necessary to reform this process. In this paper, it is assumed that DC knows the relationship between SM and user, and in the process of data transmission, there are three links that may lead to the disclosure of user privacy, which are anonymous identity acquisition, data upload, and bill delivery. A) Anonymous identity acquisition. When SM joins the smart grid, it needs to register with IT and obtain the key and anonymous identity from IT. If the direct distribution method is adopted, IT knows the relationship between the anonymous identity and SM, and DC knows the relationship between SM and the user. DC can know the user corresponding to the anonymous identity. B) Data upload. In the process of data upload, IT will collect user data from SM, which is equivalent



**Fig. 1.** Data security interaction based on the intelligent terminal

to IT knowing the relationship between data and SM, and DC can determine the user identity corresponding to anonymous data through the relationship. C) Bill delivery. In this step, the IT needs to know the relationship between the bill and SM before it can deliver the bill to the corresponding SM. However, because the bill is identified by an anonymous identity, the IT can indirectly obtain the relationship between the anonymous identity and SM through the relationship between the bill and SM. In this paper, dynamic anonymous identity management, cooperative forwarding, and OT protocol are used to solve the hidden dangers existing in the above links and realize the separation of data and specific user identity.

**2.2.1 Parameter Initialization**

In this paper, DC uses the ECC algorithm to generate the key required for encryption. The elliptic curve cryptography algorithm is widely considered to be the best asymmetric algorithm in the case of a given key length. The initialization process is as follows:

- (1) Chose an elliptic curve  $E_p(a, b)$ :

$$y^2 = x^3 + ax + b(modp), x, y \in [0, p - 1] \tag{2}$$

where p is a prime number, and a and b satisfy  $4a^3 + 27b^2 \neq 0$ . Take a point  $G(x, y)$  on the elliptic curve as the base point, determine the order n of G (n is a prime number).

- (2) Determine the private key  $k(k < n)$ , and generate the public key  $Q = kG$ .
- (3) DC sends the curve  $E_p(a, b)$ , public key  $Q$ , and base point  $G$  to IT and stores them locally in IT. When SM registers with IT, it sends them to SM, and the private key is stored in DC.

### 2.2.2 Dynamic Anonymous Identity Management

In order to solve the collusion problem of IT and DC, this scheme designed a dynamic anonymous identity management mechanism in anonymous identity assignment. SM needs to have an anonymous identity before participating in data sharing, and the anonymous identity is managed and allocated by IT. The newly joined SM first registers with IT. The registration process is as follows:

- (1) When the SM requests the IT, it will send the verification information and the registration request to the IT, and the IT will send the verification request to the DC after receiving the request.
- (2) DC will check upon receipt and inform IT after successful verification. After IT confirms, it will generate a set of anonymous identity  $IDS_{an} = \{an_1, \dots, an_k\}$  and jump times  $c$ , which will be assigned to SM with public key  $Q$  and the device score table  $Tab_{trust}$ .
- (3) After receiving, SM will randomly choose an anonymous identity  $an_i$  from  $IDS_{an}$  and save it locally, then remove the identity from  $IDS_{an}$ , subtract  $c$  by 1, and send the remaining identity  $IDS_{an} - an_i$  to the next SM, which is randomly selected from the high trust score SM of  $Tab_{trust}$ .
- (4) The received SM decides with probability  $P$  whether to pick one of them to replace its original identity. If so, it will be removed from the  $IDS_{an}$ ,  $c = c - 1$ , and sent to the next SM in the delegation domain.
- (5) If  $IDS_{an}$  are nonempty and  $c > 0$ , repeat (4). Otherwise, it ends.

### 2.2.3 Cooperative Forwarding

In the data upload process, this paper adopts cooperative forwarding to realize the separation of data and SM. In this method, the user data of SM ( $SM_{source}$ ) is not directly uploaded to IT but indirectly forwarded by other SM ( $SM_{transfer}$ ) in the same domain. However, SM with a high score is selected as  $SM_{transfer}$  according to the score table  $Tab_{trust}$  obtained from IT. At the same time, in the process of selection, multiple  $SM_{source}$  may select the same SM as  $SM_{transfer}$ . Considering the limitation of SM resources, the SM cannot afford such a scale of forwarding tasks. To solve this problem,  $SM_{source}$  will select multiple SM as  $SM_{transfer}$  from  $Tab_{trust}$  and deliver the data to the corresponding  $SM_{transfer}$  after fragmentation, and finally reproduce in DC. In this mode, on the one hand, the amount of data processed by  $SM_{transfer}$  can be balanced to avoid the extreme situation that a single  $SM_{transfer}$  handles all forwarding requests around it. On the other hand, data security can be improved because a  $SM_{transfer}$  can only obtain a part of the complete user data, and only DC can obtain all the data fragments to reassemble the complete user data. The complete process is as follows:

$SM_{source}$  to  $SM_{transfer}$ : At the beginning of data upload,  $SM_i$  will select  $l$  high score SM from  $Tab_{trust}$ , from which  $t$  SM will be selected to form  $SM_{transfer}$  set  $SMS_{transf} = \{SM_1, \dots, SM_t\}$ . After determining  $SMS_{transf}$ ,  $SM_i$  will fragment the transmitted data  $D_j$  and divide it into a set of data sub-slices  $Ds_i = \{D_i^1, \dots, D_i^l\}$  to ensure that the information of the overall data cannot be deduced from a single  $D_i^j$  as much as possible. After fragmentation,  $SM_i$  will concatenate its anonymous identity  $an_i$  with each data slice to generate plaintext message  $u_j = an_i || D_i^j$  and obtain plaintext message set

$us = \{u_1, \dots, u_t\}$ .  $SM_i$  will use public key  $Q$  to encrypt the plaintext message in  $us$  to generate ciphertext message  $m_j = \text{Encrypt}_Q(u_j)$  and obtain ciphertext set  $ms = \{m_1, \dots, m_t\}$ , and then forward the message in  $ms$  to SM in  $SMs_{transf}$ .

$SM_{transfer}$  to IT: After receiving the forwarding message,  $SM_{transfer}$  will query the score corresponding to  $SM_{source}$  from  $Tab_{trust}$ , reject the message from low-scoring  $SM_{source}$ , accept the ciphertext message from high-scoring  $SM_{source}$ , and upload the ciphertext message to IT.

IT to DC: IT will query the score corresponding to the  $SM_{transfer}$  sending message from  $Tab_{trust}$ , discard the message with a low score, cache it locally with a high score, and finally upload it to DC uniformly.

Through the three trusted queries of  $SM_{source}$ ,  $SM_{transfer}$ , and IT, it can ensure that the participating entities in the whole data upload process are high-score entities.

## 2.2.4 Bill Delivery Based on Oblivious Transfer Technology

In the process of bill delivery, this paper uses OT technology to achieve the anonymity of the real user identity. DC delivers the user bill with an anonymous identifier to each IT and then sends it to the corresponding subordinate SM. The bill delivery of IT can be transformed into a query problem. SM queries the corresponding user bill from IT according to the anonymous identity. OT technology can ensure that IT cannot obtain SM query content. The bill delivery process is as follows:

DC to IT: DC receives the ciphertext set  $M_{IT} = \{m_1^1, \dots, m_n^1\}$  uploaded by IT and needs to perform decryption and reassembly operations on  $M_{IT}$ . In the decryption process, DC uses the private key  $k$  to decrypt the ciphertext fragments  $m_i$  in  $M_{IT}$  in turn to obtain the plaintext data  $u_j = an_i || D_i^1 = \text{Decrypt}_k(m_i^1)$  and reorganizes the data fragments from the same SM according to the  $an_i$  in  $u_j$  to obtain the complete user data  $D_i$ . After obtaining the user data, DC will analyze  $D_i$  and generate the user bill  $b_i$ . When delivering a bill, DC combines the user bill  $b_i$  with the corresponding anonymous identity  $an_i$  to generate the message  $B_i = an_i || b_i$ , and obtains  $m$  groups of message sets  $Bs = \{B_1, \dots, B_n\}$ . When delivering a bill, DC will send these  $m$  groups of  $Bs$  to the corresponding IT.

IT to SM: When the IT receives the  $Bs$ , it will initiate an OT interaction request with the affiliated SM and send the bill  $b_i$  to the  $SM_i$  whose anonymous identity is  $an_i$  through the OT protocol. The IT can know that the  $SM_i$  queried its bill from the  $Bs$ , but it cannot determine which specific bill was queried by the  $SM_i$ . The anonymity of  $b_i$  in the corresponding  $SM_i$  query can be well guaranteed by OT protocol in the interaction process. The OT protocol in this paper adopts the scheme proposed by Tzeng [7], and the specific process is as follows:

- (1) IT determines the system parameters  $(g, h, G_q)$ , where  $G_q$  is a group of order  $q$ ,  $q$  is a large prime number,  $g$  and  $h$  are two generators of  $G_q$ . At the same time, the anonymous index table  $Tab_{index}$  is generated. The parameters and  $Tab_{index}$  are shared to the subordinate  $SM_i$ .
- (2) When  $SM_i$  obtains the parameters  $(g, h, G_q)$  and  $Tab_{index}$ , it participates in the OT interaction process.  $SM_i$  will generate a random number  $r$ ,  $r \in Z_q$  and save  $r$ .  $SM_i$

determines the index  $i$  of anonymous identity  $an_i$  according to  $Tab_{index}$ , calculates  $y = g^r h^i$  by  $r$  and  $i$ , and then  $SM_i$  will send  $y$  to IT.

- (3) After receiving  $y$ , IT will generate a random number  $d$ ,  $d \in Z_q$  and calculate  $a = g^d$ , and  $c_i = b_i \otimes H((y/h^i)^d, i)$ , where  $H()$  is a cryptographic strong hash function. Finally, the IT will send the encrypted data  $(a, c_1, \dots, c_n)$  to the  $SM_i$ .
- (4) When the  $SM_i$  receives  $(a, c_1, \dots, c_n)$ , it will use the parameters  $r, a$ , and  $c_i$  generated in steps 2 and 3 to calculate  $b_i = c_i \otimes H(a^r, i)$ , which is the electricity bill of the  $SM_i$  user, and the  $SM_i$  will send the bill to the user.

In the data interaction scheme proposed in this paper, IT and DC can confirm that the SM participating in data interaction is trusted through the device score table, and  $SM_{source}$  can ensure that the  $SM_{transfer}$  forwarding data is a trusted SM, which eliminates the participation of untrusted SM and solves the problem of the untrusted source. In the data upload process, the relationship between data and source SM can be unlinked through the cooperative forwarding between SM. In the process of data delivery, the IT, instead of the TTP, complete the delivery of user bills by using OT technology to avoid the risk of internal leakage and single point in TTP. In the interaction process, no entity except DC has the opportunity to obtain the complete user data and bill, which solves the untrusted transmission problem.

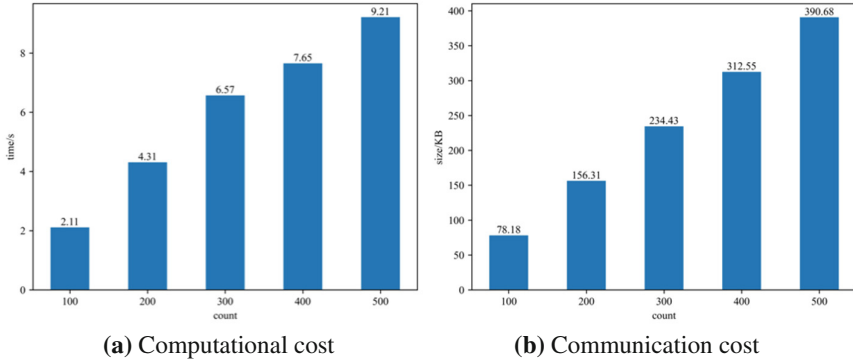
### 3 Scheme Analysis and Experiment

This section evaluates the performance of the proposed method and analyzes the computational and communication costs of the proposed scheme. In the experiment, this paper uses Pytorch, phe, and tinyec libraries to simulate the data interaction process to evaluate the cost of the scheme. The experimental environment is Win10, 2.5 GHz Intel Core i5 CPU, 16GB RAM, and Python3.

In this scheme, the cost can be divided into two parts, the cost of trust evaluation and the cost of data exchange. The former is borne by IT, and the latter is borne by SM, IT, and DC.

#### 3.1 The Cost of Trust Evaluation

In the evaluation of the trust evaluation cost, the computational cost are defined as the time consumption of the model to analyze the data, and the communication cost are defined as the communication cost generated by collecting the user data. The hybrid data set composed of the HDFS [8] and N-BaIoT [9] datasets is used to simulate the computation time of the model in the trust evaluation. In the simulation, it is assumed that the activity data generated by each SM in each period is 100 samples, the different number of SM is set, and the evaluation model is used to calculate the evaluation delay of the corresponding dataset. (a) is the calculation delay of a trust evaluation when the number of SM is different in Fig. 2. When the number of SM is 100, 200, 300, 400, and 500, the computational cost is about 2.11, 4.31, 6.57, 7.65, and 9.21 s, respectively. (b) shows the communication cost generated by a trust evaluation under the assumed conditions in Fig. 2. When the number of SM is 100, 200, 300, 400, and 500, it is about 78.18, 156.31, 234.43, 312.55, and 390.68 KB, respectively, which is mainly generated by the activity data collection between IT and SM.



**Fig. 2.** The cost of trust evaluation

### 3.2 The Cost of Data Interaction

The computational cost of data interaction mainly comes from three steps, which are the encryption operation performed by SM when data is uploaded, the decryption operation performed by DC after the ciphertext data is collected, and the OT protocol executed between IT and SM when the bill is delivered. The computational cost involves SM, FN (fog node devices, such as IT or BG), and DC. The three types of entities contribute different computational costs, respectively, and the lighter operation overhead, such as addition operation, is ignored in the calculation. The applied symbols and definitions are shown in Table 1. At the same time, this scheme is compared with scheme [3] and scheme [5]. In the scheme,  $n$  is assumed to be the number of SM, the computation cost of a single SM is denoted as  $T_{enc} + 3T_{eq} + T_{mq}$ , the computation cost of FN is denoted as  $(2n + 1)T_{eq}$ , and the computation cost of DC is denoted as  $nT_{dec}$ . In scheme [3], these costs are respectively  $2T_m + (2n + 5)T_{mq}$ ,  $4T_{mq} + T_{enc}$ , and  $nT_{dec}$ , and in scheme [5], these costs are respectively  $2T_e + T_m + T_{sig} + T_{enc}$ ,  $n(T_{ver} + T_{dec}) + (n - 1)T_m$ , and  $T_e$ . Obviously, compared with schemes [3, 5], this scheme requires less computing resources for SM, and the computing cost generated on IT or fog nodes is mainly the exponential operation required to execute OT protocol in the bill delivery process.

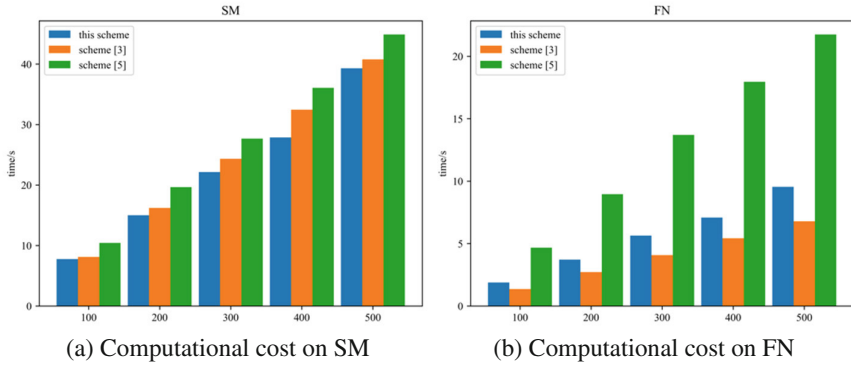
In scheme [3], this portion of the cost is the responsibility of the TTP. At the same time, this section simulates and tests the actual computing cost. The dataset adopted for the experiments is the REFIT electrical load measurement dataset [10], which includes clean electricity consumption data (in watts) for 20 households at the aggregate and device level with a timestamp and sampling interval of 8 s. Because the ECC algorithm is used in this scheme, the data needs to be plaintext encoded and mapped to a point on the elliptic curve before encryption, and the koblitz method [11] is used to realize this process in the experiment. Through simulation, the average time for a single SM in this scheme to encrypt plaintext data into ciphertext data is about 70ms. When DC performs data decryption, the time to decrypt the ciphertext data provided by a single SM is about 16 ms and the total time increases as the number of SM increases.

This paper compares the proposed scheme with the schemes [3, 5]. This experiment is based on ECC and Paillier encryption algorithm to reproduce the scheme [3] and scheme [5]. In this scheme and scheme [3], data uploading of SM is a parallel process,

**Table 1.** Symbol and definitions

Symbol	Definition
$T_{enc}$	Encryption operation of a single SM data
$T_{dec}$	Decryption operation of a single SM data
$T_{sig}$	The signing operation of a single SM data
$T_{ver}$	Signature verification operation for a single SM data
$T_e$	Exponentials on $Z_q$
$T_m$	Multiplication on $Z_q$
$T_{eq}$	Exponentials on $G_q$
$T_{mq}$	Multiplication on $G_q$

and multiple SM can be executed at the same time. In contrast, the data uploading of reference [5] scheme is a serial process of constructing a virtual ring, and terminals on the same virtual ring cannot be carried out simultaneously. As shown in (a) of Fig. 3, the computational cost in the figure is the sum of the computational cost of all SM. The computational cost of the proposed scheme includes the cost of encrypted uploading and executing OT protocol, which increases with the increase of the number. The proposed scheme's computational cost is less than schemes [3, 5]. Compared with the scheme [3], it is 0.361, 1.217, 2.181, 4.579, 1.47s, respectively, and compared with the scheme [5], it is 2.683, 4.646, 5.51, 8.209, 5.603s, respectively.

**Fig. 3.** Computational cost

(b) Shows the computational cost of multiple schemes on the fog node devices between SM and DC in Fig. 3. In order to simulate the execution process of the OT protocol of this scheme, the snowflake algorithm is used to generate a set of anonymous identity sets, and data is extracted from the REFIT dataset to simulate the billing dataset. In the process of execution, the terminal needs to communicate three times if it wants to get the corresponding bill from the IT. In the experiment, the oblivious transmission



process between IT and SM was simulated when the bill number was 100, 200, 300, 400, 500. The cost of this scheme was slightly higher than that of the scheme [3] but less than that of the scheme [5] and about 0.52, 1.003, 1.57, 1.659, 2.755 s higher than that of the scheme [3]. Compared with the scheme [5], it is reduced by about 2.795, 5.239, 8.069, 10.869, and 12.212 s.

## 4 Conclusion

To solve these problems, this paper proposes a reliable data exchange scheme based on OT technology in smart grid. This scheme evaluates the status of smart meters by analyzing the multi-source activity data of SM through the trusted evaluation module deployed on the IT and uses the IT to manage the generation and maintenance of anonymous identities. In this way, the trust evaluation of the terminal is used to ensure the trust of the source of the interaction, and the OT technology is used between SM and IT to get rid of the dependence on the TTP and ensure the trust of the interaction transmission. Finally, the experimental results show that the scheme can share fine-grained data and get rid of the dependence on TTP, and realize the protection of user privacy. Meanwhile, compared with other schemes, this scheme has certain advantages in the computing cost of data interaction.

**Acknowledgement.** This work is supported by National Key R&D Program of China (2022YFB3105102).

## References

1. Sultan, S.: Privacy-preserving metering in smart grid for billing, operational metering, and incentive-based schemes: a survey. *Comput. Secur.* **84**, 148–165 (2019)
2. Ambrosin, M., Hosseini, H., Mandal, K., et al.: Despicable me(ter): anonymous and fine-grained metering data reporting with dishonest meters. In: 2016 IEEE Conference on Communications and Network Security (CNS), pp. 163–171. IEEE, Philadelphia, PA, USA (2016)
3. Zhang, S., Zhao, Y., Wang, B.: Certificateless ring signcryption scheme for preserving user privacy in smart grid. *Autom. Electr. Power Syst.* **42**(3), 118–123 (2018)
4. Afrin, S., Mishra, S.: An anonymized authentication framework for smart metering data privacy. In: IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1–5. IEEE, Minneapolis, MN, USA (2016)
5. Xia, Z., Zhang, Y., Gu, K., Zhou, K., Li, X.: Virtual ring privacy preserving scheme based on fog computing for smart meter system. *J. Electron. Inf. Technol.* **45**(3), 819–827 (2023)
6. ENISA Threat Landscape Report 2016. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016>. Accessed 15 April 2023
7. Tzeng, W.G.: Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters. *IEEE Trans. Comput.* **53**(2), 232–240 (2004)
8. Xu, W., Huang, L., Fox, A., et al.: Detecting large-scale system problems by mining console logs. In: Proceedings of the ACM SIGOPS 22nd Symposium on Operating Systems Principles, pp. 117–132, Association for Computing Machinery, New York, NY, United States (2009)

9. Meidan, Y., Bohadana, M., Mathov, Y., et al.: N-baiot—network-based detection of iot botnet attacks using deep autoencoders. *IEEE Pervasive Comput.* **17**(3), 12–22 (2018)
10. Murray, D., Stankovic, L., Stankovic, V.: An electrical load measurements dataset of United Kingdom households from a two-year longitudinal study. *Sci. Data* **4**(1), 1–12 (2017)
11. Trappe, W., Lawrence, C.W.: *Introduction to Cryptography with Coding Theory* (2004)



# Research on FlexE Network Routing Algorithm for High Traffic Services

Ruilin Wang<sup>(✉)</sup> and Zhili Wang

State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China  
{wrl, zlwang}@bupt.edu.cn

**Abstract.** Compared with traditional Ethernet, FlexE network has the advantages of flexible and variable multi-grain rates, decoupling from the optical transmission capability, IP and optical convergence networking, and enhanced QoS for multi-service bearers. In this context, an algorithm (JLRB algorithm) is designed in this paper for FlexE networks with high traffic services. This paper first introduces the FlexE network technology and the research background, and then two factors: load balancing and risk balancing to be considered and optimized by the algorithm are analyzed. In the next section, the expressions of each parameter in the algorithm are defined and the specific procedure of the algorithm is designed. In the simulation experiments, the performance of the proposed algorithm is tested and compared with the comparison algorithm (LRWS algorithm). The superiority of the designed algorithm is proved by the comparison experiments with the comparison algorithm.

**Keywords:** FlexE network · Load balancing · Risk balancing

## 1 Introduction

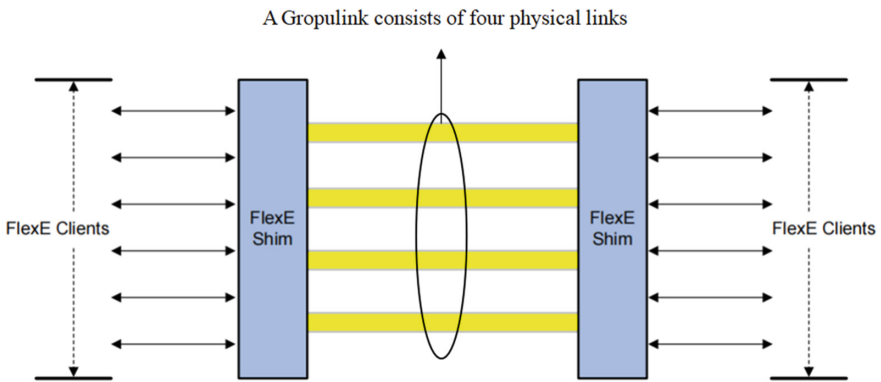
Flexible Ethernet (FlexE) is a technology developed on the basis of Ethernet to meet the needs of high-speed transmission and flexible bandwidth configuration. Since the 1980s, the development of Ethernet technology fully follows the standard architecture set by IEEE 802.3, and is rapidly developing under the joint drive of industrial technology and business needs, becoming the most widely used L2 interconnection technology with the most complete ecosystem in the IT industry. Ethernet technology follows the MAC/PHY layer standard defined by IEEE 802.3 at the interface level, and develops according to the evolution path of 10G-25G-50G-200G-400G-800G.

In recent years, with the rise of services such as cloud computing, video and mobile communications, people's demands on IP networks have gradually shifted from focus on bandwidth to service experience, quality of service and networking efficiency. In order to meet the above requirements, Ethernet as the underlying connection technology, in addition to keeping the advantages of low cost, high reliability and operation and maintenance, also needs the following capabilities: flexible and variable multi-grain

rates, decoupling from the optical transmission capability, IP and optical convergence networking, enhanced QoS capability for multi-service bearing.

The FlexE technology was created by introducing the FlexEShim layer on the basis of IEEE802.3 to decouple the MAC layer from the PHY layer, thus enabling flexible rate matching. In the FlexE network, multiple Ethernet PHYs are combined together as a FlexEGroup and carry one/multiple FlexEClient data streams distributed and mapped through FlexEShim. In this way, FlexE implements three functions: ① Binding: bundling multiple IEEE 802.3 standard physical interfaces so that multiple PHYs can work together to support higher rates. ② Sub-rate: lower-rate data streams share one PHY or multiple PHYs. ③ Channelization: multiple lower-rate data streams share one PHY or multiple PHYs.

FlexEShim layer can divide each 100GE PHY(also 50GE) in a FlexE Group into 20 time slots of data bearing channels, each PHY corresponding to this group of time slots is called a Sub-calendar, where the bandwidth corresponding to each Slot is 5 Gbps.



**Fig. 1.** GroupLink structure

Figure 1 shows an example of the link structure between two FlexEGroups. Each FlexEGroup consists of four PHYs. Four physical links form a logical GroupLink (a link not specifically described in this paper refers to such a GroupLink composed of several physical links).

The routing function of FlexE devices and management software generally uses the shortest path routing. The current research lacks the study of routing strategies for networks composed of FlexE devices in different service scenarios, and lacks further division and planning of the degree of protection for different types of services. In this paper, we proposed a routing algorithm for FlexE networks with high-traffic services, and verified the advantages of this algorithm, which can improve network utilization, reduce network risks, and enable more efficient utilization of resources.

## 2 Related Work

FlexE networks and network routing algorithms have been studied and applied by a number of scholars. Reference [1] and reference [2] verified the effectiveness of FlexE hard slicing on network resource utilization enhancement. Reference [3] investigated the application of FlexE devices to edge nodes of multi-layer multi-domain networks formed by combining IP networks with optical networks, and their algorithms for time slot allocation and routing computation. The cross-layer routing planning problem for both single-hop and multi-hop scenarios in the case of combined FlexE and Elastic Optical Network is discussed in reference [4]. Reference [5] uses the Long Short Term Memory model to predict the next moment service traffic and dynamically allocate the time slot resources to improve the resource utilization. In reference [6], hybrid multiplexing of FlexE groups is used to improve the utilization of group bandwidth resources. Reference [7] proposed a route balancing algorithm for managing the degree of balancing of small granularity service slices, but this study did not consider service characteristics or distinguish node types. Reference [8] proposed a load balancing technique (LBT) that can be used for different networks. Reference [9] studied a joint routing algorithm using load balancing and risk balancing in power networks. Reference [10] proposed a service-based routing wavelength assignment (RWA) algorithm in power optical transmission networks. The algorithm is designed to solve the problem of routing wavelength assignment for multiple service level requests in complex power optical transmission network topology. Two load balancing algorithms with different objectives are provided in reference [11]. Reference [12] and reference [8] investigated the load balancing mechanism in resilient optical networks. Reference [13] investigated the algorithm for balancing based on service importance, which is helpful for the risk balancing idea in this paper.

It can be seen that the current research lacks the study of routing strategies for networks composed of FlexE devices in different scenarios, as well as the further division and planning of routing and protection strategies for different types of services. This paper takes this aspect as the starting point for research.

## 3 Algorithm Design for Joint Load and Risk Balancing

The routing algorithm studied in this paper focuses on high-traffic services. The business characteristics of such services are listed as follows: high traffic, high bandwidth demand, tight FlexE resources, and relatively low delay sensitivity and reliability requirements. In such a scenario, bandwidth resources are relatively tight, so 1:N protection is used for such services. A typical service example is the IPTV service.

The routing of such services needs to consider the following two factors: load balancing and risk balancing. The routing algorithm designed in this paper considers the optimization degree of both factors in a balanced way, i.e., the joint optimization of load balancing and risk balancing is used as the routing strategy.

### 3.1 Load Balancing Analysis

As bandwidth resources for high traffic services are tight, so using the idea of load balancing for routing planning can improve network resource utilization, increase the

number of bearable services, and prevent congestion. This paper proposes the parameter load weight as one of the metrics for routing. Displayed equations are centered and set on a separate line. The load weight of link  $xy$  ( $C1(x, y)$ ) is calculated as follows:

$$C1(x, y) = \frac{C0}{s(x) * [1 + k(x)] * s(y) * [1 + k(y)] * w(x, y)} \quad (1)$$

In expression (1),  $C0$  is a constant.  $s(x) = \frac{\text{freeslot}}{\text{phynum} \times \text{slotnum}}$  indicates the service admission capacity of node  $x$  (the number of free time slots of node  $x$  as a percentage of the number of all time slots of node  $x$ ).  $k(x) = \frac{\text{freephy}}{\text{phynum}}$  indicates the ability of node  $x$  to add the remaining group links again (the number of unused PHY of node  $x$  as a percentage of the total number of PHY of node  $x$ ).

$w(x, y) = \frac{\text{freebandwidth}}{B(x, y)}$  indicates the unused bandwidth on link  $xy$  as a percentage of the total bandwidth of link  $xy$  ( $B(x, y)$ ).

### 3.2 Risk Balancing Analysis

Since most of the protection policies for high traffic services use 1:N protection, which is a low level protection, so during the routing process, it is necessary to consider the risk level of the current links, to prevent the entire network and operators from being greatly affected by link failures of a more concentrated risk of a certain link. This paper proposes the parameter risk weight as another one of the metrics for routing.

When  $s(x)$  or  $s(y)$  or  $w(x, y)$  is equal to 0, it means that the resources of the corresponding node or link are exhausted, then link  $xy$  should not be selected as the routing path, and  $C1(x, y)$  at this time is set to an extreme value in the specific process of routing path calculation. The risk weights of link  $xy$  ( $C2(x, y)$ ) is calculated as follows:

$$C2(x, y) = - \sum_{i=1}^M D(x, y) \ln \eta * \frac{Ri(x, y)}{1 + RiMax(x, y) - Ri(x, y)} \quad (2)$$

In expression (2),  $M$  is the actual number of fibers between node  $x$  and node  $y$  (i.e., the number of Group-bound PHY). For a service carried on FlexEGroup, it can use any number of PHY bound by the Group for transmission, and according to the number of PHY used, the risk weight on each physical fiber used by this service is calculated and summed up respectively.  $D(x, y)$  denotes the link length and  $\eta$  denotes the availability rate per fiber length which is defined in detail in in reference [14].

The parameter  $Ri(x, y)$  in expression (2) represents the risk on the physical link and is calculated as follows:

$$Ri(x, y) = \sum_{j=1}^N \left( \text{Priority}_j + \frac{B_j - B_{\min}}{B_{\max} - B_{\min}} \right) * [1 - \eta^{D(x, y)}] \quad (3)$$

This expression represents the risk of a physical link in link  $xy$ .  $N$  is the number of services carried on the physical link,  $\text{Priority}_j$  is a floating point number from 1.0 to 9.0, representing the service weight.  $B_j$  is the service bandwidth, and  $B_{\max}$  is the maximum bandwidth of the services on the physical link. In the expression the impact of bandwidth  $B_j$  is scaled to the  $[0, 1]$  interval, so that its impact on link risk only shows a more significant effect between services of the same priority.

### 3.3 Joint Load and Risk Balancing Algorithm

Considering the above load weights and risk weights, the two weights need to be normalized and mapped onto the interval [0, 1] and weighted to obtain the path weights of link  $xy$  as the selection index of the final routing algorithm. The path weights of link  $xy$  ( $C(x, y)$ ) is calculated as follows:

$$C1'(x, y) = \frac{C1(x, y) - C1Min(x, y)}{C1Max(x, y) - C1Min(x, y)} \quad (4)$$

$$C2'(x, y) = \frac{C2(x, y) - C2Min(x, y)}{C2Max(x, y) - C2Ma'x(x, y)} \quad (5)$$

$$C(x, y) = \alpha C1'(x, y) + (1 - \alpha) C2'(x, y) \quad (6)$$

The value of  $\alpha$  in the path weight is a weighting factor in the range of [0, 1], and multiple experiments are conducted to determine the appropriate value for load balancing and risk balancing to achieve better results. In the normalization, if the maximum value of the load weight or risk weight is equal to the minimum value (e.g., when initializing the network topology), the normalized weight is set to 0.

The optimization objectives in this paper are as follows:

Link time-slot utilization standard deviation:

$$\sigma1 = \sqrt{\frac{\sum_{e \in E} (\mu_e - \tilde{\mu})^2}{|E| - 1}} \quad (7)$$

Link risk standard deviation:

$$\sigma2 = \sqrt{\frac{\sum_{(x,y) \in E} [R(x, y) - R(\tilde{x}, \tilde{y})]^2}{|E| - 1}} \quad (8)$$

In this paper, an algorithm is designed to make both objective standard deviations small as a way to achieve good optimization results, which is called the joint load and risk balancing algorithm (JLRB algorithm). In the simulation, firstly, multiple sets of experiments are conducted to observe the optimization of the two target standard deviations under different weighting factors, and the appropriate one will be chosen. After that, the capacity of certain links in the network topology is changed to compare the degree of optimization of the two objectives between the algorithm designed in this paper and the comparison algorithm. Figure 2 shows the flow chart of the algorithm, and Table 1 shows the specific steps of the algorithm.

## 4 Simulation

The simulation uses the same network topology as in reference [10]. It is the communication network topology of a city in Jiangsu Province of the State Network in China to verify the effectiveness of the algorithm proposed in this paper. The topology consists of 29 network nodes and 48 different types of fiber optic cable links with a node average degree of 3.3, as shown in Fig. 3.

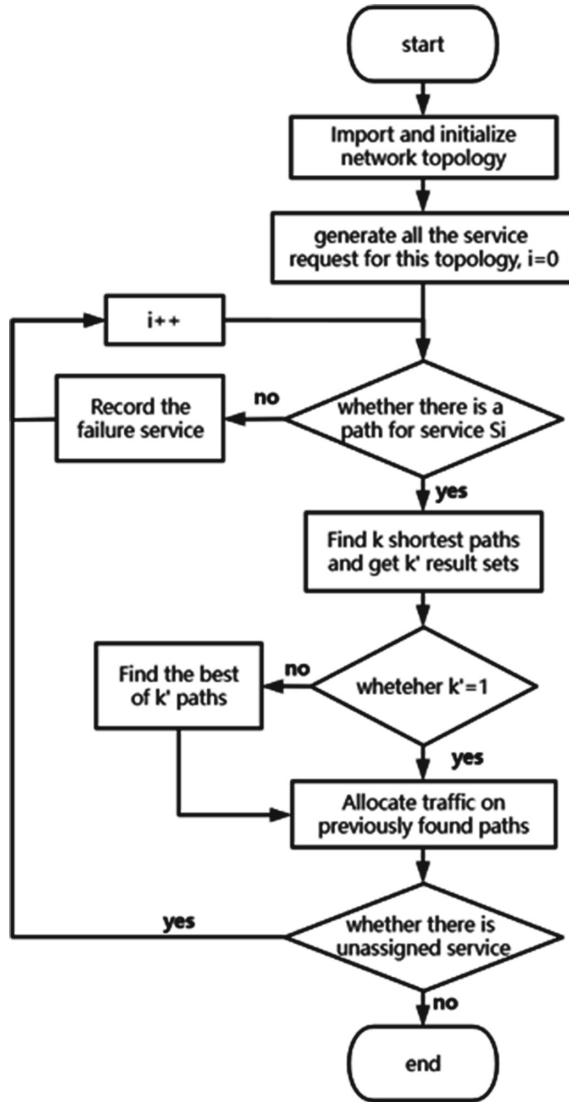


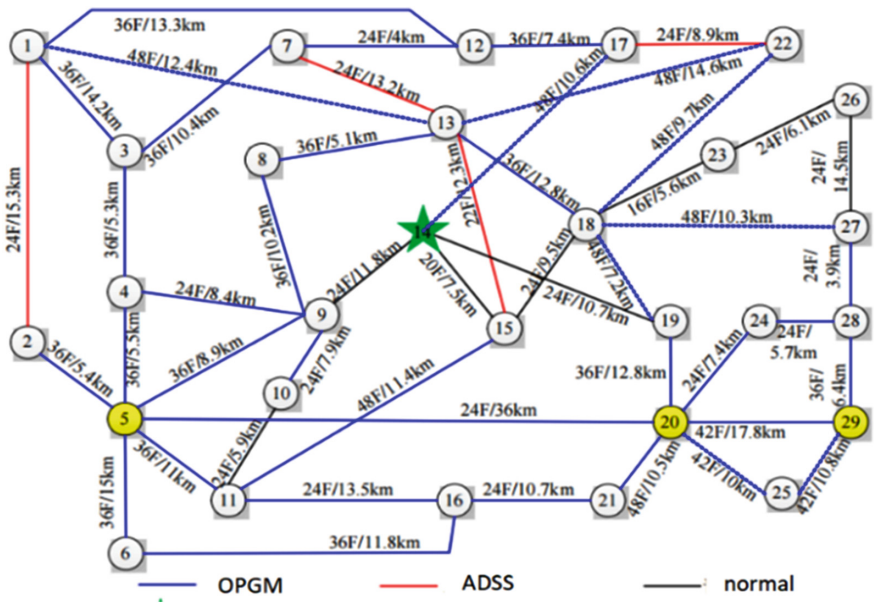
Fig. 2. Algorithm flow chart

In Fig. 3: Node 14 is the first-level dispatch center. Nodes 5, 20 and 29 are the second-level dispatch centers, and the rest of the sites are ordinary network nodes. The nodes are linked by fiber optic cables, and the number and length of fiber optic cables are marked in the figure. There are three colors of links in the diagram, which correspond to three different types of fiber optic cables. The blue link is OPGW fiber optic cable, with 99.84% availability per km  $\eta$ . The black link is a normal fiber optic cable with 99% availability per km. In the FlexE network, by default, a FlexEGroup consists of four 50G



**Table 1.** Specific steps of the JLRB algorithm

<b>Algorithm 1:</b> The Joint Load and Risk Balancing Algorithm	
1	Generate network topology $G < V, E >$ ;
2	Initialize $G < V, E >$ , allocate bandwidth, calculate weights for each link;
3	Generate a random business list $S$ according to the rules;
4	<b>for each</b> $S_i \in S$ <b>do</b>
5	Use Dijkstra algorithm to determine if there is a path between the $S_i$ start and end points that can carry bandwidth;
6	Use the K shortest path method on $G < V, E >$ for service $S_i$ to obtain $K'$ alternative paths $P$ that can accommodate the service;
7	<b>if</b> $K' == 1$ <b>then</b>
8	Assign this service on this path;
9	Recalculate each link weight;
10	<b>end</b>
11	<b>else</b>
12	<b>for each</b> $P_i \in P$ <b>do</b>
13	Calculate the sum of path weights for $P_i(SUMC)$ ;
14	Calculate the change-rate of $SUMC$ of $P_i$ ;
15	<b>end</b>
16	Select the path with the smallest change-rate among the $K'$ paths as the routing path;
17	Assign this service on this path;
18	Recalculate each link weight;
19	<b>end</b>
20	<b>end</b>



**Fig. 3.** Network topology used in the simulation

PHYs. This means that each link has a default capacity of 200G and consists of four physical links.

The services carried by the network topology in Fig. 3 are characterized by large bandwidth, relatively low requirements for latency and reliability, and centralized scheduling near the center. Therefore, the services are randomly generated according to the following rules: 70% of the services are near the primary and secondary dispatch centers, and one of Nodes is randomly selected. 14, 5, 20 and 29 are as one of the endpoints of the services, and then a node no more than three hops away from the endpoint is randomly selected as the other endpoint of the service. The source and destination nodes of the remaining 30% of the services are randomly selected among all nodes. The weights of all services are one random floating point number between 1.0 and 9.0, and the bandwidths are one random floating point number between 10.0 and 30.0G.

#### 4.1 Choose Weighting Factor

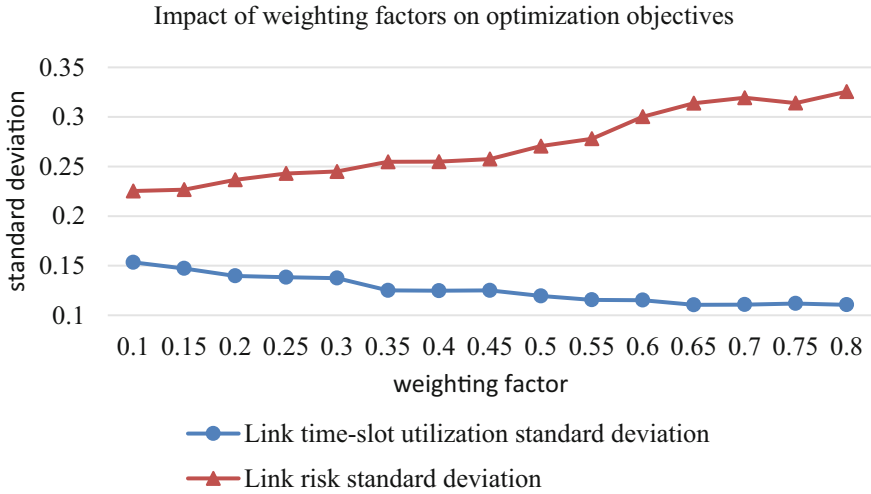
After initializing the network topology, 25 services are randomly generated according to the above rules, i.e., 70% of the services are concentrated near the dispatch center and the remaining 30% are random. And the routing planning is performed for each service in turn using the designed algorithm with different weighting factors. The standard deviation of time slot utilization and link risk standard deviation are calculated for each link after the planning is completed. The value of  $\alpha$  is adjusted several times, and the same set of services is planned again and two standard deviations are calculated. The two standard deviation vs.  $\alpha$  line graphs are plotted as shown in Fig. 4.

The two optimization objectives are the standard deviation of link time slot resource utilization and the standard deviation of link risk. The smaller the standard deviation of link time slot resource utilization, the more balanced the allocation of time slot resources on each link, i.e., the better the optimization degree of load balancing. The smaller the standard deviation of link risk, the more balanced the risks induced by the assigned services on each link, and the less likely multiple important services will fail because of one link failure, i.e., the better the optimization of risk balancing.

As shown in Fig. 4, the standard deviation of link time slot resource utilization decreases with the increase of the weighting factor  $\alpha$  on the whole and fluctuates in some intervals, while the standard deviation of link risk changes in the opposite direction, increasing with the increase of the weighting factor. According to the analysis of the two line graphs, we can see that when  $\alpha$  is taken around 0.45, both load balancing and risk balancing can get good optimization results. For high traffic services, the standard deviation of link time slot resource utilization is more important, so  $\alpha = 0.5$  is selected. In the subsequent simulation experiments, the value of  $\alpha = 0.5$  is taken.

#### 4.2 Simulation and Analysis

In this paper, we choose the LRWS algorithm (Load and Risk Weight Smallest algorithm) proposed in reference [10] as the comparison algorithm of JLRB algorithm. LRWS algorithm is similar to Dijkstra algorithm, which directly selects the path with the minimum sum of path weights for each service and dynamically updates the path weights. The path weights of LRWS algorithm are also derived from the load weights and risk weights



**Fig. 4.** Impact of the weighting factor  $\alpha$  on optimization objectives

which ensures that the comparison algorithm can also take effect for both optimization objectives. In this paper, the path weight calculation formula of LRWS algorithm is changed to be the same as the path calculation formula of JLRB algorithm in order to adapt it to the FlexE network with high traffic service. This allows a visual comparison of the difference in the degree of optimization of the two objectives between the JLRB algorithm and the LRWS algorithm.

For FlexE networks with high traffic services, a common situation is to build the network with trunk links as high-capacity links to cope with the concentrated high traffic services. Corresponding to the network structure in this experiment, the links near the primary dispatch center and the secondary dispatch center are set as high-capacity links, i.e., 400G links with eight physical links bound. In this experiment, when the number of 400G links is 0, all links are 200G, and when it is 3, links 5–6, 9–14, 20–21 are set to 400G, and the rest of the links are still 200G. The topology is initialized in the similar way when it is of other values. Six experimental scenarios are set from the smallest to the largest number of 400G links.

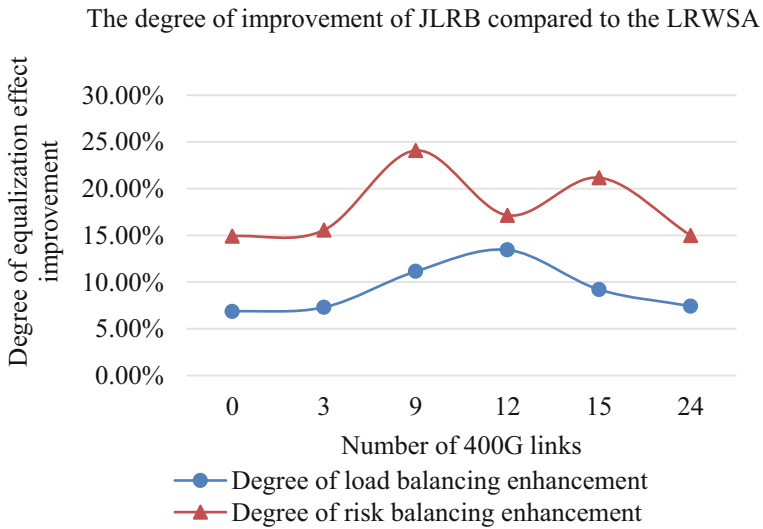
With the expansion of the trunk link, the random range of service bandwidth was doubled to 20.0–60.0G. The experimental data of the JLRB algorithm and the LRWS algorithm are shown in Table 2.

The percentage reduction of the two standard deviations of the JLRB algorithm compared to the LRWS algorithm is used as an indicator of the performance improvement of the JLRB algorithm on load balancing and risk balancing. Based on the data in Table 2, the performance improvement curve of the JLRB algorithm compared to the LRWS algorithm can be plotted.

It can be seen from Fig. 5 that the JLRB algorithm outperforms the LRWS algorithm in both load balancing and risk balancing in all six scenarios. The overall trend of load balancing improvement of JLRB algorithm is that it increases with the number of 400G

**Table 2.** Comparison of the two target standard deviations of JLRB and LRWS

Number of 400G links	$\sigma_1$		$\sigma_2$	
	JLRB	LRWS	JLRB	LRWS
0	0.155978499	0.167448117	0.320082041	0.376150177
3	0.158156863	0.170605014	0.316764964	0.375181164
9	0.143226034	0.161175867	0.262590306	0.345898818
12	0.12812342	0.148012604	0.25360387	0.297080131
15	0.097974598	0.107907227	0.246062283	0.312148146
24	0.095792394	0.103475166	0.260295402	0.306150177



**Fig. 5.** The degree of improvement of JLRB compared to the LRWS

links, then decreases after reaching the peak, and the risk balancing improvement of JLRB algorithm is roughly the same trend although there are fluctuations in the middle.

The reason for this trend is that the JLRB algorithm can effectively prevent a spike in time-slot utilization for a link with a small capacity but a large percentage of free time slots for a service with a lot of traffic (which appears in the LRWS algorithm). As the number of 400G links near the primary and secondary dispatch centers increases, the degree of link variation in the service concentration area increases and then decreases (when 24 400G links, almost all links in the service concentration area, are 400G, and the degree of variation is small). The link variability in the service concentration area leads to the above-mentioned phenomenon of link time slot utilization spike in the

LRWS algorithm, i.e., the LRWS algorithm will face the problem of choosing a high-capacity, high time slot utilization path or a small-capacity, low time slot utilization path. Therefore, the degree of load balancing and risk balancing optimization of the JLRB algorithm increases and then decreases with the increase of the number of 400G links.

## 5 Conclusion

In this paper, a routing algorithm is designed for high traffic FlexE networks, and this JLRB algorithm integrates the load and risk values of links, and introduces weighting parameters to design the expressions of link weights. In the simulation experiments, the values of the weighting parameters are determined by the simulation results of the JLRB algorithm with different weighting parameters. After that, several sets of experiments were conducted in different scenarios together with the comparison algorithm (LRWS algorithm). The simulation results show that the JLRB algorithm has improved in both load balancing and risk balancing compared with the LRWS algorithm, and at the same time, the degree of load balancing and risk balancing of the JLRB algorithm both increase with the increase of the degree of inter-zone link differences. When a certain number of high-capacity backbone links are reached, the inter-zone link discrepancy increases to the peak and the performance of the JLRB algorithm reaches the peak, and then turns to a decreasing trend. The experiment proves the effectiveness of the JLRB algorithm proposed in this paper, which has some reference significance for FlexE network planning, network routing, and risk reduction.

## References

1. Vilalta, R., et al.: Network slicing using dynamic flex Ethernet over transport networks. In: 2017 European Conference on Optical Communication (ECOC), pp. 1–3. Gothenburg, Sweden (2017). <https://doi.org/10.1109/ECOC.2017.8346065>
2. Zhang, M.: Flex ethernet technology and application in 5G mobile transport network. *China Commun.* **18**(2), 250–258 (2021). <https://doi.org/10.23919/JCC.2021.02.017>
3. Koulougli, D., Nguyen, K.K., Cheriet, M.: Efficient routing using flexible Ethernet in multi-layer multi-domain networks. *J. Light. Technol.* **39**(7), 1925–1936, 1 April 2021. <https://doi.org/10.1109/JLT.2020.3044845>
4. Liang, H., da Fonseca, N.L.S., Zhu, Z.: On the cross-layer network planning for flexible Ethernet over elastic optical networks. *IEEE Trans. Netw. Serv. Manage.* **18**(3), 3691–3705 (2021). <https://doi.org/10.1109/TNSM.2020.3044702>
5. Dai, Y., Wu, X., Zhao, J., et al.: A flexible Ethernet calendar allocation based on client traffic. In: *Journal of Physics: Conference Series*. IOP Publishing, vol. 2224, no. 1, p. 012131 (2022)
6. Zhang, S., Zhong, Q., Zha, M., Zuo, T.: Hybrid multiplexing over FlexE group. In: 2018 23rd Opto-Electronics and Communications Conference (OECC), pp. 1–2. Jeju, Korea (South) (2018). <https://doi.org/10.1109/OECC.2018.8730124>
7. Wu, D., Xin, P., Liu, L., Bai, H., Zhang, Y.: Routing policy for balanced management of slices using flexible Ethernet. In: 2022 7th International Conference on Computer and Communication Systems (ICCCS), pp. 537–542. Wuhan, China (2022). <https://doi.org/10.1109/ICCCS5155.2022.9846474>
8. Constantinou, C.K., Ellinas, G.: A load balancing technique for efficient survivable multicasting in mesh optical networks. *Opt. Switch. Netw.* **22**, 1–8 (2016)

9. Brown, D., Trowbridge, S.: Can FlexE deliver on promises for programmable and dynamic optical networking?. In: 2018 European Conference on Optical Communication (ECOC), pp. 1–4. Rome, Italy (2018). <https://doi.org/10.1109/ECOC.2018.8535299>
10. Bin, L.I., Chao, L.U., Dongsheng, J.I.N.G., et al.: An optimized routing algorithm with load and risk joint balance in electric communication network[J]. Proc. CSEE **39**(9), 2713–2722 (2019). (in Chinese)
11. Sun, Y., Zhou, S., Lu J., et al.: Wave-channel balanced dynamic routing and wavelength assignment algorithm for power optical transport network. Autom. Electr. Power Syst. **40**(13), pp. 114–120 (2016) (in Chinese)
12. Kang, J., et al.: Load balance based deflection routing for optical burst switching. In: 2018 23rd Opto-Electronics and Communications Conference (OECC), pp. 1–2. Jeju, Korea (South) (2018).<https://doi.org/10.1109/OECC.2018.8730053>
13. Liming, C., Jingyue, S., Shanjun, L., et al.: An algorithm for business resource uniform distribution in power communication network. Power Syst. Technol. **41**(9), 3066–3073 (2017). (in Chinese)
14. Ziyang, Z., Jianming, L.: A new service risk balancing based method to evaluate reliability of electric power communication network. Power Syst. Technol. **35**(10), 209–213 (2011). (in Chinese)



# Network Fault Lightweight Prediction Algorithm Based on Continuous Knowledge Distillation

Wei Huang<sup>1,2</sup>, Jie Huang<sup>1(✉)</sup>, Chengwen Fan<sup>3</sup>, and Yang Yang<sup>3</sup>

<sup>1</sup> School of Cyber Science and Engineering, Southeast University, Nanjing, Jiangsu, People's Republic of China

jiehuang\_lw@163.com

<sup>2</sup> The 54th Research Institute of CETC, Shijiazhuang, Hebei, People's Republic of China

<sup>3</sup> State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, People's Republic of China

**Abstract.** Network fault prediction is one of the important means to ensure network security and stable operation. Efficient fault prediction can improve the ability of operation and maintenance personnel to deal with faults and reduce losses caused by faults. In edge scenarios, device resources may be limited by hardware resources, such as storage space, memory, processing power. They may also be limited by unstable network connections, such as limited bandwidth, high packet loss rate, and large delay. This paper investigates the research status of network fault prediction at home and abroad. Currently, commonly used network fault prediction methods include methods based on statistics, based on machine learning, and based on deep learning. These network fault prediction methods can learn the characteristics of network faults and have achieved good results in network fault prediction tasks. However, the methods based on neural networks have a large computational resource overhead and are easily limited by device performance in edge scenarios. The methods based on statistics and machine learning have low cost but low accuracy. In this paper, an edge side network fault prediction model based on improved BiLSTM is designed, and improve the continuous distillation technology to design Stage Continuous Knowledge Distillation (SCKD). The simulation experiments prove that the student model performs similarly to the teacher model in terms of accuracy and F1-Score, and has lower memory usage and parameter volume.

**Keywords:** Knowledge distillation · Fault prediction · Lightweight method · BiLSTM

## 1 Introduction

In the modern network environment, the occurrence of network failure may lead to serious consequences such as communication interruption, business interruption and data loss. These failures not only pose threats to the security and stability of the network,

but also negatively impact business operations and user experience. In order to ensure the reliability and normal operation of the network, network fault prediction becomes a crucial task.

In edge scenarios, device resources may be limited by hardware resources, such as storage space, memory, processing power, etc. They may also be limited by unstable network connections, such as limited bandwidth, high packet loss rate, and large delay. Traditional network fault prediction methods usually rely on large-scale computing and storage resources, and perform poorly in this scenario. In this context, network fault prediction technology based on knowledge distillation emerged as the times require, providing a new solution for network fault prediction.

Knowledge distillation is a transfer learning method that transfers knowledge from a large neural network to a smaller, more deployable neural network. This method can improve the accuracy and real-time performance of network fault prediction while reducing the consumption of computing and storage resources, which has broad prospects and great significance in practical applications. In practical applications, network fault prediction based on knowledge distillation can be widely used in various network environments, such as data center networks, enterprise networks, IoT, 5G communication networks, etc. In these scenarios, network fault prediction techniques have important practical value. For example, in the Internet of Things, timely prediction and handling of network failures can ensure the normal operation of IoT devices and improve the stability of the entire system.

This paper aims at the problem of high overhead of traditional methods of network fault prediction on the edge side, and adopts the method of continuous knowledge distillation, so that the student model with less memory usage and model parameters has the same accuracy as the teacher model. Through the research in this paper, the overhead of network fault prediction in the edge network will be reduced, and the current situation of being limited by device computing resources will be improved.

## 2 Related Work

### 2.1 Network Fault Prediction Based on Statistical Method

Early network fault prediction mainly relied on statistical methods, such as time series analysis and event tree analysis. These methods are simple and easy to use, but have limitations in dealing with complex nonlinear relationships and high-dimensional feature data. Time series analysis is a common statistical method that uses statistical analysis to infer future failures based on historical patterns and trends of time series data. By observing cyclical, trending, and seasonal changes in time-series data, potential failure modes can be identified and predicted accordingly. In [1], Zhang analyzed the log data in IBM Blue Gene and built a predictive model using the nearest neighbor method. Event tree analysis is a method based on fault tree theory, which is used to analyze and predict the probability of occurrence of various events and faults in the system. By building an event tree, a fault event can be decomposed into a series of possible sub-events, and the probability of the overall fault occurrence can be calculated according to the occurrence probability of each sub-event. In [2], Guan used a decision tree classifier, a supervised



learning method, to predict network failures. Although network fault prediction methods relying on statistical methods have the advantage of being simple and easy to use! and have achieved some success in some scenarios, they also have some limitations. First, these methods are limited in dealing with complex nonlinear relationships and high-dimensional feature data. Network faults often involve the interaction of multiple factors, and statistical methods are often difficult to capture such complex relationships. Second, the predictive power of statistical methods is limited by the quality and reliability of historical data and may perform poorly for new failure modes or unknown data distributions. Therefore, with the complexity of the network environment and the increase of data scale, the limitations of statistical methods are gradually revealed.

## 2.2 Network Fault Prediction Based on Machine Learning and Deep Learning

To overcome the limitations of the aforementioned statistical methods, researchers use machine learning for network fault prediction to improve prediction accuracy and model adaptability. These algorithms build a suitable classifier based on the training set, and then use this classifier to make predictions on the collected data. Common machine learning algorithms include Support Vector Machine, Naive Bayes, K-Nearest Neighbor, and Random Forest. The random forest algorithm can effectively deal with data with noise and missing values by constructing multiple decision trees and synthesizing their prediction results, and has a high prediction accuracy. In [3], Qiu used the random forest algorithm in machine learning to predict network faults.

In addition to machine learning, some researchers also use deep learning to predict network faults. They use models such as deep neural network, convolutional neural network (CNN), recurrent neural network (RNN) and long short-term memory network (LSTM) to capture spatiotemporal information in network data, thereby improving the accuracy and real-time performance of predictions. In [4], Tan used a neural network mixed with CNN and LSTM for network fault prediction. CNN can extract local features in input data through convolution operation, thus effectively capturing spatial information. LSTM uses a cyclic structure to model the temporal relationship in sequence data, which can capture the dynamic information of time evolution. Tan made full use of the strengths of CNN in feature extraction and LSTM in processing sequence data, this hybrid model can utilize both spatial and temporal information to more comprehensively analyze network data and make accurate fault predictions.

## 2.3 Network Fault Prediction Based on Knowledge Distillation

In order to solve the challenge of network fault prediction in edge scenarios, researchers began to focus on how to transform complex network fault prediction models into lightweight and efficient models through effective model compression and optimization methods. In this context, Knowledge Distillation has attracted widespread attention as an effective model compression technique. Knowledge distillation was first proposed by Hinton et al. [5] in 2015. Knowledge distillation is a method to incorporate the knowledge of a pre-trained complex teacher model when training a lightweight student model. By introducing the knowledge of the teacher model, the lightweight student model can achieve a level similar to the teacher model in terms of accuracy while maintaining

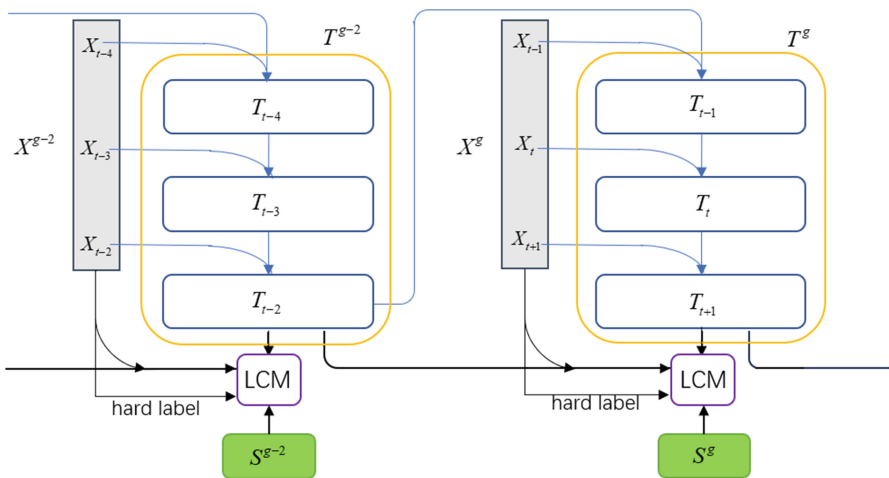
low computational complexity and memory footprint. In this technique, the teacher's knowledge is provided to the student by minimizing the difference between the logic generated by the teacher model and the student model [6, 7]. Ruffy and Chahal [8] validated various knowledge distillation techniques for classification tasks and implemented some state-of-the-art techniques to examine the effectiveness of knowledge distillation in classification-based tasks.

### 3 Proposed Method

#### 3.1 Stage Continuous Knowledge Distillation

In edge scenarios, device resources may be limited by hardware resources, such as storage space, memory, processing power, etc. They may also be limited by unstable network connections, such as limited bandwidth, high packet loss rate, and large delay. Traditional network fault prediction methods usually rely on large-scale computing and storage resources, which perform poorly in this scenario. In this context, network fault prediction technology based on knowledge distillation emerged as the times require, providing a new solution for network fault prediction.

In network fault prediction, the data is not given in large quantities at one time, but the data is reported immediately when a fault occurs. However, general knowledge distillation cannot preserve the model and its knowledge trained on historical data as a new batch. When the data comes, the knowledge of the teacher model will be overwritten by these data. Also, storing a predictive model is more efficient than storing data because the model takes up minimal storage space. Based on the above two considerations, this paper uses continuous knowledge distillation to propose a method of saving and updating the prediction model over time. The overall framework of stage continuous knowledge distillation is shown in Fig. 1.



**Fig. 1.** Overall architecture of stage continuous knowledge distillation (SCKD).

In the continuous knowledge distillation framework, the teacher model and student model are continuously updated with the continuous input of data. Before the arrival of new network failure data  $n$ , save the old teacher model trained on the previous network failure data. This old model retains knowledge of historical network failures. When learning a new model from the dataset collected by task  $n$ , knowledge distillation techniques are applied to transfer knowledge from the old model to the new model. By transferring knowledge from old models to new models, continuous knowledge distillation enables new models to benefit from insights and information captured by old models.

As shown in Fig. 1, the network fault data  $x_t$  is generated at time  $t$ , which is input to the teacher model  $T_{t-1}$  at time  $t-1$ , and a new teacher model  $T_t$  is obtained through training. We take the failure data of a group of moments as a data group  $X^g$ , and input it into the teacher model group at the same stage. Loss calculation and knowledge distillation are performed in the LCM. The structure of the LCM is shown in Fig. 2.

The loss calculation formulas of the teacher model are as follows:

$$L_1 = \frac{1}{m} \sum_i^m d(f_T^g(x_i), y_i) \tag{1}$$

$$L_2 = \frac{1}{m} \sum_i^m d(f_T^g(x_i), f_T^{g-2}(x_i)) \tag{2}$$

$$L_T = L_1 + L_2 \tag{3}$$

where  $m$  is the number of network failure data input in one stage,  $x_i$  refers to the input data at time  $i$ , and  $y_i$  refers to the label of the input data at time  $i$ .  $f_T^g(x_i)$  is the output of the teacher model group  $T^g$ ,  $x_i$  refers to the input data at time  $i$ , and  $y_i$  refers to the label of the input data at time  $i$ .

We can see that the loss function when training the teacher model is divided into two parts, and  $L_1$  realizes the prediction result and the real label of the fitted teacher model. At the same time, in order to realize the transfer of knowledge from the old model to the new model,  $L_2$  realizes the prediction results of the two teacher model groups in the fitting adjacent stages, and it realizes the prediction ability inherited from the previous teacher model.

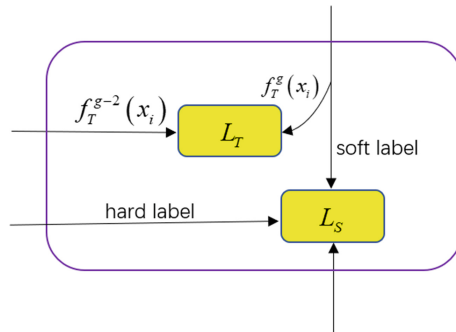


Fig. 2. Structure of loss calculation module (LCM).

In the process of implementing distillation, the student model needs to combine the hard labels and the soft labels output by the teacher model to calculate the loss. This paper proposes the loss function  $L_S$  of the student model for the continuous knowledge distillation.

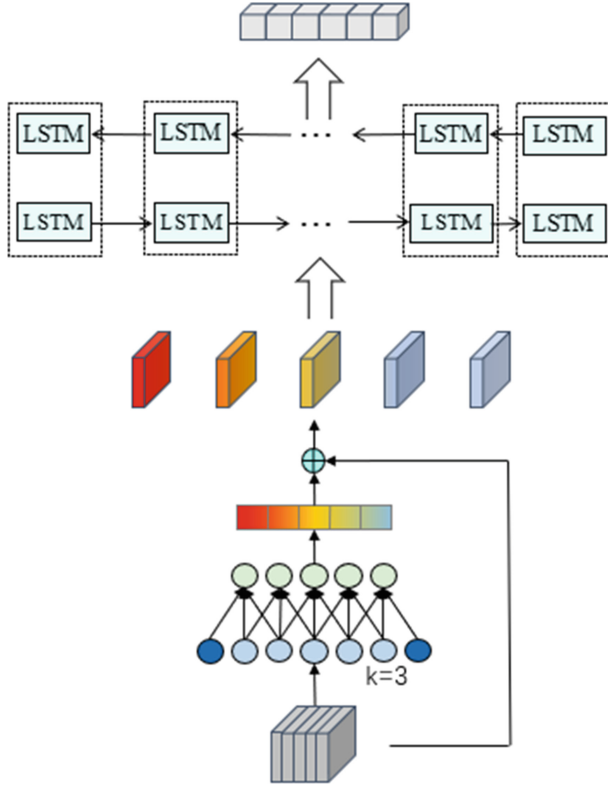


Fig. 3. Overall architecture of the ECA-BiLSTM.

The first loss function is the hard label loss, denoted as  $L_{hard}$ . It calculates the difference between the predictions generated by the student model and the real labels. Its calculation formula is shown in Eq. (4).

$$L_{hard} = \frac{1}{m} \sum_i^m d(f_S^g(x_i), y_i) \tag{4}$$

The second loss function is the soft label loss, denoted as  $L_{pred}$ . It quantifies the difference between the predictions of the teacher model and the predictions of the student model. Its calculation formula is shown in Eq. (5).

$$L_{soft} = \frac{1}{m} \sum_i^m d(f_T^g(x_i), f_S^g(x_i)) \tag{5}$$

Finally, the loss function of the final training student model can be obtained by summing. By minimizing the loss function to update the parameters of the student model, the output of the student model is close to the teacher model.

$$L_S = L_{hard} + L_{soft} \quad (6)$$

### 3.2 Fault Prediction Algorithm Based on Improved BiLSTM

Based on BiLSTM, we propose a new network fault prediction algorithm. Efficient Channel Attention (ECA) module is a local cross-channel interaction strategy without dimensionality reduction, which effectively avoids the impact of dimensionality reduction on channel attention learning. After the ECA module uses the non-dimension-reducing GAP to aggregate convolution features, it first adaptively determines the kernel size  $k$ , then performs 1D convolution, and then performs the Sigmoid to learn channel attention.

In this paper, we use the ECA module to process a set of input network fault data, regard the data at a time in this set of data as a channel, and perform cross-channel weight distribution on the data of different channels. Then the weighted data is input into BiLSTM, and the prediction result is obtained according to the output of BiLSTM. The overall architecture of the network fault prediction algorithm is shown in Fig. 3.

## 4 Evaluation

### 4.1 Dataset

The dataset used in this experiment is obtained through a self-collected sensor cluster operation and maintenance data built in the laboratory and injecting faults. The sensor operation and maintenance dataset simulates the edge network by self-organizing a sensor network, and uses ChaosBlade to generate faults for sensor device nodes.

In the built wireless sensor network, the types of faults injected include CPU overload, memory overflow, I/O abnormality, network delay, network packet loss, network transmission packet damage, network packet disorder and CPU temperature abnormality. Finally, the performance data of the sensor network system during operation in January 2021 was extracted.

Through such experimental settings and data collection, we simulate the occurrence of network faults in a real edge environment and use these data to conduct research and evaluation of network fault prediction algorithms.

### 4.2 Metrics

We assess each method according to the accuracy, F1-score, memory usage and number of parameters. The significance of the accuracy is to measure the overall classification accuracy of the model, and the degree to which the model prediction is correct. A higher

accuracy indicates a better predictive ability of the model. The accuracy rate is shown in Eq. (7).

$$Accuracy = \frac{TP + TN}{TP + FP + FN + Tn} \quad (7)$$

The significance of F1-score is that it comprehensively considers the accuracy and recall of the model, and can more comprehensively evaluate the classification performance of the model. Their formulas are as follows:

$$Precision = \frac{TP}{TP + FP} \quad (8)$$

$$Recall = \frac{TP}{TP + FN} \quad (9)$$

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (10)$$

where true positive, true negative, false positive, and false negative are denoted respectively by TP, TN, FP, and FN.

In order to better measure the ability of the knowledge matrix distillation algorithm, we counted the memory usage data and parameter quantities of the teacher model and the student model.

### 4.3 Experiments

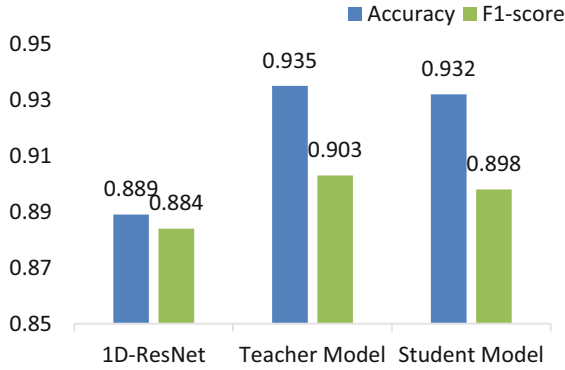
In this experiment, we compared the performance of 1D-ResNet [9] and ECA-BiLSTM models before and after distillation, and analyzed their accuracy, F1-score, memory usage and number of parameters. The experimental results are shown in Tables 1 and 2.

**Table 1.** Comparison of accuracy, F1-score and memory usage of three models.

Algorithm	Accuracy	F1-score	Memory usage(MB)
1D-ResNet	0.889	0.884	250.93
ECA-BiLSTM (Teacher Model)	0.935	0.903	425.74
ECA-BiLSTM (Student Model)	0.932	0.898	361.37

As shown in Table 1, the accuracy and F1-Score of the random forest algorithm are slightly lower, 0.889 and 0.884, respectively. This may be due to the limitation of the random forest algorithm in processing complex time series data (Figs. 4, 5 and 6).

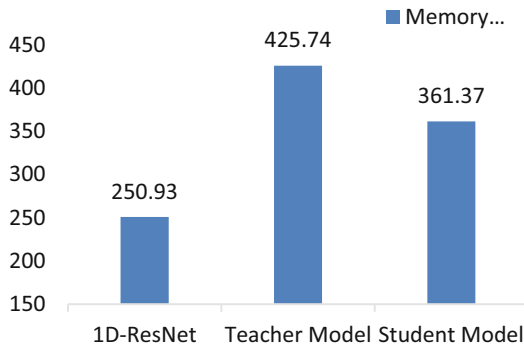
As shown in Table 2, from the perspective of memory usage and parameters, the memory usage of the random forest algorithm is 250.93 MB, the memory usage of the teacher model is the highest, reaching 425.74 MB, and the memory usage of the student model is comparable to 15.11% less memory usage than the teacher model.



**Fig. 4.** Accuracy and F1-score of the three models.

**Table 2.** Comparison of parameters before and after distillation.

Algorithm	Params
ECA-BiLSTM (Teacher Model)	32808
ECA-BiLSTM (Student Model)	16408



**Fig. 5.** Memory usage of three models.

At the same time, the teacher model has 32808 parameters, while the student model only has 16408 parameters which is 49.98% less than the teacher model. This means that the student model is more lightweight than the teacher model in terms of model size and complexity. A smaller number of parameters not only reduces the computational and storage requirements of the model, but also improves the efficiency and inference speed of the model.

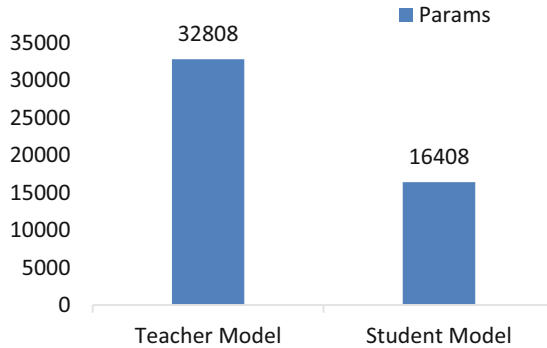


Fig. 6. Parameters of three models.

## 5 Conclusion

For the network fault prediction scenario, this paper proposes an effective continuous knowledge distillation framework and a network fault prediction algorithm based on improved BiLSTM. Experiments show that the method proposed in this paper can effectively predict network faults, and the model can be deployed on resource-constrained network terminals. The algorithm we propose can effectively help improve network stability and reliability, reduce operation and maintenance costs.

## References

1. Zhang, Y., Sivasubramaniam, A.: Failure prediction in IBM BlueGene/L event logs. In: Proceedings of the 2008 IEEE International Symposium on Parallel and Distributed Processing, pp. 1–5, Miami (2008)
2. Guan, Q., Zhang, Z., Fu, S.: Ensemble of Bayesian Predictors and Decision Trees for Proactive Failure Management in Cloud Computing Systems. In: Journal of Communications, pp.52–61, (2012)
3. Shaoming, Q., Wensheng, Y., Xiuli, D.: Optimizing random forest model for network fault prediction[J]. *Comput. Appl. Softw.* **38**(02), 103–109+170 (2021)
4. Tan, Z., Pan, P.: Network fault prediction based on CNN-LSTM Hybrid neural network. In: 2019 International Conference on Communications, pp. 486–490. Haikou (2019)
5. Hinton, G., Vinyals, O., Dean, J.: Distilling the Knowledge in a Neural Network (2015). [arXiv:1503.02531](https://arxiv.org/abs/1503.02531)
6. Li, Z., Xu, P., Chang, X., Yang, L., Zhang, Y., Yao, L., Chen, X.: When object detection meets knowledge distillation: a survey. In: IEEE Transactions on Pattern Analysis and Machine Intelligence, pp. 1–25. Xiamen (2023)
7. Wang, L., Yoon, K.: Knowledge distillation and student-teacher learning for visual intelligence: a review and new outlooks. In: IEEE Transactions on Pattern Analysis and Machine Intelligence, pp. 1–38 (2021)
8. Ruffy, F., Chahal, K.: The state of knowledge distillation for classification (2019). [arXiv:1912.10850](https://arxiv.org/abs/1912.10850)
9. Zhou, K., Dai, R., Li, X., Zhao, B., Chen, Z., Guo, W., Gao, J.: Fault diagnosis method of power electronic equipment based on improved resnet neural network. In: 2022 4th International Conference on Electrical Engineering and Control Technologies, pp.50–54 (2022)





# Quality of Service Oriented Power Communication Network Test Mechanism

Wandi Liang<sup>1</sup>, Hongguang Yu<sup>1</sup>, Huicong Fan<sup>1</sup>, Shijia Zhu<sup>1</sup>, Jianhua Zhao<sup>1</sup>,  
Wenxiao Li<sup>1</sup>, Fan Tang<sup>2</sup>(✉), and Caiyun Li<sup>2</sup>

<sup>1</sup> Economic and Technological Research Institute of State Grid Hebei Electric Power Co., Ltd.,  
Shijiazhuang 050081, China

<sup>2</sup> Beijing InfoTel Network Testing Laboratory Co., Ltd., Beijing 100088, China  
tangfan@infotel.com.cn

**Abstract.** SDN technology realizes the separation of network control and data forwarding, and improves the efficiency and resource utilization of network communication. However, the current research lacks the research on network testing mechanism in SDN environment from the perspective of service quality, resulting in higher probability of network service problems and longer service repair time. In order to solve this problem, this paper first designs a network test architecture oriented to service quality under SDN environment. Secondly, the power communication network test mechanism oriented to service quality under SDN environment is designed. This mechanism includes six steps: the business management system discovers business exceptions, the test management global center triggers the test, the test management global center sends the test task to the test domain management center, the test domain management center sends the test request to the SDN domain controller, the SDN domain controller sends the flow table and feeds back the results to the test domain management center, and the test management global center collects the test domain management center results and analyzes them. Finally, the test mechanism proposed in this paper is analyzed from the two dimensions of usability and enforceability, which verifies that this mechanism has good performance.

**Keywords:** SDN · Power communication network · Network test · Business quality

## 1 Introduction

SDN technology realizes the separation of network control and data forwarding, and improves the efficiency and resource utilization of network communication. To ensure network performance, network testing has become a research focus [1, 2]. Literature [3] analyzes common methods of network performance analysis from the perspective of Mesh network, and proposes the feasibility of building a small-scale platform to improve performance analysis. In order to solve the problem of conflict when sending test platform data, literature [4] proposes a mechanism of grouping and collecting test data. Literature [5] proposes a mechanism to dynamically identify conflicts, providing

efficiency for network performance testing. On the basis of literature [5], literature [6] proposes a strategy to update the testing mechanism, which further improves the testing performance. Literature [7] proposes a data plane verification mechanism based on the characteristics of SDN network, which improves the availability of test rules. Literature [8] proposes a hybrid network architecture model, which solves the problem of low network test performance in a multi-domain environment. According to the existing research and analysis, network testing research has accumulated a lot of research results. However, the current research lacks the research on network testing mechanism in SDN environment from the perspective of service quality, resulting in higher probability of network service problems and longer service repair time.

In order to solve this problem, this paper first designs a network test architecture oriented to service quality under SDN environment. The architecture mainly includes four types of modules: business management system, test center, SDN controller and SDN domain. Secondly, the power communication network test mechanism oriented to service quality under SDN environment is designed. This mechanism includes six steps: the business management system discovers business exceptions, the test management global center triggers the test, the test management global center sends the test task to the test domain management center, the test domain management center sends the test request to the SDN domain controller, the SDN domain controller sends the flow table and feeds back the results to the test domain management center, and the test management global center collects the test domain management center results and analyzes them. Finally, the performance of the testing mechanism proposed in this paper is analyzed from the two dimensions of usability and enforceability, which verifies that this mechanism has good performance.

## 2 Network Test Architecture

In order to manage the power communication network test from the perspective of service quality assurance, this paper designs a network test architecture as shown in Fig. 1. The figure mainly includes four types of modules: business management system, test center, SDN controller, and SDN domain.

### (1) Business management system

According to the operation and maintenance experience, the business management system generally has the functions of business view, business performance monitoring, business failure recovery, etc. According to the development trend of the business and the work needs of the power company, this paper divides the business into four types: remote control, cloud analysis, immersion and the Internet of Things.

In terms of remote control business, this kind of business is mainly to complete the remote control of power equipment, significantly improve the management efficiency of power equipment, and reduce the time and financial expenses caused by travelling. For example, the common remote control business is transformer control business. From the perspective of network resource demand of services, the demand of such services for power communication network is low latency and large uplink bandwidth. In terms of cloud analysis business, this business is mainly to upload power grid data to the cloud

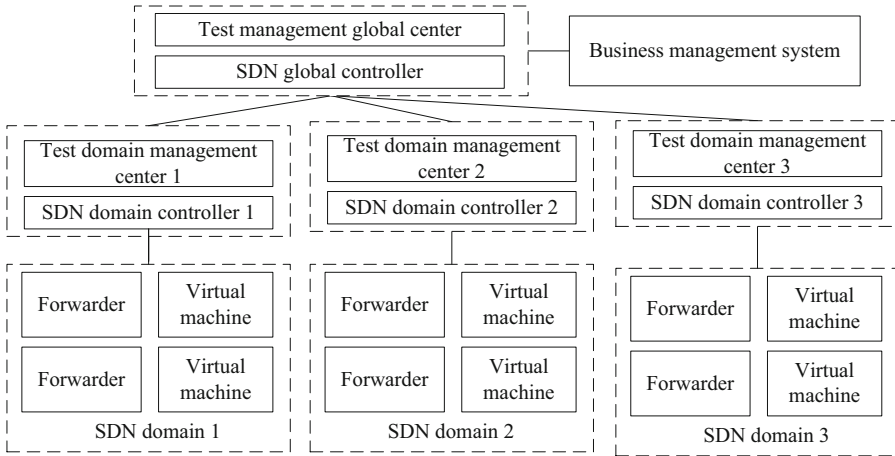


Fig. 1. Network test architecture.

platform for big data analysis, so as to explore the potential value of power grid data. For example, the common cloud analysis business is the operation and maintenance data analysis business. From the perspective of business demand for network resources, the demand of this kind of business for the power communication network is large uplink bandwidth. In terms of immersive services, such services mainly take advantage of the gradual increase of network bandwidth, and will use virtual reality technology to implement the work requiring complex environment. For example, the common immersion service is the VR-based network maintenance training service. From the perspective of network resource demand of services, the demand of such services for power communication network is low latency and large downlink bandwidth.

In terms of IoT business, this kind of business mainly uses IoT technology to manage a large number of widely distributed equipment, so as to improve management efficiency and save management costs. For example, the common Internet of Things business is intelligent meter reading business. From the perspective of business demand for network resources, this kind of business demand for power communication network is low packet loss and high reliability. In order to quickly obtain the business operation, the test management global center connects with the business management system.

## (2) Test center

Since the main research object of this paper is the network test mechanism in the multi-SDN domain environment, the architecture of the test center also adopts the multi-domain distributed test architecture. The test center is composed of one test management global center and multiple test domain management centers. The test management global center is responsible for receiving and sending test tasks. In terms of receiving test tasks, the test management global center interfaces with the business management system. The business management system sets the conditions for starting the test. The test management global center performs test tasks according to the test requirements of the business management system. To complete the test task, the business management system needs

to send the resource information used by the business to the test management global center. In terms of sending test tasks, the test management global center needs to interact with the SDN global controller to obtain the SDN domain information of the resources used by the business.

### (3) SDN controller

SDN controller includes SDN global controller and SDN domain controller. The main task of the SDN global controller is to interact with the SDN domain controller and distribute the test tasks of the test management global center to the relevant SDN domain controller. The main task of the SDN domain controller is to generate a test flow table according to the test needs and send it to the forwarder for execution. For multiple test domain management centers, one test domain management center is deployed for each SDN domain. After the test domain management center obtains the test task from the SDN global controller, it interacts with the SDN domain controller in the domain, generates the test flow table and sends it to the forwarder.

### (4) SDN domain

In the SDN domain, it includes multiple forwarders and multiple virtual machines. The function of the forwarder is to receive the flow table of the SDN domain controller and perform data forwarding. The function of virtual machine is to deploy specific business. In order to improve the network test performance and test quality, the repeater needs to report the execution of the forwarded data to the SDN domain controller in the domain according to the setting requirements. The SDN domain controller can report the results to the test domain management center to obtain the test results.

## 3 Network Test Mechanism

In order to guarantee the service quality and improve the service quality of the power communication network, this paper designs a quality-oriented power communication network test mechanism, as shown in Fig. 2. This mechanism includes six steps: the business management system discovers business exceptions, the test management global center triggers the test, the test management global center sends the test task to the test domain management center, the test domain management center sends the test request to the SDN domain controller, the SDN domain controller sends the flow table and feeds back the results to the test domain management center, and the test management global center collects the test domain management center results and analyzes them.

### (1) The business management system finds business exceptions

Based on the characteristics of current new network services, this paper divides network services into remote control services, cloud analysis services, immersive services, and Internet of Things services. According to the characteristics of these services, formulate exception discovery strategies. In terms of remote control business, take the remote power equipment control business as an example. When the service delay increases and the uplink bandwidth throughput decreases, the test mechanism needs to be triggered. The main test indicators are the network delay and uplink throughput. In terms of

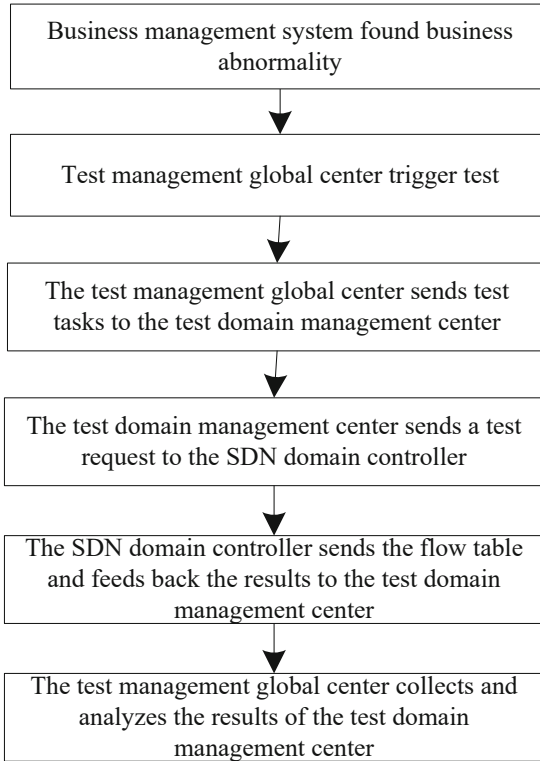


Fig. 2. Network test mechanism.

cloud analysis business, take the operation and maintenance data analysis business as an example. When the service uplink bandwidth throughput becomes small, the test mechanism needs to be triggered. The main test indicator is network throughput. In terms of immersive business, take VR conference business as an example. When the service delay increases and the downlink bandwidth throughput decreases, the test mechanism needs to be triggered. The main test indicators are the network delay and downlink throughput. In terms of IoT business, take intelligent meter reading business as an example. When the service packet loss becomes larger, the test mechanism needs to be triggered. The main test indicator is the network packet loss rate.

(2) Test management global center triggers test

The test management global center obtains the business exception notification from the business management system and business information. The obtained service information includes the service name, the network resource information used by the service, and the exception information of the service. In order to test the business-related network resources, the test management global center needs to obtain the business-related network resource information from the SDN global controller. The test management global center sends the service information to the SDN global controller to obtain the network resource information corresponding to the service. First, the virtual resource

information used by the business is obtained according to the business information, including the information of the forwarder and virtual machine. Secondly, according to the mapping relationship between virtual resources and physical resources, locate the underlying resource information, including the domain ID and resource ID of the controller and server.

(3) The test management global center sends test tasks to the test domain management center

The test management global center judges the test requirements according to the business situation and sends them to the relevant test domain management center for execution. In order to ensure the high-quality operation of network services, this paper divides the test tasks into four types: delay test, throughput test, packet loss rate test and fault location test. Among them, the delay test obtains the results by recording the receiving time of each test packet, the throughput test obtains the results by gradually increasing the number of test packets until the packet loss rate exceeds the threshold as the end condition, the packet loss rate test obtains the test results by recording the received proportion of the transmitted data packets, and the fault location test obtains the test results by specifying the proportion of the equipment data packets.

(4) The test domain management center sends a test request to the SDN domain controller

To complete the test task of the test management global center, the test request sent by the test domain management center to the SDN domain controller includes the type of test service, the information of test equipment, and the feedback method of test results. The type of test service can be one or more of four types: delay test, throughput test, packet loss rate test and fault location test. The information of the test equipment includes resource attributes such as resource ID, resource connection relationship, and the importance of the resource carrying service. The test results are fed back to the test domain management center and the test management global center. When the test result obtained by the SDN domain controller cannot determine the test target, it shall be fed back to the test domain management center. The test domain management center determines the feedback method of test results. When the test results obtained by the SDN domain controller are consistent with the test requirements, they can be directly fed back to the test management global center, and also fed back to the test domain management center for backup, so as to improve the efficiency of the test.

(5) SDN domain controller sends the flow table and feeds back the results to the test domain management center

After the test domain management center issues the test task to the SDN domain controller, each relevant SDN domain controller performs the test according to the requirements. In order to execute the test as required, each relevant SDN domain controller needs to generate a flow table according to the test task and distribute it to the in-domain forwarder. The intra-domain forwarder performs the test according to the flow table and returns the test results to the domain controller. According to the different requirements of the test work, the main technical indicators concerned during the test are different. For the delay test, the main test indicators include the number of test packets and the average

receiving time. For the throughput test, the main test index is the maximum number of test packets within the threshold of packet loss rate. For the packet loss rate test, the main test indicators include the number of test packets and the proportion of received data packets sent. For fault location test, the main test indicators include the number of test packets and the proportion of data packets passing the specified equipment. After the forwarder feeds back the test results to the domain controller, the domain controller feeds back the flow table and execution results to the test domain management center. The test domain management center calculates and feeds back to the test management global center.

(6) The test management global center collects and analyzes the results of the test domain management center

The test management global center analyzes the results of each domain management center and obtains the test results. The specific test result analysis method can be based on rules or artificial intelligence. In terms of how to use the test results, different strategies need to be adopted according to the test results. If the test results meet the requirements, the test management global center can feed back the business management system. The business management system calls other systems to implement business migration, network resource recovery, optimization and other strategies. If the test results cannot meet the requirements, the test management global center needs to adopt the iterative test strategy until the test results meet the requirements.

## 4 Performance Analysis

In order to understand the availability of the power communication network test mechanism proposed in this paper, the performance of the mechanism is analyzed below. According to the process and purpose analysis of the mechanism, the performance analysis in this paper is analyzed from the two dimensions of the availability and enforceability of the mechanism.

The availability of the mechanism mainly analyzes the value of the mechanism in service quality assurance. This mechanism is connected with the business management system and can quickly sense the operation of the business. The network operation and maintenance personnel can set the technical indicators that trigger the test according to the importance of the business, so as to quickly understand the status of the network to ensure the reliability of the business. In terms of ensuring business reliability, we can analyze it from the perspective of business reliability perception. The services involved in this mechanism include at least remote control, cloud analysis, immersion and Internet of Things. These businesses are the current mainstream business types and the development trend of new businesses in the future. Therefore, the mechanism can cover more business types. Secondly, the testing functions of this mechanism include at least delay, throughput, packet loss rate and fault location. These test functions can effectively sense the operation of the business, and cover the common needs of testing. Therefore, the test mechanism proposed in this paper can trigger tests according to management requirements, and can cover more business types and test methods, with good usability.

The enforceability of the mechanism mainly analyzes whether the mechanism can be implemented for power companies. The implement ability of this mechanism mainly involves two dimensions: the implement ability of technology and the convenience of maintenance personnel. The technical feasibility can be analyzed from the construction feasibility of the test component of the mechanism. In terms of the construction feasibility of test components, the mechanism mainly involves four components: business management system, test center, SDN controller, and SDN domain. Among them, business management system, SDN controller and SDN domain are common network management system components, which can be easily implemented. The test center component in the mechanism is the core component, including one test management global center and multiple test domain management centers. The difference between the function of the test center component and the existing system is that the interaction process of the test is different. It mainly includes the interaction between test center and SDN controller, test management global center and multiple test domain management centers. These interactive processes can be implemented using Socket technology or RESTful technology. Therefore, the test mechanism proposed in this paper is feasible in terms of construction feasibility. In terms of the convenience of maintenance personnel, the main work that maintenance personnel need to participate in is the setting of test trigger conditions and the analysis of test results. In terms of setting test trigger conditions, maintenance personnel can complete this work through knowledge base or discussion. This problem can be better solved through the strategy of experience accumulation. In the analysis of test results, maintenance personnel need to have strong analytical ability. In order to improve the ability of test result analysis, artificial intelligence technology can be used to improve the ability of maintenance personnel. Therefore, the test mechanism proposed in this paper is feasible in terms of technical implementation and ease of use.

To sum up, the mechanism proposed in this paper has good performance in terms of availability and enforceability, and can be applied to the test work of power communication network to improve service quality.

## 5 Conclusion

With the rapid development of virtualization technology, SDN technology is applied more and more widely in power communication network. In the SDN environment, network control and data forwarding are separated, improving the efficiency of network communication and resource utilization. However, SDN environment poses new challenges to service quality assurance, resulting in higher probability of network service problems and longer service repair time. In order to solve this problem, this paper first designs a network test architecture oriented to service quality under SDN environment. Secondly, the power communication network test mechanism oriented to service quality under SDN environment is designed. Through performance analysis, it is verified that the mechanism proposed in this paper has good performance in the two dimensions of availability and enforceability. In the performance analysis part, it can be seen that the trigger mechanism of the test and the analysis of the test results require the maintenance personnel to have strong maintenance ability. However, the maintenance ability of maintenance personnel is uneven, which easily leads to errors in some indicator settings and



analysis results. To solve this problem, based on the research results of this paper, further study the application of AI technology in business indicator exception trigger test and intelligent analysis of test results, so as to improve the application value of the research results of this paper.

## References

1. Li, Y., Yin, X., Wang, Z., et al.: A survey on network verification and testing with formal methods: approaches and challenges[J]. *IEEE Commun. Surv. Tutorials* **21**(1), 940–969 (2018)
2. Anerousis, N., Chemouil, P., Lazar, A.A., et al.: The origin and evolution of open programmable networks and SDN[J]. *IEEE Commun. Surv. Tutorials* **23**(3), 1956–1971 (2021)
3. Baert, M., Rossey, J., Shahid, A., et al.: The Bluetooth mesh standard: an overview and experimental evaluation[J]. *Sensors* **18**(8), 2409–2432 (2018)
4. Murillo, Y., Reynders, B., Chiumento, A., et al.: A multiprotocol low-cost automated testbed for BLE mesh[J]. *IEEE Commun. Mag.* **57**(3), 76–83 (2019)
5. Fang, Y., Lu, Y.: Checking intra-switch conflicts of rules during preprocessing of network verification in SDN[J]. *IEEE Commun. Lett.* **23**(9), 1547–1550 (2019)
6. Fang, Y., Lu, Y.: Real-time verification of network properties based on header space[J]. *IEEE Access* **8**, 36789–36806 (2020)
7. Zhao, Y., Zhang, P., Wang, Y., et al.: Troubleshooting data plane with rule verification in software-defined networks[J]. *IEEE Trans. Netw. Serv. Manage.* **15**(1), 232–244 (2017)
8. Amin, R., Reisslein, M., Shah, N.: Hybrid SDN networks: A survey of existing approaches[J]. *IEEE Commun. Surv. Tutorials* **20**(4), 3259–3306 (2018)



# Service Slice Resource Allocation Algorithm Based on Node Capability in Power Communication Network

Zhen Zheng<sup>1</sup>, Detai Pan<sup>1</sup>, Yunzhou Dong<sup>1</sup>, Zhengdong Lin<sup>1</sup>, and Peng Lin<sup>2</sup>(✉)

<sup>1</sup> Hainan Power Grid Communication Branch, HaiKou 570203, China

<sup>2</sup> Beijing VectInfo Technologies Co., Ltd., Beijing 100088, China  
linpeng@vectinfo.coms

**Abstract.** In the context of service slicing, network resource allocation has become a research focus. To reduce the energy consumption of power communication networks, this paper proposes a service slice resource allocation algorithm based on node capability in power communication network. This algorithm adopts a strategy of simultaneous node mapping and link mapping for resource allocation. Use breadth first algorithm for each virtual node to allocate resources for the virtual node and its connected links. When allocating resources to virtual nodes, based on the historical mapping experience of the underlying network, priority is given to opening the underlying node that has been mapped the most times. When allocating resources for virtual links, the shortest path algorithm is used to select the underlying links that have already been mapped to the underlying links from multiple paths, thereby reducing the energy consumption of the underlying link resources. By comparing existing algorithms, it has been verified that this algorithm saves energy consumption on underlying network resources and improves the success rate of virtual network mapping.

**Keywords:** Power communication network · Service slicing · Resource allocation · Underlying network · Virtual network

## 1 Introduction

With the rapid increase in the types and quantities of power business, the demand for power communication networks is rapidly increasing. To address the rapid increase in investment in the construction of power communication networks, network slicing technology has become the preferred network construction technology for power companies [1, 2]. In the network slicing environment, traditional power communication networks are divided into underlying networks and virtual networks. The underlying network focuses on building underlying nodes and links. Virtual networks focus on building electricity business by renting underlying network resources. In this context, how the underlying network allocates resources for virtual networks has become an important research topic.

In order to solve the problem of low resource utilization in the network slicing environment, literature [3] proposed an end-to-end slicing algorithm for 5G networks based on deep Q-learning. Reference [4] designed a virtual network resource backup mechanism based on node importance measurement, which improves the reliability of network slicing. Reference [5] designed an online allocation algorithm for network slicing resources, which improved the real-time performance of resource management. To address the issue of malicious competition among service providers leading to a decrease in service quality, Ref. [6] designed a resource competition mechanism for service providers with strategic resource allocation, which improved service quality. To solve the problem of low network reliability caused by demand uncertainty, Ref. [7] proposed a network slicing demand prediction algorithm, which improves the reliability of the network in environments with frequent changes in network topology. Through analysis of existing research, it can be seen that there are many algorithms that can allocate resources from the underlying network to the virtual network. However, existing algorithms have conducted less research on energy consumption, resulting in higher energy consumption in the underlying network, which not only increases the operating costs of the underlying network, but also leads to an increase in carbon emissions.

To reduce energy consumption in power communication networks, this paper proposes a service slice resource allocation algorithm based on node capability in power communication network. This algorithm adopts a strategy of simultaneous node mapping and link mapping, and uses a breadth first algorithm to allocate resources one by one for virtual nodes and their connected edges. When allocating resources to virtual nodes, based on the historical mapping experience of the underlying network, priority is given to opening the underlying node that has been mapped the most times. When allocating resources for virtual links, the shortest path algorithm is used to select the underlying links that have already been mapped from multiple paths, thereby reducing the energy consumption of the underlying link resources. By comparing existing algorithms, it has been verified that this algorithm saves energy consumption on underlying network resources and improves the success rate of virtual network mapping.

## 2 Network Model

In the network slicing environment, the power communication network is divided into underlying networks and virtual networks. The underlying network consists of underlying nodes and underlying links. The main function of the underlying network is to provide network resources for the virtual network. Virtual networks include virtual nodes and virtual links. The main function of virtual networks is to rent underlying network resources and carry power services. How to efficiently lease underlying nodes and links to virtual networks in the underlying network is an important research topic.

When allocating resources to virtual networks in the underlying network, the allocated resources include node resources and link resources. Node resources refer to the computing resources of nodes, while link resources refer to the bandwidth resources of links. Use  $G_c = (N_c, E_c)$  to represent the underlying network, where  $N_c$  represents the set of underlying nodes and  $E_c$  represents the set of underlying links. Use  $G_v = (N_v, E_v)$  to represent a virtual network, where  $N_v$  represents a set of virtual nodes and  $E_v$  represents a set of virtual links. The computing resources of the underlying node  $n_c^i \in N_c$

are represented by  $CPU(n_c^i)$ . The bandwidth resources of the underlying link  $e_c^i \in E_c$  are represented by  $BW(e_c^i)$ . The computing resources requested by virtual node  $n_v^i \in N_v$  from the underlying node are represented by  $CPU(n_v^i)$ , while the bandwidth resources requested by virtual link  $e_v^i \in E_v$  from the underlying link are represented by  $BW(e_v^i)$ .

### 3 Priority of Underlying Nodes

In order to improve the acceptance rate of virtual networks and reduce the energy consumption of underlying network resources, it is necessary to select appropriate underlying network resources for virtual networks. Below, with the goal of optimizing the resources of the underlying nodes, this paper will design a priority calculation method for the underlying nodes. When the virtual node to be mapped is  $n_v^i \in N_v$ , the set of virtual nodes directly connected to the surrounding allocated resources of virtual node  $n_v^i \in N_v$  is represented by  $N_v^i$ , and each element included is represented by  $n_v^j \in N_v^i$ . The underlying node set corresponding to the virtual node set  $N_v^i$  that has been allocated resources is represented by  $N_c^{N_v^i}$ , and each element is represented by  $n_c^{j-v} \in N_c^{N_v^i}$ . The set of underlying nodes directly connected to the elements in the set  $N_c^{N_v^i}$  of underlying nodes with unallocated resources around them is represented by  $N_c^{noUse-N_v^i}$ , and each element is represented by  $n_c^{j-noUse-v} \in N_c^{noUse-N_v^i}$ .

By filtering and sorting the elements in set  $N_c^{noUse-N_v^i}$ , the priority of each underlying node in set  $N_c^{noUse-N_v^i}$  can be obtained. Firstly, delete nodes that cannot meet the resource requirements of virtual node  $n_v^i \in N_v$ . Secondly, use formula (1) to calculate the carrying capacity of each underlying node, which is the sum of all virtual node resources carried on it, and arrange them in descending order. At this point, the larger the sum of resources, the more important and capable the current underlying nodes are, and they have strong resource allocation capabilities. Among them,  $n_v^j$  represents the virtual nodes hosted on the current underlying node, and  $n$  represents the number of virtual nodes hosted.

$$cap_{n_c^i} = \sum_{j=1}^n CPU(n_v^j) \quad (1)$$

In terms of link analysis of underlying nodes, formula (2) is used to calculate the link capacity  $abl_{n_c^i}^{link}$  of each underlying node. Among them,  $n_c^i \in N_c^{noUse-N_v^i}$ ,  $n_c^j \in N_c^{N_v^i}$ .  $hop(n_c^i, n_c^j)$  Represents the number of links in the shortest path between two underlying nodes. From formula (2), it can be seen that the greater the link capacity of each underlying node, the shorter the path between the current underlying node and the relevant underlying node, and the greater the degree of the node. At this point, resource allocation can save link resources, increase the number of selectable paths, and thus improve the success rate of mapping.

$$abl_{n_c^i}^{link} = \frac{degree_{n_c^i}}{\sum_{n_c^j \in N_c^{N_v^i}} hop(n_c^i, n_c^j)} \quad (2)$$

By adding weights to formulas (1) and (2), the priority of each underlying node can be obtained. Among them,  $\alpha$  is used to adjust the weight of the bearing capacity  $cap_{n_c^i}$  of the underlying node and the link capacity  $abl_{n_c^i}^{link}$  of the underlying node.

$$pri_{n_c^i} = \alpha * cap_{n_c^i} + (1 - \alpha) * abl_{n_c^i}^{link} \quad (3)$$

## 4 Resource Allocation Algorithm

In order to save energy consumption, this article adopts a mapping strategy of node mapping and link mapping simultaneously, and designs a Service slice Resource Allocation Algorithm based on Node Capability in power communication Network (SRAAoNC).

When allocating resources for virtual networks, the breadth first allocation algorithm is used to determine the relationship between the underlying nodes and the underlying links they are connected to one by one, thereby saving energy consumption. When mapping nodes, based on historical mapping experience, priority is given to the nodes that have been mapped the most times, and the underlying nodes that have been opened and cannot be mapped repeatedly are selected. When mapping links, the shortest path algorithm is used to obtain multiple alternative paths, and the energy consumption of the links is reduced by selecting the links that have already been mapped to the underlying links. The SRAAoNC proposed in this article is shown in Table 1.

**Table 1.** SRAAoNC.

---

### 1. Select the first virtual node and allocate resources to it

- (a) Weighted sum based on resource requirements and degrees to obtain the largest virtual node
- (b) Select an underlying node from the underlying nodes that has a larger weighted sum of available resources and degrees, and meets the virtual resource requirements, to allocate resources to it

### 2. Allocate resources for other virtual resources

- (a) Starting from the virtual nodes with allocated resources, use the breadth first algorithm to obtain the virtual nodes that need to be mapped
  - (b) Use formula (3) to obtain the  $pri_{n_c^i}$  of underlying node of the virtual node
  - (c) Determine whether there are virtual links between the mapped virtual nodes and they are not mapped. If so, perform link allocation (step d). If not, select the next virtual node for allocation (step a)
  - (d) Use the shortest path to find k underlying path resources for the current virtual link
  - (e) Delete underlying paths that contain underlying links that cannot meet bandwidth requirements
  - (f) If there are more than one underlying path, calculate the number of underlying links that have already hosted virtual links on each underlying path
  - (g) Select the underlying path with the highest number of underlying links and allocate resources for the current virtual link
-

This algorithm mainly includes two steps: selecting the first virtual node and allocating resources to it, and allocating resources to other virtual resources. In the step of selecting the first virtual node and assigning resources to it, the first weighted sum is calculated based on resource requirements and degrees, and the virtual node with the highest sum is used as the first virtual node to allocate resources. When allocating resources to virtual nodes, select the underlying nodes with a larger sum of available resources and degree weighting, and meet the virtual resource requirements, to allocate resources to them.

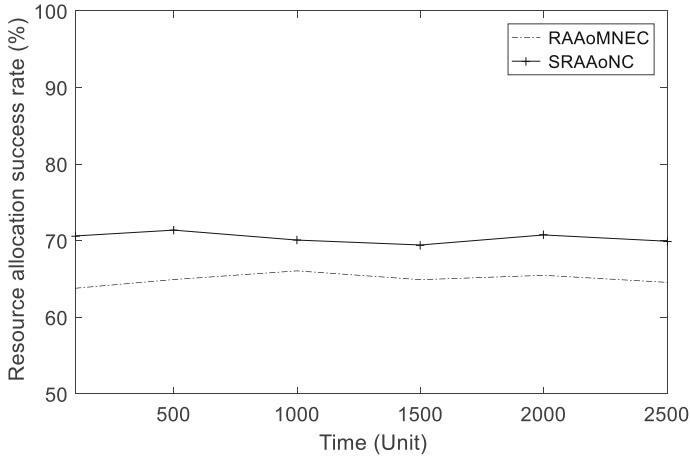
When allocating resources to other virtual resources, a strategy of simultaneous allocation of virtual nodes and virtual links is adopted. When allocating nodes, starting from the virtual nodes that have already been allocated resources, the breadth first algorithm is used to obtain the virtual nodes that need to be mapped. And use formula (3) to obtain the optimal bottom node  $pri_{n_c}$  value of the virtual node. In the step of allocating links, when there are virtual links between mapped virtual nodes and they are not mapped, the shortest path algorithm is used to find the underlying path that meets bandwidth requirements and has a large number of virtual links already carried, and allocate resources for it. In the algorithm, the number of underlying links that have already hosted virtual links on each underlying path refers to the number of underlying links that have already hosted virtual links in the underlying path. The more virtual links are already hosted, the fewer new underlying links need to be opened.

## 5 Performance Analysis

In order to analyze the performance of the power communication network service slicing resource allocation algorithm based on node capability SRAAoNC proposed in this article, the GT-ITM tool [8] was used in the experiment to generate a network environment. The network environment includes both the underlying network and the virtual network, where the underlying network is composed of 500 underlying network nodes, and the number of virtual nodes in the virtual network follows a uniform distribution of [2, 6]. In terms of network resources, the computing resources of the underlying nodes and the bandwidth resources of the underlying links follow a uniform distribution of [40, 60], while the computing resources of the virtual nodes and the bandwidth resources of the virtual links follow a uniform distribution of [3, 5]. To analyze the convergence of algorithms after long-term operation, set a certain duration for the arrival and lifecycle of each virtual network. The arrival of each virtual network is set to 2 Unit of time, and the life cycle of each virtual network is set to 10 Unit of time. Due to the optimization strategy of sharing existing resources, the comparative algorithm used in this article is the Resource Allocation Algorithm based on Minimizing Node Energy Consumption (RAAoMNEC). The comparison algorithm RAAoMNEC adopts an optimization strategy of minimizing energy consumption for resource allocation.

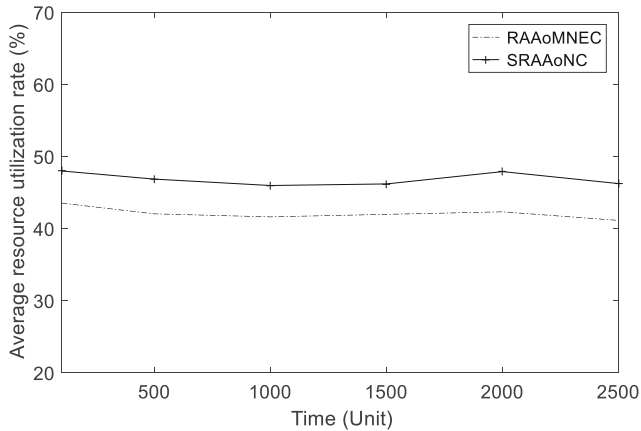
The comparison results of the success rate of virtual network resource allocation are shown in Fig. 1. The X-axis in the figure represents the running time of the two algorithms, while the Y-axis represents the success rate of resource allocation. From the running results, it can be seen that compared with the comparison algorithm RAAoMNE, the success rate of virtual network resource allocation under the algorithm SRAAoNC

in this paper is higher. This is because the algorithm in this article selects resources with high node link capacity for allocation. The greater the link capacity of a node, the shorter the path between the current underlying node and the related underlying node. When the degree of a node is large, it can save more link resources and select more paths, which improves the success rate of virtual network mapping.



**Fig. 1.** Comparison of success rates of virtual network resource allocation.

The comparison results of the average utilization of underlying network resources between the two algorithms are shown in Fig. 2, where the X-axis represents the running time of the algorithm and the Y-axis represents the average utilization of network resources. From the running results of the two algorithms, it can be seen that for the RAAoMNE algorithm, the SRAAoNC algorithm in this paper has a higher utilization rate of network resources. This is because the algorithm in this article uses the shortest path algorithm to obtain multiple paths during link mapping, and selects the links that have already been mapped to the underlying links, thereby saving link energy consumption. In addition, selecting allocated resources during each resource allocation saves more available link resources for the network, thereby improving the success rate of virtual network allocation. So, the underlying network allocates more underlying network resources to the virtual network, improving the utilization rate of underlying network resources.



**Fig. 2.** Average utilization rate of underlying network resources.

## 6 Conclusion

In the network slicing environment, the efficiency of creating network services is rapidly improving. To improve the utilization of underlying network resources, resource allocation of network slicing has become a research focus. To reduce the energy consumption of power communication networks, this paper proposes a service slice resource allocation algorithm based on node capability in power communication network. This algorithm adopts a strategy of simultaneous node mapping and link mapping, allocating resources one by one for virtual nodes and their connected edges. By comparing existing algorithms, it has been verified that this algorithm saves energy consumption on underlying network resources and improves the success rate of virtual network mapping. Due to the reliability of network services being an important aspect of customer satisfaction. In the next step of work, based on the research results of this article, we will study the improvement mechanism of network business reliability and further enhance the application value of the research results of this article.

## References

1. Shurman, M., Taqieddin, E., Oudat, O. et al.: Performance enhancement in 5G cellular networks using priorities in network slicing[C]. In: 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pp. 822–826. IEEE (2019)
2. Chen, X., Ng, D.W.K., Yu, W., et al.: Massive access for 5G and beyond[J]. *IEEE J. Sel. Areas Commun.* **39**(3), 615–637 (2020)
3. Li, T., Zhu, X., Liu, X.: An end-to-end network slicing algorithm based on deep Q-learning for 5G network[J]. *IEEE Access* **8**, 122229–122240 (2020)
4. Wang X, Lu X, Fu M, et al. Optimization for Survivable 5G Network slice provisioning with augmented infrastructure[C]. In: 2021 9th International Conference on Communications and Broadband Networking, pp. 192–196 (2021)
5. Zhao, H., Deng, S., Liu, Z., et al.: Dpos: decentralized, privacy-preserving, and low-complexity online slicing for multi-tenant networks[J]. *IEEE Trans. Mob. Comput.* **21**(12), 4296–4309 (2021)



6. Guijarro, L., Vidal, J.R., Pla, V.: Competition between service providers with strategic resource allocation: application to network slicing[J]. *IEEE Access* **9**, 76503–76517 (2021)
7. Zhou, J., Zhao, W., Chen, S.: Dynamic network slice scaling assisted by prediction in 5G network[J]. *IEEE Access* **8**, 133700–133712 (2020)
8. Zegura, E.W., Calvert, K.L., Bhattacharjee, S.: How to model an internetwork[C]. Proceedings of IEEE INFOCOM'96 Conference on Computer Communications. *IEEE* **2**, 594–602 (1996)



# Evaluation of Activation Functions in Convolutional Neural Networks for Image Classification Based on Homomorphic Encryption

Huixue Jia<sup>1</sup>, Daomeng Cai<sup>2</sup>, Zhilin Huo<sup>2</sup>, Cong Wang<sup>3,4(✉)</sup>, Shibin Zhang<sup>5,6</sup>, Shujun Zhang<sup>7(✉)</sup>, Xiaoyu Li<sup>1</sup>, and Shan Yang<sup>8</sup>

<sup>1</sup> School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China

<sup>2</sup> CSCC System Engineering Research Institute, Beijing, China

<sup>3</sup> Intelligent Policing Key Laboratory of Sichuan Province, Chengdu, China

<sup>4</sup> Sichuan Police College, Chengdu, China

`cong-wang@foxmail.com`

<sup>5</sup> Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Chengdu, China

<sup>6</sup> Chengdu University of Information Technology, Chengdu, China

<sup>7</sup> School of Aeronautics and Astronautics, University of Electronic Science and Technology of China, Chengdu, China

`zhangsj@uestc.edu.cn`

<sup>8</sup> Department of Chemistry, Physics, and Atmospheric Sciences, Jackson State University, Jackson, MS, USA

**Abstract.** In the dynamic environment of big data and cloud computing, image feature classification has become a key factor spanning various fields. Ensuring the security, privacy, and computational efficiency of image data, while minimizing the processing of image data and maintaining the effectiveness of encrypted classification, is a significant challenge. In this paper, we propose a new method, Homomorphic Encryption Image Classification Evaluation (HEICE), for secure image classification. This method leverages the power of Convolutional Neural Networks (CNNs) and the security of Homomorphic Encryption (HE) to perform image classification on encrypted data. Each model uses different activation functions: square function, polynomial approximation of ReLU, polynomial approximation of Sigmoid and Tanh, and a piecewise linear approximation. These modified models are then used to test encrypted images, and the results are compared with the baseline. This method allows us to evaluate the performance of different activation functions when processing encrypted data and to choose the most suitable model for image classification, i.e., the classification model with the square function as the activation function. Our method provides a systematic approach to address the challenge of ensuring model performance while maintaining data security in image classification. This comparison validates the effectiveness of our method in achieving the dual objectives of maintaining data privacy and achieving accurate image classification.

**Keywords:** Homomorphic encryption · Image classification · Convolutional Neural Networks

## 1 Introduction

In the era of big data and machine learning, image classification has emerged as a key task in a variety of applications, from medical imaging to autonomous driving. However, as these applications often involve sensitive data, ensuring privacy during the image classification process has become a paramount concern.

A reasonable solution to these issues is to delegate the training task to the users [1]. In the era of cloud computing and big data, the practice of outsourcing data to cloud servers is increasingly prevalent [2]. However, with the surge of malicious users on the internet and the inherent unreliability of cloud service providers, privacy and security issues are paramount. Therefore, developing an efficient and privacy-centric deep learning framework is of utmost importance.

Homomorphic encryption, which allows computation on encrypted data, is a promising solution to this problem [1, 3]. It enables the model to learn from the data without actually seeing it, thereby preserving privacy [4]. By leveraging the inherent sparsity of image data, we reduce the computational burden of fully homomorphic encryption while preserving the privacy of sensitive image data.

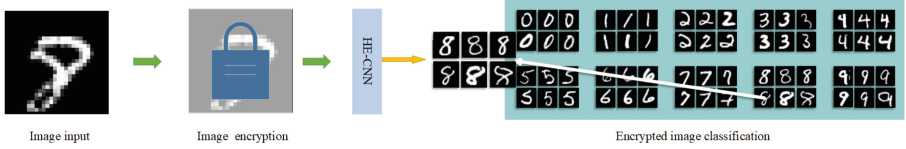
This paper presents a new method for image classification on fully homomorphic encrypted data. The approach modifies a traditional Convolutional Neural Network (CNN) model to process encrypted images and explores different activation functions compatible with homomorphic encryption [5]. The performance of these models is evaluated against a baseline, with the goal of identifying the most suitable model and activation function for encrypted image classification.

Our work contributes significantly in three main areas: We develop an innovative model that modifies traditional Convolutional Neural Networks (CNNs) to handle encrypted data, ensuring accurate image classification while preserving data privacy. We implement an adaptive selection of activation functions, including a square function and polynomial approximations of ReLU, Sigmoid, and Tanh, allowing us to evaluate their performance with encrypted data and choose the most suitable one. We conduct a comprehensive evaluation of our results by comparing the performance of our models trained on encrypted data with baseline models trained on original images, validating the effectiveness of our approach (Fig. 1).

## 2 Related Work

### 2.1 Convolutional Neural Networks for Image Classification

Convolutional Neural Networks (CNNs) have gained significant traction in the realm of image classification tasks, primarily due to their inherent capability to autonomously and adaptively learn spatial hierarchies of features from the



**Fig. 1.** We utilized Complete Homomorphic Encryption (CKKS) to encrypt original images, which were then classified using a modified Convolutional Neural Network, ensuring both effective image classification and data privacy

input images. This unique characteristic allows CNNs to capture complex patterns and structures within the data, making them particularly suited for tasks involving high-dimensional data such as images. The seminal work of Krizhevsky et al. [6] served as a catalyst in demonstrating the power of CNNs in large-scale image recognition tasks. Their model, known as AlexNet, achieved state-of-the-art results on the ImageNet dataset, a large-scale, diverse web images dataset designed for visual object recognition software research. This achievement marked a significant milestone in the field of computer vision, showcasing the potential of CNNs in handling complex image recognition tasks.

Following this breakthrough, a multitude of CNN architectures have been proposed, each aiming to further enhance the performance of image classification tasks. The VGGNet [7], proposed by Simonyan and Zisserman, introduced a deeper and wider variant of CNNs. It demonstrated that the depth of the network (i.e., the number of layers) is a critical component for good performance.

He et al. introduced the ResNet [8], which incorporated the concept of residual learning to address the problem of training extremely deep neural networks. By using shortcut connections or skip connections, the ResNet model can effectively learn feature representations with a significantly increased depth, leading to improved classification performance. DenseNet [9], proposed by Huang et al., further extended this idea by connecting each layer to every other layer in a feed-forward fashion. This dense connectivity pattern resulted in improved information flow between layers, which in turn led to better performance and efficiency.

These advancements in CNN architectures have significantly pushed the boundaries of what is possible in image classification tasks, demonstrating the ongoing evolution and adaptability of CNNs in tackling complex, high-dimensional data.

## 2.2 Homomorphic Encryption for Privacy-Preserving

Homomorphic Encryption (HE) allows computations to be performed directly on encrypted data without requiring decryption, thereby ensuring data privacy. This revolutionary concept was first proposed by Gentry [10] in a fully homomorphic encryption scheme, which supports arbitrary computations on encrypted data.

Since Gentry’s groundbreaking work, various HE schemes have been proposed to enhance the efficiency and security of computations on encrypted data. Among

these, the BGV scheme proposed by Brakerski et al. [11] stands out for its efficiency in performing numerous operations on encrypted data. This scheme has significantly advanced the field of homomorphic encryption by reducing the computational complexity and improving the practicality of computations on encrypted data.

Further extending the capabilities of HE, Cheon et al. [12] proposed the CKKS scheme, which supports approximate arithmetic on encrypted real or complex numbers. Unlike previous schemes that primarily focus on integer operations, the CKKS scheme is designed to handle real or complex numbers, making it particularly suitable for tasks that require computations on floating-point numbers, such as image classification tasks. This scheme has opened up new possibilities for applying homomorphic encryption in machine learning and image processing tasks, where the ability to perform computations on encrypted real numbers is crucial.

## 3 Method

### 3.1 Establishment of the Encryption Model

**3.1.1 Image Data Preprocessing** The first stage of our method involves comprehensive preprocessing of image data. This crucial step ensures the normalization and enhancement of input data for the Convolutional Neural Network (CNN) model [13], thereby promoting effective feature learning. Preprocessing includes several transformations:

**Image Resizing:** Utilizing the OpenCV library, we adjust the size of all images to a uniform  $256 \times 256$  pixels. This ensures the consistency of the input data, a prerequisite for CNN models that require fixed-size input.

**Data Augmentation:** To enhance the robustness of the model and prevent overfitting, we employ data augmentation techniques, including rotation ( $\pm 15^\circ$ ), horizontal flipping, and translation ( $\pm 10\%$ ).

**Contrast Enhancement:** Linear contrast stretching maps the minimum and maximum pixel intensity values of the image to predetermined minimum and maximum intensity values to enhance contrast. By stretching the contrast of the image, the features of the image become more prominent [14].

$$I_{out} = (I_{in} - I_{min}) \times \frac{(O_{max} - O_{min})}{(I_{max} - I_{min})} + O_{min} \quad (1)$$

where  $I_{in}$  represents the pixel intensity values of the input image,  $I_{min}$  and  $I_{max}$  are the minimum and maximum pixel intensity values of the input image,  $O_{min}$  and  $O_{max}$  are the predetermined minimum and maximum intensity values,  $I_{out}$  represents the pixel intensity values of the output image.

**Data Augmentation:** To enhance the robustness of the model and prevent overfitting, we employ data augmentation techniques, including rotation ( $\pm 15^\circ$ ), horizontal flipping, and translation ( $\pm 10\%$ ).

**3.1.2 Image Homomorphic Encryption** We employ the Cheon-Kim-Kim-Song (CKKS) homomorphic encryption scheme to encrypt the original image test set, resulting in an encrypted test set. The Cheon-Kim-Kim-Song (CKKS) homomorphic encryption scheme is employed to encrypt the original image test set, creating an encrypted test set. CKKS offers several advantages over other encryption methods, including the ability to handle real or complex numbers, high security, efficiency, scalability, and robustness against noise. It is particularly suitable for encrypting data types like image pixels that contain real or complex values. CKKS also allows for a wide range of computations on encrypted data, including addition and multiplication, making it a powerful tool for secure computation on encrypted data [15].

There is actually different ways for doing convolution, and one way we can do it is via a well-known algorithm that translates the 2D convolution into a single matrix multiplication operation. In this process, it is imperative to ensure that the encryption scheme is robust enough to thwart any potential decryption attacks. This means that the encryption scheme must provide a high level of security, making it computationally infeasible for an attacker to decrypt the encrypted data without the correct key.

The CKKS and encryption schemes, which we employ in our method, are complex and involve several mathematical operations. However, a simplified representation of the encryption process can be given as follows:

$$E(m) = (m + r) \pmod{q} \quad (2)$$

where  $E(m)$  is the encrypted message,  $m$  is the original message,  $r$  is a random number, and  $q$  is a large prime number.

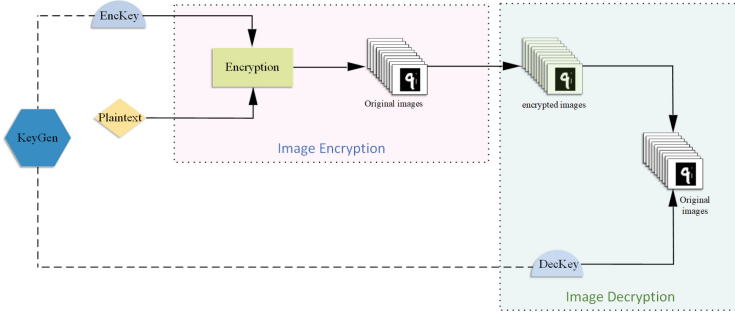
Moreover, the encryption scheme must be capable of handling the size and complexity of image data [15]. Image data, particularly high-resolution images, can be quite large and complex, with thousands of pixels each having multiple intensity values. Therefore, the encryption scheme must be efficient and scalable, capable of encrypting and decrypting large amounts of data quickly and without significant computational overhead.

This step of encrypting the image data is crucial as it ensures the privacy of the data while still allowing for computations to be performed on the encrypted data. This is the cornerstone of privacy-preserving image classification tasks, enabling the development of models that can operate directly on encrypted data. The encryption and decryption process is shown in the Fig. 2.

## 3.2 Constructing Encrypted Image Classification Models

Given the complexity of the image dataset, we construct a simple CNN model for encrypted image classification. Given the proven efficacy of CNNs in image recognition tasks, we favor the use of CNNs as they are capable of independently learning hierarchical features from images.

**Network Design:** The network comprises two convolutional layers with  $3 \times 3$  kernels and 16 and 32 filters, respectively. These layers are designed to learn



**Fig. 2.** The figure illustrates the use of full homomorphic encryption in image processing, where an encryption key is generated to encrypt unique image blocks, and a decryption key is used to decrypt these blocks

spatial hierarchical features. A fully connected layer with 128 neurons serves as the output, classifying these features into image classes. Finally, an output layer with six neurons is implemented, corresponding to the six categories in our dataset [16].The convolution layer is calculated as shown in Eq. 3:

$$(F * I)(i, j) = \sum_m \sum_n F(m, n)(i - m, j - n) \tag{3}$$

where  $F$  is the filter or kernel,  $I$  is the input image, and  $(i, j)$  are the spatial coordinates.

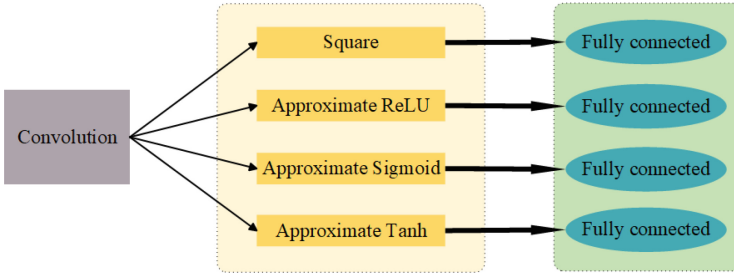
Activation Function: Rectified Linear Unit (ReLU) activation functions are applied after the convolutional and pooling layers. ReLUs introduce non-linearity without affecting the receptive fields of the convolutional layers. The Rectified Linear Unit (ReLU) activation function is represented as Eq. 5:

$$f(x) = \max(0, x) \tag{4}$$

Optimization and Training: Cross-entropy is used as our loss function. For network optimization, we employ the Adam optimizer, which updates weights based on adaptive estimates of lower-order moments. The model is trained on the training set and validated on the validation set to evaluate its performance. Regular monitoring of the performance on the validation set allows early detection of overfitting and provides feedback on when to stop training [17]. The update rule for Adam can be represented as:

$$\theta_{t+1} = \theta_t - \frac{\eta}{\sqrt{\hat{v}_{t+1} + \epsilon}} \hat{m}_{t+1} \tag{5}$$

where  $\theta$  are the parameters (weights),  $\eta$  is the learning rate,  $\hat{v}_{t+1}$  and  $\hat{m}_{t+1}$  are estimates of the first and second moments of the gradients, and  $\epsilon$  is a small constant to avoid division by zero.



**Fig. 3.** The figure shows how the four activation functions can be used in the model, includes a square function, a polynomial approximation of the Rectified Linear Unit (ReLU) function, polynomial approximations of the Sigmoid and Tanh functions

### 3.3 Evaluation of Various Activation Functions

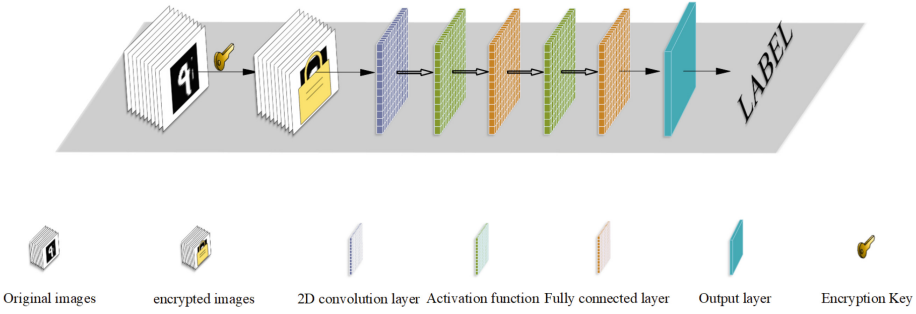
**3.3.1 Modification of the Model for Encrypted Data** The original image model is adapted to handle encrypted data. We construct four distinct models, each employing a different activation function. These include a square function, a polynomial approximation of the Rectified Linear Unit (ReLU) function, polynomial approximations of the Sigmoid and Tanh functions, and a piecewise linear approximation [18,19]. The Fig. 3 shows how the four activation functions can be used in the model.

The modification process ensures that the changes do not compromise the performance of the model. It may necessitate adjustments to the model's architecture or parameters to accommodate the characteristics of the encrypted data [20].

**3.3.2 Training and Testing of the Models** Each of the four models is trained on the encrypted image training set and tested on the encrypted image test set. This process is crucial in evaluating the performance of the models when handling encrypted data [20]. The training and testing procedures are conducted in a manner that ensures the test set is representative, thereby allowing the test results to reflect the models' performance in practical applications [21]. A generic model of the modified image model processing process for various activation functions is shown in Fig. 4.

The training phase involves adjusting the model parameters to minimize the loss function, while the testing phase involves evaluating the model's performance on unseen data. The results from these phases provide valuable insights into the effectiveness of the different activation functions when applied to encrypted data [22].





**Fig. 4.** This image illustrates a complex image processing pipeline. Initially, the original images are encrypted using Complete Homomorphic Encryption. Subsequently, these encrypted images are processed by a modified Convolutional Neural Network. This procedure is capable of performing effective image classification while safeguarding the privacy of the image data

### 3.4 Evaluation of Various Activation Functions

**3.4.1 Comparison of Test Results** The evaluation of our proposed models is conducted through a rigorous comparison of their test results with the classification outcomes of the original, unencrypted images [23].

The comparison process is meticulously designed and executed in a systematic manner [24]. This approach ensures that any observed differences in performance are accurately captured and can be directly attributed to the variations in the activation functions employed in each model. This systematic comparison not only provides a fair and comprehensive evaluation of each model’s performance but also offers valuable insights into the influence of different activation functions on the classification accuracy of encrypted images.

Through this rigorous evaluation process, we aim to identify the most effective activation function for encrypted image classification, thereby contributing to the optimization of neural network models for secure and privacy-preserving image classification tasks [24].

## 4 Result

### 4.1 Classification of Encrypted Images

In this section, we elucidate the process of classifying encrypted images using the image classification models we have constructed. We delve into the intricacies of building the encryption model, emphasizing its accuracy and performance. The performance of the models is gauged in terms of their ability to accurately classify encrypted images, and a comparative analysis is conducted to evaluate their relative efficiencies. This comprehensive assessment provides valuable insights into the effectiveness of our models and their potential for practical application in the realm of encrypted image classification. The time spent and the number of

polynomial modes used for classification by different activation function models are shown in the Table 1.

It is evident from our analysis that the classification time consumed by the square function is significantly less than that of the other three functions. Concurrently, the polynomial modulus can reach twice the magnitude of the other three functions. Furthermore, an increase in the polynomial modulus correlates with an enhancement in the accuracy of encryption. Therefore, in an overarching perspective, the square function emerges as the optimal choice for the activation function of the model in this study. This is attributed to its capacity to augment computational accuracy while concurrently reducing classification time substantially.

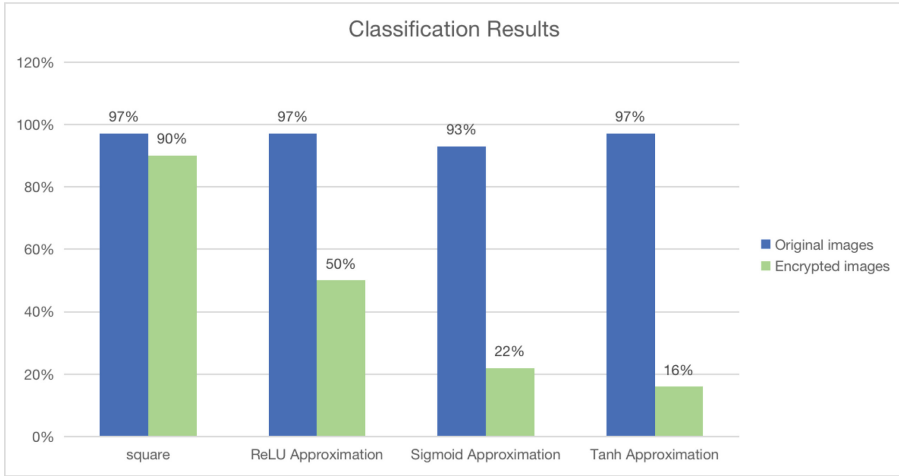
**Table 1.** This table shows the number of time and polynomial patterns used for classification by different activation function models, square function, ReLU approximation function, Sigmoid approximation function and Tanh approximation function

	Time(s)	Polynomial modulus
Square	644.8	32768
Relu approximation	7447.2	16384
Sigmoid approximation	7666.5	16384
Tanh approximation	7658.3	16384

## 4.2 Evaluation of Activation Functions

In this subsection, we present a rigorous evaluation of the performance of various activation functions employed within the models. We have incorporated a diverse set of activation functions, including a square function, a polynomial approximation of ReLU, polynomial approximations of Sigmoid and Tanh, and a piecewise linear approximation. The accuracy of each model, characterized by these distinct activation functions, was meticulously assessed and compared. This comparative analysis provides a comprehensive understanding of the impact of different activation functions on the performance of the models in the context of encrypted image classification.

The comparative results between the original model and the cryptographic model, each employing different activation functions for classification, are illustrated in Fig. 5. The accuracy of the original image classification, when utilizing the square function, polynomial approximation of ReLU, polynomial approximation of Sigmoid and Tanh, and a piecewise linear approximation as activation functions, are recorded as 97%, 97%, 93%, and 97%, respectively. These results underscore the high accuracy achieved by the CNN model in its application. Conversely, the accuracy of the encrypted models, when these activation functions are employed, are observed to be 90%, 55%, 22%, and 16%, respectively.



**Fig. 5.** This image depicts the comparison results of the classification performed by the original model and the encrypted models with different activation functions. This visual representation underscores the practicality and effectiveness of the method we propose to a certain extent

Notably, only the square function achieves a more satisfactory result. This visual representation underscores, to a certain extent, the practicality and effectiveness of our proposed methodology.

### 4.3 Comparison with Other Models

The methodology delineated in this thesis demonstrates a remarkable performance in terms of both time efficiency and classification effectiveness. This evaluation takes into account a multitude of factors, including encryption time, classification accuracy, and computational overhead, among others. A comparison is shown in the Table 2.

The Residue Activation Network (ResActNet) [25], a novel deep network architecture that employs a scaled power activation function. In the context of encrypting 100 image samples, a task that is both computationally intensive and time-consuming, our proposed model exhibits a significant reduction in the encryption time compared to that of ResActNet. This improvement in time efficiency underscores the computational advantages of our proposed model, particularly in scenarios involving large-scale image datasets.

Furthermore, we draw a comparison with the implementation of ResNet-20 on the RNS-CKKS scheme [26]. This implementation applies Fully Homomorphic Encryption (FHE) with a bootstrap function to the standard deep machine learning model, thereby enabling secure computation on encrypted data. Despite the inherent complexity and computational demands of FHE, our proposed model manages to markedly enhance encryption efficiency.

Importantly, this enhancement in efficiency does not come at the expense of classification accuracy. Our proposed model maintains a similar encryption classification accuracy to the model implemented on the RNS-CKKS scheme. This balance between efficiency and accuracy is a testament to the robustness of our proposed model, highlighting its potential for practical application in the realm of secure image classification. In conclusion, the superior performance of our proposed model, as evidenced by its time efficiency, classification effectiveness, and robustness against other existing methods, underscores its potential as a viable solution for secure image classification tasks.

**Table 2.** The table offers a comparative evaluation of our proposed method against existing techniques like the RNS-CKKS Scheme and ResActNet. It assesses parameters such as classification accuracy on original and encrypted images, encryption time, and dataset size, providing a robust measure of our method’s performance and efficiency relative to established techniques

Method	Accuracy (%)	Encryption accuracy (%)	Time(s)	numbers
RNS-CKKS Scheme	91.89	92.43	10602	1000
ResActNet	83.82	83.82	685.4	100
<b>Our Method</b>	<b>97.00</b>	<b>90.00</b>	<b>644.8</b>	<b>1000</b>

## 5 Summary

This paper presents a detailed procedure for classifying encrypted images using a specially engineered image classification model. The focus is on the construction of the encryption model, with an emphasis on its precision and performance. The models’ effectiveness is assessed based on their ability to accurately classify encrypted images, and a comparative analysis is conducted to evaluate their relative efficiency.

The performance of various activation functions within the model is rigorously evaluated, including the square function, the polynomial approximation of ReLU, the polynomial approximations of Sigmoid and Tanh, and the segmented linear approximation. The accuracy of each model, characterized by these distinct activation functions, is carefully assessed and compared. This analysis provides a comprehensive understanding of the impact of different activation functions on model performance, contributing to the advancement of homomorphic encryption-based image classification techniques.

The outcomes of our model are compared with a baseline, which is the classification of the original, unencrypted images. This comparison serves as a critical benchmark for evaluating the performance of our proposed methodology. The trade-off between accuracy and security is explored, and the effectiveness of our approach in achieving accurate image classification while preserving data privacy is thoroughly assessed. The square function is found to exhibit superior

performance in terms of both time consumption and cryptographic classification outcomes, suggesting its potential use as an activation function in cryptographic classification models.

**Funding Statement** This work was supported in part by the Open Fund of Advanced Cryptography and System Security Key Laboratory of Sichuan Province (No. SKLACSS-202111), in part by the Opening Project of Intelligent Policing Key Laboratory of Sichuan Province (No.ZNJW2023KFMS005), in part by the Innovative Research Foundation of Ship General Performance(No. 25422218) and in part by the National Key R&D Program of China (No. J2019-V-0001-0092).

## References

1. Preuveneers, D., Rimmer, V., Tsingenopoulos, I., Spooren, J., Joosen, W., Ilie-Zudor, E.: Chained anomaly detection models for federated learning: an intrusion detection case study. *Appl. Sci.* **8**(12), 2663 (2018)
2. Rathore, S., Pan, Y., Park, J.H.: Blockdeepnet: a blockchain-based secure deep learning for iot network. *Sustainability* **11**(14), 3974 (2019)
3. Hayes, J., Melis, L., Danezis, G., De Cristofaro, E.: Logan: membership inference attacks against generative models (2017). [arXiv:1705.07663](https://arxiv.org/abs/1705.07663)
4. Riad, K., Hamza, R., Yan, H.: Sensitive and energetic iot access control for managing cloud electronic health records. *IEEE Access* **7**, 86384–86393 (2019)
5. Hitaj, B., Ateniese, G., Perez-Cruz, F.: Deep models under the gan: information leakage from collaborative deep learning. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 603–618 (2017)
6. Krizhevsky, A., Sutskever, I., Hinton, G.E.: Imagenet classification with deep convolutional neural networks. *Commun. ACM* **60**(6), 84–90 (2017)
7. Simonyan, K., Zisserman, A.: Very deep convolutional networks for large-scale image recognition (2014). [arXiv:1409.1556](https://arxiv.org/abs/1409.1556)
8. He, K., Zhang, X., Ren, S., Sun, J.: Deep residual learning for image recognition. In: *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 770–778 (2016)
9. Huang, G., Liu, Z., Van Der Maaten, L., Weinberger, K.Q.: Densely connected convolutional networks. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 4700–4708 (2017)
10. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: *Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing*, pp. 169–178 (2009)
11. Yagisawa, M.: Fully homomorphic encryption without bootstrapping. *Cryptology ePrint Archive* (2015)
12. Cheon, J.H., Kim, A., Kim, M., Song, Y.: Homomorphic encryption for arithmetic of approximate numbers. In: *Advances in Cryptology—ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3–7, 2017, Proceedings, Part I*, vol. 23, pp. 409–437. Springer (2017)
13. Zheng, D., Tang, X., Wu, X., Zhang, K., Lu, C., Tian, L.: Surge fault detection of aeroengines based on fusion neural network. *Intell. Autom. Soft Comput.* **29**(3) (2021)

14. Zheng, D., Ran, Z., Liu, Z., Li, L., Tian, L.: An efficient bar code image recognition algorithm for sorting system. *Comput. Mater. Continua* **64**(3) (2020)
15. Kamilaris, A., Prenafeta-Boldú, F.X.: Deep learning in agriculture: a survey. *Comput. Electron. Agric.* **147**, 70–90 (2018)
16. Patel, M., Jernigan, S., Richardson, R., Ferguson, S., Buckner, G.: Autonomous robotics for identification and management of invasive aquatic plant species. *Appl. Sci.* **9**(12), 2410 (2019)
17. Waisman, A., La Greca, A., Möbbs, A.M., Scaraffia, M.A., Velazque, N.L.S., Neiman, G., Moro, L.N., Luzzani, C., Sevlever, G.E., Guberman, A.S., et al.: Deep learning neural networks highly predict very early onset of pluripotent stem cell differentiation. *Stem Cell Rep.* **12**(4), 845–859 (2019)
18. Xie, T., Yamana, H., Mori, T.: Che: channel-wise homomorphic encryption for ciphertext inference in convolutional neural network. *IEEE Access* **10**, 107,446–107,458 (2022)
19. Phan, N., Wu, X., Dou, D.: Preserving differential privacy in convolutional deep belief networks. *Mach. Learn.* **106**(9–10), 1681–1704 (2017)
20. Huang, K., Liu, X., Fu, S., Guo, D., Xu, M.: A lightweight privacy-preserving cnn feature extraction framework for mobile sensing. *IEEE Trans. Dependable Secure Comput.* **18**(3), 1441–1455 (2019)
21. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., Wang, C.: Machine learning and deep learning methods for cybersecurity. *IEEE Access* **6**, 35365–35381 (2018)
22. Gupta, O., Raskar, R.: Distributed learning of deep neural network over multiple agents. *J. Netw. Comput. Appl.* **116**, 1–8 (2018)
23. Zeng, Y., Gu, H., Wei, W., Guo, Y.: *deep – full – range*: a deep learning based network encrypted traffic classification and intrusion detection framework. *IEEE Access* **7**, 45182–45190 (2019)
24. Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., Lloret, J.: Network traffic classifier with convolutional and recurrent neural networks for internet of things. *IEEE Access* **5**, 18042–18050 (2017)
25. Song, C., Shi, X.: Secure deep learning on genomics data via a homomorphic encrypted residue activation network. *bioRxiv* pp. 2023–01 (2023)
26. Lee, J.W., Kang, H., Lee, Y., Choi, W., Eom, J., Deryabin, M., Lee, E., Lee, J., Yoo, D., Kim, Y.S., No, J.S.: Privacy-preserving machine learning with fully homomorphic encryption for deep neural network. *IEEE Access* **10**, 30039–30054 (2022). <https://doi.org/10.1109/ACCESS.2022.3159694>



# An Efficient Data Reduction Method for DAG Blockchain

Chengyao Zhang and Dongyan Huang<sup>(✉)</sup>

Ministry of Education Key Lab. of Cognitive Radio and Information Processing, University of Electronic Technology, Guilin 541004, Guangxi, China  
huangdongyan-gua@163.com

**Abstract.** Compared with the traditional blockchain, the blockchain system based on directed acyclic graph (DAG) has higher throughput and greater storage pressure, and there is also redundancy of transaction data in the block, which is caused by concurrent block sending, that is, the same transaction may appear in different blocks, and different blocks are attached to the DAG at the same time, which aggravates the storage pressure. In this paper, to solve the above problems, we propose a method that can reduce data twice. The first data reduction is aimed at the redundancy in the block, which is in the blockchain system based on DAG. And the second data reduction is based on the user's experience and the first basis. The experimental results show that the proposed method can save 92.18% of the storage space and effectively alleviate the storage pressure.

**Keywords:** Blockchain · Directed acyclic graph · Data reduction

## 1 Introduction

Since the Blockchain Was Proposed in 2008, It Has Attracted Worldwide Attention for Its Advantages of Decentralization, Tamper-Proof, Traceability and Transparency. The Traditional Blockchain Has Only One Single Chain, and the Packaged Blocks Cannot Be Executed Concurrently. These Traditional Blockchain Applications Include Bitcoin [1], Ethereum [2], Hyperledger Fabric [3] and so on. At Present, the Transactions Per Second (TPS) of the Traditional Blockchain with Single-Chain Structure Cannot Meet the Actual Needs of Reality. To Improve the TPS of Traditional Blockchain, a Mesh Topology of DAG Comes into View. Its Specific Idea is to Change the Chain Storage Structure of the Block and Change the Single Chain Structure into the Network Topology of DAG, so that Concurrent Writing Can Be Realized, and the Transaction Confirmation Speed and TPS Can Be Improved. As a Result, DAG Blockchain Technology Began to Develop Rapidly.

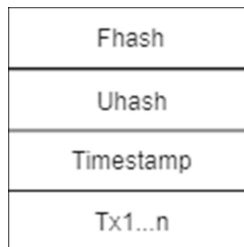
Supported by the Guangxi NSF Project under Grant 2022GXNSFBA035645; by the Guangxi Key Research and Development Program under Grant AB20238026; by the Chinese NSF Project under Grant 6217070229; by the Director Fund of Key Laboratory of Cognitive Radio and Information Processing, Ministry of Education (Guilin University of Electronic Technology) under Grant CRKL210104; and by the Innovation Project of GUET Graduate Education under Grant 2022YCXSO52.

On the one hand, the security of the blockchain is obtained by cryptography, on the other hand, it is obtained by redundant storage. By using the distributed consensus algorithm, the blockchain nodes agree on the stored data, and finally each node stores the same data. This combination of redundant storage and secure password hash algorithm and Merkle tree makes the data in the tampered blockchain must exceed 50% of the computing power of the node pool, ensuring the security of the blockchain. However, redundant storage will lead to a rapid increase in data storage on the blockchain as the volume of transactions increases. As the earliest blockchain application Bitcoin, the data on the chain has exceeded 370 GB. The newly generated data needs about 50GB to store every year. What's worse, the size of data storage is proportional to the performance of the blockchain system, that is, the transaction volume per second TPS [4]. It is foreseeable that the data storage pressure of the DAG-based blockchain system will be greater.

To solve the problem of increasing storage capacity of the blockchain system, Nakamoto [1], the founder of Bitcoin, proposed a method to redesign the blockchain system protocol based on the trust assumption. The core idea of this method is to divide the nodes in the blockchain system into light nodes and full nodes. The full node grasps all the information of the block and performs transaction verification. The light node only needs to store the block header, thereby reducing the storage cost. But, light nodes must trust other full nodes. Once the full node fails to respond to data requests in a timely manner, system failure, malicious attacks, etc., it may bring the risk of permanent data loss. At this time, the data related to the light node stored by the whole node is most likely not available later. Although this method has risks, it is more effective in practical applications and has its targeted design in various scenarios.

In the DAG-based blockchain, especially the blockchain with the block as the DAG vertex, the design of the light node and the full node is still effective, but the redundancy within the block may be more serious. The reason is that the blockchain system based on DAG is highly concurrent, that is, there can be multiple nodes out of the block at the same time point. The same transaction may appear in different blocks, and different blocks are attached to the DAG at the same time, which in turn aggravates the storage pressure.

In practical applications, especially in the Internet of Things (IoT) scenario [5], the storage capacity of blockchain nodes is limited, and it is impractical to store all blockchain data. The users behind these nodes may only care about the transaction data related to themselves, and have no obligation to save other transaction data.



**Fig. 1.** DAG block structure.



In our previous work [6], we proposed a blockchain system based on DAG, but there was a problem of redundant transaction data in the block when the block was issued. When storing blocks, the block header only accounts for a small part of the block, and the block size mainly depends on the complete transaction data in the block. Figure 1 is the block structure of Directed Acyclic Blockchain Graph (DABG) [6].  $T \times 1 \dots n$  represents  $n$  transaction data. And Fhash and Uhash are the unique block connection pointers in [6]. When the number of transaction data cached by each node reaches a certain amount, it will be packaged into blocks. Therefore, it is very likely that the same transaction will appear in multiple nodes packaged blocks. Based on the actual application scenarios and the storage defects of DABG, we believe that not every user of the maintenance node is willing to pay an extra price to save transaction data which is not related to themselves. At the same time, we also consider that the optimization of the system should retain its original attributes, such as decentralization and non-tampering. Therefore, we propose a data reduction method that can be performed twice to optimize the storage problem of [6]. Our main contributions are as follows:

- A new data reduction method is proposed based on the block redundancy defect of DABG and the user experience.
- The advantages and disadvantages of this data reduction method on the basis of retaining the original attributes of DAG-based blockchain are described in detail.
- The proposed method is verified by experiments, and the experimental results prove its feasibility and efficiency.

The experimental results show that the proposed data reduction method can save 92.18% of the storage space while maintaining the normal operation of the system.

The remainder of this paper is organized as follows. Section 2 summarizes the related work. Section 3 introduces the system model. Section 4 gives the evaluation results of the data reduction method and the setting of the experimental parameters. Sections 5 and 6 give conclusions and future work.

## 2 Related Work

The new blockchain system with directed acyclic graph (DAG) structure takes transactions or blocks as vertices, and the vertices are still connected by hash pointers to maintain the traceability and non-tampering characteristics of the blockchain. The graph structure allows the system to generate blocks in parallel. Therefore, the performance of blockchain (such as TPS) is greatly improved. Table 1 shows the TPS of traditional blockchain technology and DAG based blockchain technology. Table 2 reflects the relationship between TPS and storage cost. The larger is TPS, the larger is storage cost. Therefore, whether a traditional blockchain system or a new DAG-based blockchain system, they all have storage pressure. Some works have done to reduce the data storage pressure of blockchain systems. Xu et al. [7] tried to form multiple consensus units by grouping nodes, each aggregation point in a consensus unit only need to store a part of the entire blockchain data. However, their method is based on the strong trust assumption between nodes in the consensus unit. This is difficult to apply in DABG systems dedicated to applications in IoT environments. Dai et al. [8] proposed a data reduction

method similar to puzzles. Each node only stores data related to itself, and uses Merkle path to verify the authenticity of the transaction. Jia et al. [9] proposed a repeated proportion mechanism to store different blocks in different proportions to achieve lower storage costs. In addition, there are attempts to eliminate data duplication at the storage engine layer. Forkbase [10], proposed by Wang et al., aims to improve storage performance while reducing storage size. With the help of fast-based deduplication, Forkbase successfully deleted large file duplicates containing a large amount of public content. However, in the blockchain scenario, the repetition rate of transactions and blocks stored by nodes is usually low, so the effect is not ideal.

**Table 1.** TPS of DAG based blockchain technology and traditional blockchain technology.

Blockchain technology classification	Blockchain technology	TPS
DAG blockchain	IOTA	100
	NANO	1000
	Conflux	3000
	Hashgraph	10000
Traditional blockchain	Bitcoin	7
	Ethereum	15
	Hyperledger fabric	3000

**Table 2.** Increase of storage cost as TPS increases.

TPS	7	100	1000
Data(GB/Year)	50	750	7500

All of the above are optimized for the traditional blockchain system, and some work has given optimization schemes for the DAG-based blockchain system. Such as Yang et al. [11] proposed a blockchain LDV based on lightweight directed acyclic graph, and proposed a social-based data reduction method. In LDV, each node only stores the data of interest in the subject group of interest, while ignoring the data that is not interested. To avoid huge storage costs in large groups with large amounts of data, [11] further proposed a method of pruning historical data within the group to meet storage requirements by reducing the number of duplicate data stored in each node. Fu et al. [12] proposed an efficient consensus algorithm Teegraph for IoT, which mainly includes a message communication mechanism based on the Gossip protocol to generate DAG-based data structures for efficient consensus processes. When there are no new transactions, Teegraph can reduce communication overhead and save storage space. There are also some schemes that indirectly reduce storage pressure, such as Li et al. [6] proposed an efficient DAG blockchain architecture for IoT. The use of federated learning to optimize the propagation mode of the Gossip protocol reduces the redundancy of the Gossip protocol and indirectly alleviates some of the storage pressure.

Compared with the above work, our work is a continuation of the paper “An Efficient DAG Blockchain Architecture for IoT [6]”. Optimize the shortcomings of DABG in terms of storage, and propose a user-based data reduction method, that is, each node only packages transactions initiated by itself and transactions related to itself when sending blocks, reducing storage pressure.

### 3 System Model

In this section, we will show our method. In addition, our design is optimized for DABG, so we will give a brief introduction to DABG.

#### 3.1 DABG Introduction

The architecture of DABG can be divided into two parts, one for building a Gossip network based on federated learning, and the other for reaching consensus. Initially, nodes use the original Gossip protocol to propagate transactions and conduct virtual voting through signatures. The submitted transactions are packaged into blocks and synchronized to other nodes through the Gossip protocol to maintain consistency between nodes. At the same time, the node will store some relevant data of federated learning locally as samples. When the sample reaches a certain number, the federated learning is used to construct the tree Gossip network, and the tree Gossip protocol is used to consensus. Finally, the weight-based block selection algorithm is used to attach the block to the DAG.

The design of DABG refers to a part of hashgraph, which belongs to parallel chain DAG, but still retains the concept of block. When a node receives a certain number of submitted transactions, it will initiate a block out operation. Each node can send out blocks at the same time, so there is no small redundancy in the DAG formed by taking blocks as vertices.

#### 3.2 Data Reduction

As shown in Fig. 2, each node first submits the completed strongly visible transaction (that is, it has been confirmed by more than  $2/3$  of the total nodes). Then, each node caches the transaction data from other nodes and the transaction data initiated by itself locally and marks the transaction data with correlation. For example,  $T \times 1$  ( $NO-NI$ ) of  $NO$  node is the transaction data of  $NO$  node and  $NI$  node. When each node caches a certain amount of transaction data, it enters the next stage and extracts the transaction data related to itself from the cache by marking. Finally, generate blocks for broadcast synchronization.

It is worth noting that the out-of-block time of each node is not necessarily the same, depending on the time it takes for each node to cache a specified amount of transaction data and perform data reduction. After block synchronization, the block is attached to the DAG by a weight-based block selection algorithm.

As shown in Fig. 3, this is the DAG global graph formed by the blocks in  $NO$  nodes according to the weight-based block selection algorithm in DABG. If each node stores

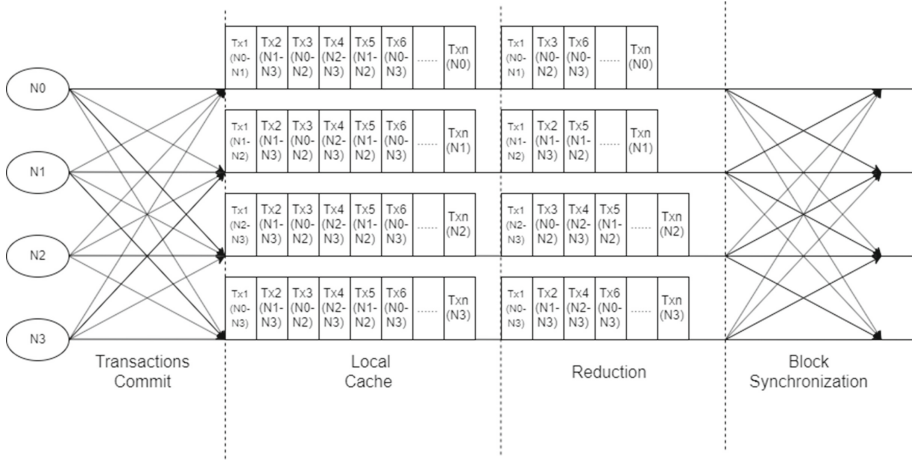


Fig. 2. Data reduction flow diagram.

all the data, the storage capacity of the device needs to be very high. And it is not in line with the interests of users who maintain their own nodes. Therefore, a secondary reduction is taken from the perspective of the correlation between the data and the user. Taking the  $N0$  node as an example, the black block represents that the  $N0$  node stores all the data completely when it is stored, and the white block indicates that the  $N0$  node only symbolically stores the block header when storing the blocks synchronized by other nodes. The second reduction also needs to set the whole node, that is, the node that stores all the data, so as to ensure that the user can still obtain the transaction information through the whole node under some bad conditions such as attack or downtime. But it also introduces the problem of third-party credibility that needs to be solved.

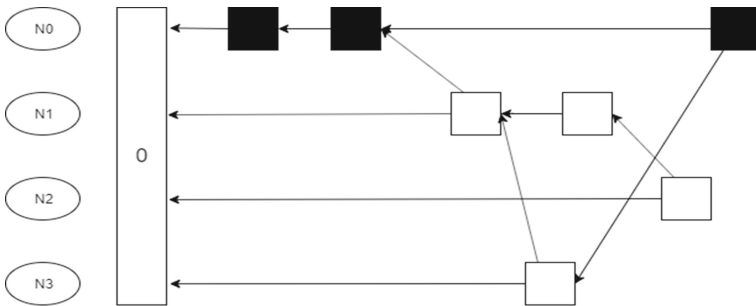


Fig. 3. DAG graph of N0 node.

### 3.3 Stability

When the node is in the cache transaction but has not yet completed the block, the downtime node only needs to issue a request like other nodes when restarting, and

performs block synchronization operation, but does not perform secondary reduction, that is, synchronizes the complete blocks of all nodes during the downtime until the synchronization is completed, and then re-opens the secondary reduction. As for the unpackaged transactions before the downtime, they exist in the complete blocks synchronized by other nodes. If multiple nodes are down at the same time, it is necessary to request the whole node at restart to complete block synchronization. As for the number of full node settings, it is related to the user's financial budget.

## 4 Performance Evaluation

In this section, we will evaluate the changes in storage performance brought by the proposed data reduction method in the DABG system through simulation.

### 4.1 Experimental Setup

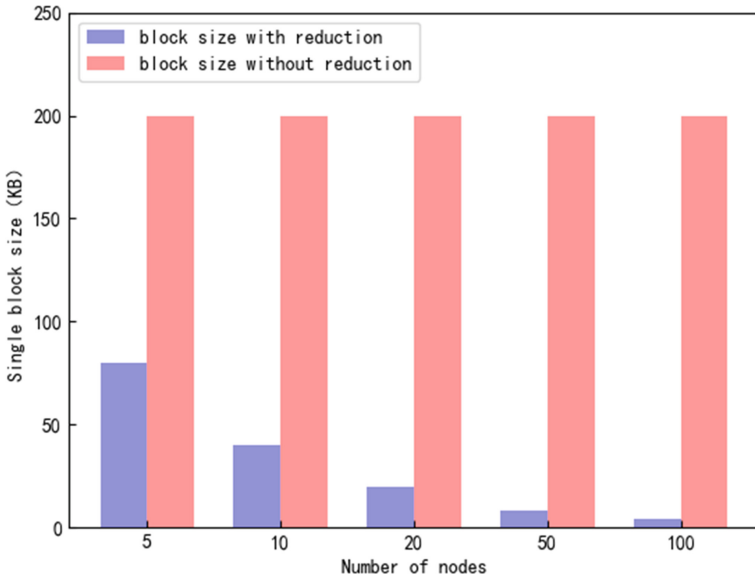
We simulate a DABG system in a multi-threaded manner. The experimental hardware uses Intel (R) Core (TM) i7-10870H CPU @ 2.20 GHz  $\times$  5 virtual host, 16GB DDR4 memory, based on Ubuntu 20.04 operating system. The software uses Golang 1.19.3 linux/amd64 development environment. To ensure the consistency of storage of different nodes, the data size within all transactions is set to the same. At the same time, we set the node to start the first data reduction for every 1000 transactions cached.

### 4.2 The Effect of the First Data Reduction

We first evaluate the method of the first data reduction. The node filters 1000 transactions per cache, and filters out the transaction data related to itself by identifying the correlation markers on the transaction data. We study the impact of the number of nodes on the size of a single block of data when each node in the network randomly initiates a total of 1000 transactions. As shown in Fig. 4, if the block packaging method of the original DABG system is used, the node packages 1000 transactions as blocks. In the case of block heads being ignored, the storage cost of the block has reached 200 KB. From the experimental results, it can be seen that when the number of nodes is more, the method of screening out the transaction data related to itself and packing out the block is better. When 100 nodes randomly initiate 1000 transactions in the network, the average block size of the nodes is only 4 KB. This is beneficial to the resource-constrained IoT environment.

### 4.3 The Effect of the Second Data Reduction

The second reduction is to consider that each node needs to store global data when participating in consensus. Considering that this situation is not in line with the user's experience and interests, each node only stores the block header of the block packaged by its own node and the block synchronized by other nodes. As shown in Table 3, the experiment is set to 5 nodes, of which N4 is the full node. The full node needs to have a global view and store all the blocks in the DAG graph. To facilitate comparison, we set up a network in which only N4 initiates transactions to the other four nodes.

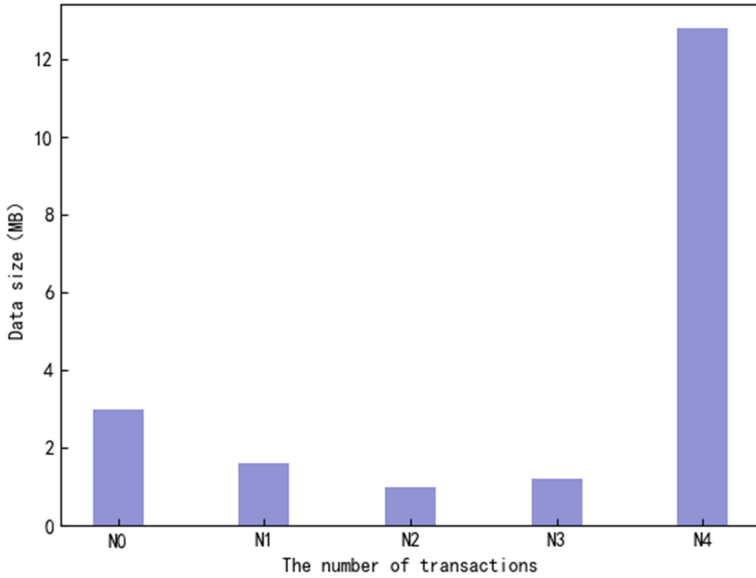


**Fig. 4.** The influence of the number of nodes on the size of a single block data.

**Table 3.** The number of related transactions received by per node.

Total transactions	30000				
Node id	N0	N1	N2	N3	N4
Txs related to per Node	15000	8000	5000	6000	30000

As shown in Fig. 5, ignoring the small storage cost generated by the block header, compared with the full node *N4*, other nodes only store their own packaged blocks when the storage cost is lower. Node *N2* consumes the least storage space, because among the 30,000 transactions randomly initiated by *N4*, the transactions related to *N2* are the least. Specifically, compared with the full-node *N4*, it saves 92.18% of storage space. This confirms the efficiency of the second reduction method.



**Fig. 5.** The storage cost of each node.

## 5 Conclusion

In this paper, we propose a method that can reduce the data twice for the DABG system proposed in the previous work to reduce the storage cost. Specifically, the first data reduction is proposed for the problem that the DABG parallel out of the block leads to excessive data redundancy in the block. The second data reduction is based on the experience and interests of the user maintenance node, which effectively reduces the storage cost of the DABG system. To ensure the stability of the network, we further propose related mechanisms in the design. The effect of data reduction has been evaluated by simulating the DABG system. Experimental results show that the proposed method can save 92.18% of storage space.

## 6 Future Work

In the future work, we will evaluate the effect of this method on data query. This is not mentioned in this work. In addition, we will continue our previous work to improve other aspects of the DABG system and further improve the performance of the blockchain.

## References

1. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cashsystem[EB/OL]. <https://bitcoin.org/en/bitcoinpaper>. Accessed 20 Feb. 2022
2. Wood, G.: Ethereum: a secure decentralised generalized transaction ledger[EB/OL]. <http://gavwood.com/Paper.pdf>. Accessed 20 Feb. 2022

3. Androulaki, E., Barger, A., Bortnikov, V. et al.: Hyperledger fabric: a distributed operating system for permissioned blockchains[C]. In: Proceedings of EuroSys'18, pp. 1–15. IEEE Press, Washington D.C., USA (2018)
4. Gray, J., Helland, P., O'Neil, P., Shasha, D.: The dangers of replication and a solution. *ACM SIGMOD Rec.* **25**(2), 173–182 (1996)
5. Dai, H.-N., Zheng, Z., Zhang, Y.: Blockchain for internet of things: a survey. *IEEE Internet Things J.* **6**(5), 8076–8094 (2019)
6. Li, L., Huang, D., Zhang, C.: An efficient DAG blockchain architecture for IoT[J]. *IEEE Internet Things J.* **10**(2), 1286–1296 (2022)
7. Xu, Z., Han, S., Chen, L.: Cub, a consensus unit-based storage scheme for blockchain system. In: Proceedings of the IEEE 34th International Conference Data Engineering, pp. 173–184 (2018)
8. Dai, X., Xiao, J., Yang, W., Wang, C., Jin, H.: Jidar: a jigsaw-like data reduction approach without trust assumptions for bitcoin system. In: Proceedings of IEEE 39th International Conference on Distributed Computing System, pp. 1317–1326 (2019)
9. Jia, D., Xin, J., Wang, Z., Guo, W., Wang, G.: Elasticchain: Support very large blockchain by reducing data redundancy. In: Proceedings of Asia-Pacific Web Web-Age Information Management Joint International Conference on Web Big Data, pp. 440–454 (2018)
10. Wang, S., Dinh, T.T.A., Lin, Q., Xie, Z., Zhang, M., Cai, Q., Cnhen, G., Ooi, B.C., Ruan, P.: Forkbase: an efficient storage engine for blockchain and forkable applications. In: Proceedings of the VLDB Endowment. VLDB Endowment, pp. 1137–1150 (2018)
11. Yang, W.H., Dai, X.H., Xiao, J., et al.: LDV: a lightweight DAG-based blockchain for vehicular social networks [J]. *IEEE Trans. Veh. Technol.* **69**(6), 5749–5759 (2020)
12. Fu, X., Wang, H.M., Shi, P.C., et al.: Teegraph: trusted execution environment and directed acyclic graph-based consensus algorithm for IoT blockchains [J]. *Sci. China Inf. Sci.* **65**(3), 1–3 (2021)





# A Compact Dual-Band Directional Button Antenna Based on Metamaterial Lens for New Power Services

Wenge Wang, Jizhao Lu, Yongjie Li, Huanpeng Hou<sup>(✉)</sup>, and Dongjiao Xu

State Grid Henan Electric Power Company Information and Communication Branch,  
Zhengzhou, China  
675575808@qq.com

**Abstract.** A compact dual-band directional button antenna is proposed for miniaturized equipment and tight space in integrated power communication networks. In this design, a metamaterial lens consisting of  $2 \times 2$  cells is applied to the radiation direction, enabling a compact and directional configuration. The antenna consists of a microstrip line feed, a monopole loaded by the dielectrics, and a metamaterial lens placed on the other side of the feed. The metamaterial unit cell has two different split resonant rings responsible for two different resonances, and the  $2 \times 2$  cells are employed to form the desired lens and are symmetrical on the monopole. The results show that the antenna with lens has the similar properties with that of the reflector metamaterial.

**Keywords:** Dual-band directional button antenna · Integrated power communication network · Metamaterial lens

## 1 Introduction

With the development of power systems and 5G technologies, the grid networking tends to integrated networks for differentiated services. Smart grids [1] can utilize advanced communications, control, and information technologies to optimize power system operations in 4G/5G networks. There are a lot of power equipment and terminals on the smart grid, which need to be monitored [2, 3]. In addition, power equipment needs to communicate with each other and transfer data [4]. Antennas are necessary for these purposes, and miniaturized antennas are one of the good candidates for deploying in power pipes and porches.

Button antenna was first proposed in [5], which has the characteristics of miniature and with flexible substrate but stable performance. It is a big advantage in new grid applications, for example, deployment in power pipes and porches. Because of the utilization of flexible substrates, the button antennas can be conformal integrated into power grid equipment to monitor the running state and performance of the power system. Moreover,

button antennas can also be used as part of a new grid communication network, allowing devices to exchange information and share data in real time.

In order to satisfy both monitoring and communication modes, a dual-band dual-mode button antenna is designed in this paper. Therefore, by using near-field resonant coupling technology [6], two resonant loops of loaded metamaterial are excited by monopole radiation so that the antenna can obtain dual-band characteristics. The pattern of omnidirectional radiation of the lower band can be used to monitor the surrounding electrical equipment. At the upper band, the directional radiation enables point-to-point communication at high rates between two devices.

## 2 Button Antenna Design

The button antenna consists of a microstrip line feed, a monopole loaded with top and bottom dielectrics, and a metamaterial lens placed on the other side of feeding line, which is away from the microstrip. The overall configuration of the proposed antenna is shown in Fig. 1, where (a), (b), (c), and (d) correspond to 3D, side view, top view, and front view, respectively. The microstrip is taken as the feed to excite the button antenna. The flexible material with dielectric constant  $\varepsilon = 1.6$  and loss tangent  $\tan \delta = 0.02$  as substrate, which can be perfectly conformal to the device. The thickness of the substrate is 1.5 mm.

The proposed button antenna uses a monopole as a radiator and loads circular dielectrics on its top and bottom. The monopole can be inserted into the circular dielectric at the bottom so that the monopole antenna is more stable and the radiation performance is less affected. The top and bottom dielectrics are loaded with the same radius and the same dielectric with thickness of 1 mm, both TP1020, dielectric constant  $\varepsilon$  and loss tangent  $\tan \delta$  are 10.2 and 0.0015, respectively.

A split-ring resonator is proposed in [7]. Based on this structure, the unit structure is modified in this paper, as shown in Fig. 2a. The magnitudes of S-parameters in which resonance in two bands are obtained, as shown in Fig. 3. The near-field radiation properties of the monopole result in different wave paths of the electromagnetic wave to each position of the metamaterial structure, and they are arranged symmetrically on the longitudinal direction. The structure of  $2 \times 2$  unit cells is shown in Fig. 2b. The designed metamaterial structure is loaded onto the button antenna and placed away from the microstrip line. This arrangement reduces the effect of microstrip lines on antenna radiation. The height of the metamaterial structure basically determines the profile of the button antenna. Therefore, the monopole is loaded with a dielectric cylinder with FR4 material, and the dielectric constant and loss tangent are 4.4 and 0.025, respectively. By adjusting the height of the cylinder and the monopole, the impedance can be changed and good matching is achieved.

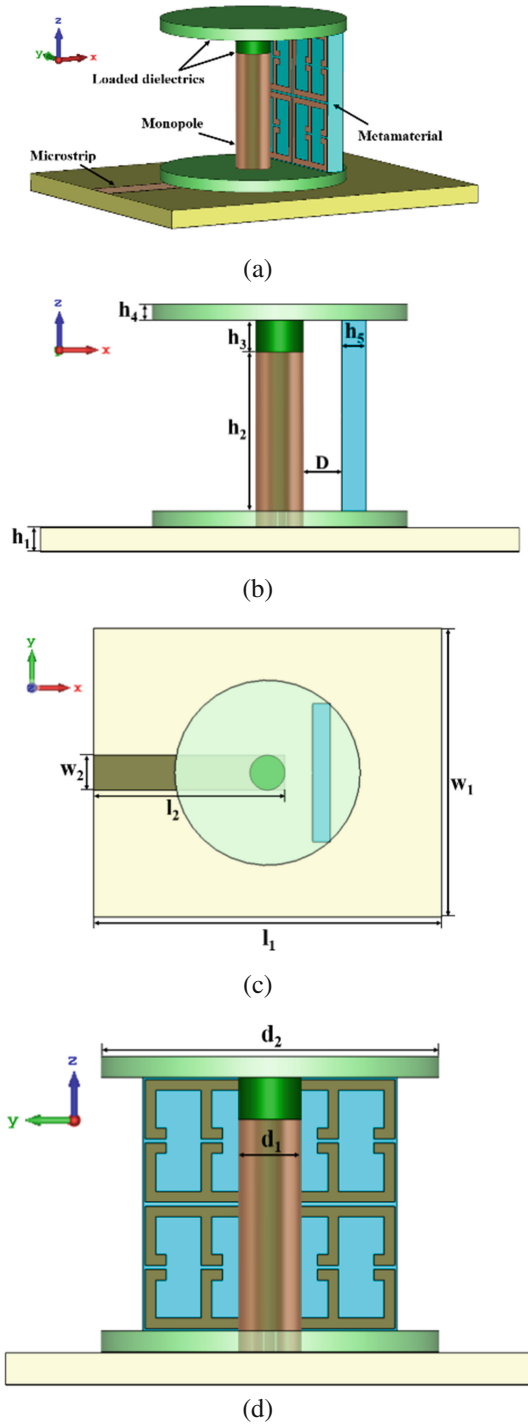
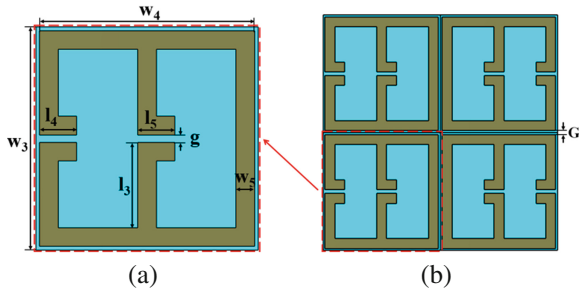
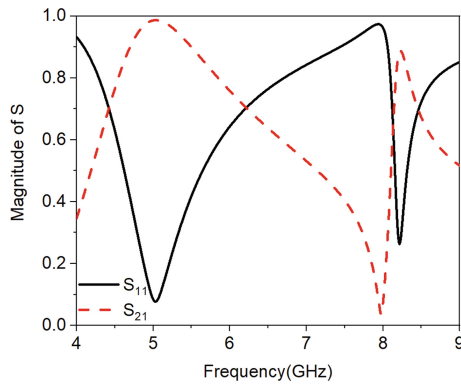


Fig. 1. Antenna construction, **a** the 3-D view, **b** the side view, **c** the top view, and **d** the front view.



**Fig. 2.** Configurations of metamaterial structure, **a** unit cell and **b**  $2 \times 2$  cells.

After careful adjustment of the above parameters of the metamaterial structure and the monopole antenna, the optimization results are shown in Table 1.



**Fig. 3.** Magnitude of S-parameter for the unit cell.

**Table 1.** The optimized values of parameters.

Parameters	$w_1$	$w_2$	$w_3$	$w_4$	$w_5$	$l_1$	$l_2$	$l_3$	$l_4$	$g$
Values (mm)	25	3	6	5.9	0.5	30	16.5	1	1.05	0.2
Parameters	$h_1$	$h_2$	$h_3$	$h_4$	$h_5$	$d_1$	$d_2$	$D$	$G$	
Values (mm)	1.5	11	1	1	1.5	3	16	2.9	0.1	

### 3 Result Analysis

#### 3.1 Parametric Analysis

In order to obtain the final optimization result of the button antenna, the influence of the parameters on the dual-band in the reflection coefficient should be considered. Thus, the corresponding effects are discussed below, where only one parameter changes during the process while the others remain constant.

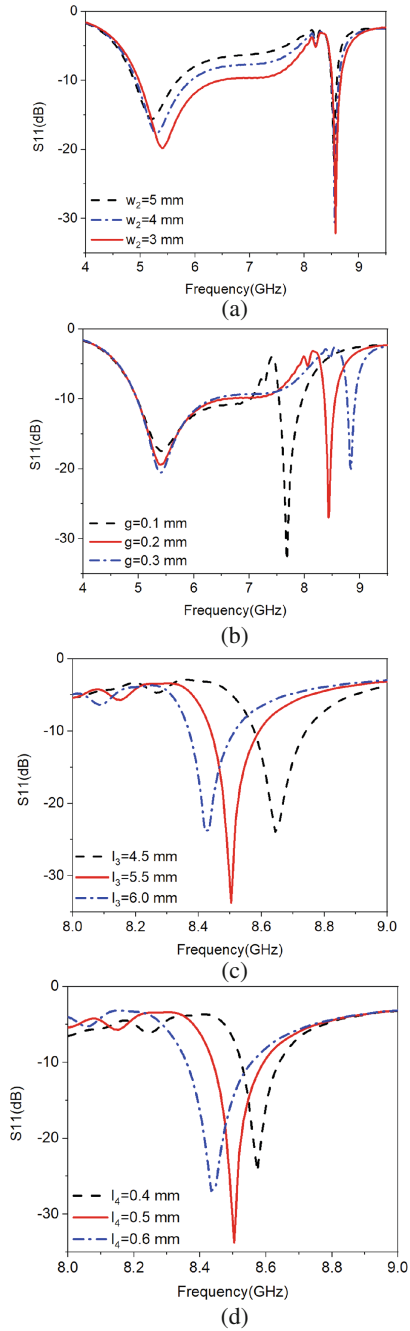
Both the monopole and the metamaterial structure should be considered in the parameter analysis. Firstly, the influence of microstrip feed in monopole on reflection coefficient is discussed, as shown in Fig. 4a. It can be seen that the width of the microstrip  $w_2$  directly affects the resonance and matching of the lower band, indicating that the lower band is more affected by the monopole, but the upper band has almost no effect. Then three variables of metamaterial structure are used to analyze their effects on resonance and matching. They are the gap width  $g$ , lengths  $l_3$  and  $l_4$  of the split-ring resonator, respectively. The corresponding results are shown in Fig. 4b–d, respectively. As we see, the three parameters are related to resonance, which is consistent with the theory of metamaterials. Among them,  $g$  slightly affects the matching of the lower band, but greatly influences the frequency points of the upper band. At the upper band, it is more sensitive to the capacitance of resonance. The increase in gap leads to the reduction of capacitance, so the resonant frequency point moves upward. When  $l_3$  and  $l_4$  are changed, the lower band is almost unaffected, so only the upper band is shown. The longer length leads to higher inductance thus lower resonance point.

#### 3.2 Surface Current

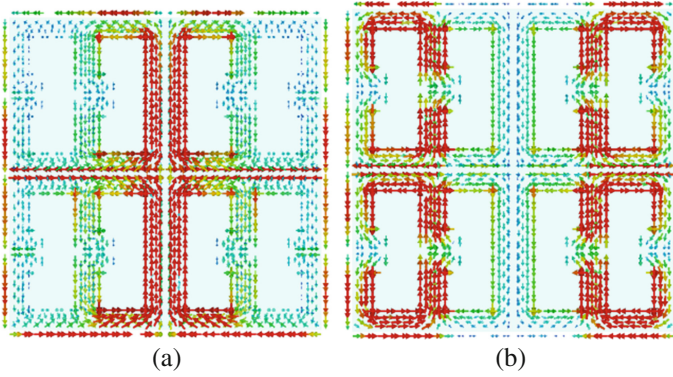
Through the near-field resonant coupling of the monopole, the metamaterial generates two different resonant loops in different bands. In order to reveal the influence of metamaterial structure parameters on the reflection coefficient more directly, the current distribution on metamaterial structure is shown. The low-frequency current is distributed in the middle resonant loop as shown in Fig. 5a, so it is not sensitive to the changes of  $l_3$  and  $l_4$  mentioned above. For the current distribution in the upper band as shown in Fig. 5b, the current is mainly concentrated in the gap part, so it is very sensitive to the changes of  $g$ ,  $l_3$  and  $l_4$ . Therefore, the resonant properties of the antenna can be observed by the change of the current distribution on the metamaterial.

#### 3.3 Radiation Pattern

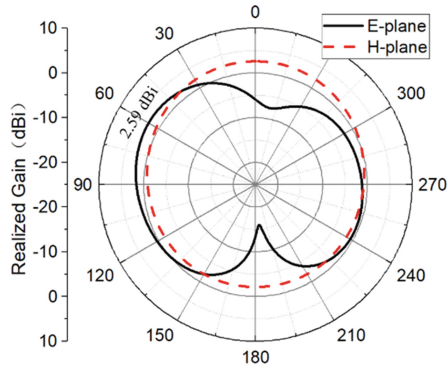
In order to meet the requirements of the application, the radiation pattern needs to present two different modes. Figure 6a shows the radiation of the antenna at the lower band, which can cover the surrounding equipment in a large range. At the upper band, the directional beam results in significant radiation enhancement on the side of the metamaterial loading, as shown in Fig. 6b. It is a huge advantage for point-to-point high-speed data transmission. In addition, the beam at both bands appears to tilt upward, which is due to the asymmetry of the microstrip line and the influence of the finite metal ground.



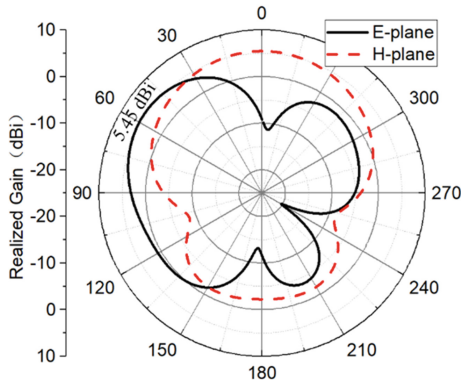
**Fig. 4.** Parametric analyses of antennas, **a** unit cell, and **b**  $2 \times 2$  cells.



**Fig. 5.** Surface current at **a** 5.4 GHz and **b** 8.5 GHz.



(a)



(b)

**Fig. 6.** Radiation pattern at, **a** 5.4, and **b** 8.5 GHz.

## 4 Conclusion

In this paper, a dual-band antenna based on metamaterial was proposed for miniaturized equipment and tight space in integrated power communication networks. This antenna consists of a microstrip line feed, the metamaterial lens, and the top and bottom loaded monopole antenna. By carefully adjusting the corresponding parameters of the antenna, the good dual-band characteristics of the final optimization were obtained, and the corresponding parameters were analyzed.

**Acknowledgment.** This work is supported by State Grid Henan Electric Power Company Science and Technology Project (No. SGHAXT00GCJS2250197).

## References

1. Fang, X., Misra, S., Xue, G., Yang, D.: Smart grid—the new and improved power grid: a survey (Review)[J]. *IEEE Commun. Surv. Tutor.* **14**(4), 944–980 (2012)
2. Wang, P., Hou, H., He, X.: Survey on application of wireless sensor network in smart grid[J]. *Procedia Comput. Sci.* **52**, 1212–1217 (2015)
3. Jha, A.V., Appasani, B., Ghazali, A.N., Pattanayak, P.: Smart grid cyber-physical systems: communication technologies, standards and challenges[J]. *Wirel. Netw.* **27**(4), 2595–2613 (2013)
4. Gungor, C., Sahin, D., Kocak, T., Ergut, S.: A survey on smart grid potential applications and communication requirements[J]. *IEEE Trans. Industr. Inf.* **9**(1), 28–42 (2013)
5. Sanz-Izquierdo, B., Miller, J.A., Batchelor, J.C., Sobhy, M.I.: Dual-band wearable metallic button antennas and transmission in body area networks. *IET Microwaves Antennas Propag.* **4**, 182–190 (2010)
6. Jin, P., Ziolkowski, R.W.: Metamaterial-Inspired, Electrically Small Huygens Sources. *IEEE Antennas Wirel. Propag. Lett.* **9**, 501–505 (2010)
7. Pendry, J.B., Holden, A.J., Robbins, D.J., Stewart, W.J.: Magnetism from conductors and enhanced nonlinear phenomena. *IEEE Trans. Microw. Theory Tech.* **47**, 2075–2084 (1999)





# Energy Efficiency Maximization for RIS-Aided Multi-user MISO Systems in Integrated Power Communication Networks

Yuqing Feng, Yalin Chen, Yutong Ji<sup>(✉)</sup>, Cong Zhu, and Yu Tian

State Grid Jibei Electric Power Co, Ltd. Information and Communication Branch, Beijing, China  
lunwenshenqing2023@163.com

**Abstract.** Recently, the integrated power communication network has gained considerable attention, because of new differentiated business. To improve the energy efficiency (EE) for information acquisition services, reconfigurable intelligent surface (RIS) is proposed. Under the constraints of the minimum rate of each user, the maximum transmit power limit of the base station and the unit modulus constraint of the phase angle of RIS, this paper aims for maximizing EE in RIS-aided multiple-input-single-output (MISO) systems. Firstly, the maximum signal-to-interference-noise ratio (SINR), the total power consumption of the system and the phase matrix of RIS are analyzed and derived, and then the optimization problem is established with the beamforming and transmission power of the base station transmitting multi-user as variables. Thirdly, in order to solve the optimization problem, this paper proposes to use the maximum ratio to send pre-coding to maximize the SINR received by users, and uses an improved sine and cosine optimization algorithm to optimize the phase matrix of RIS. Finally, a scheme of alternating iterative optimization of phase matrix and power is designed. Simulation results show that the proposed algorithm is very effective in improving the energy efficiency of the system. Compared with the traditional relay amplification scheme, the improved SCA optimization scheme achieves about 30% improvement in energy efficiency, which confirms the feasibility of the proposed method in improving the energy efficiency of MISO system.

**Keywords:** Integrated power communication network · Energy efficiency · Reconfigurable intelligent surface · Beamforming · Sine and cosine optimization algorithm

## 1 Introduction

Integrated power communication networks represent this will bring very new prospects and will greatly promote the construction of the digital economy, making smart cities more reliable, convenient and fast. Integrated power communication networks aim to develop an integrated infrastructure and differentiated services for the new smart grid. Great progress has been made in 5G wireless communication networks, and when its commercialization is in progress, 6G wireless networks are increasingly attracting the

attention of academic world. These fields tend to make demand more requirements for data transfer capability, reliability, latency and energy efficiency (EE) [1]. Especially in 6G wireless communication networks, electrical communication is crucial because various terminal intensive tasks are on the rise and the lowering of resource wastage resulting from communication technology is irreplaceable. The existing 5G technologies, such as millimeter wave communication, heterogeneous networks with large-scale access and ultra-high density are mainly studied in the design of transmitting and receiving systems, in order to deal with information acquisition services. But these technologies also have huge implementation costs and huge energy consumption. In recent years, the report calls reconfigurable intelligent surface (RIS) as intelligent reflector. Because its ability to configure wireless communication environment, it has become a popular new technology. It can skillfully adjust the reflection coefficient of the reflection element through the programmable controller, so that the reflected signal can be propagated to the expected receiver in the desired way, making the wireless environment controllable and programmable [2]. Compared with the existing amplifying and forwarding relay auxiliary communication, RIS is a more energy-saving and economical technology.

At present, RIS technology has been widely studied and concerned in respect of communication. Over the past few years, the research literature on RIS also emerges one after another. In the fields of theoretical research and application scenarios, there has been a lot of research work on RIS. For example, [3] constructed the antenna design, model design and verification results of RIS. In [4], an overview of RIS technology and its use in common wireless communications was given. The beamforming design of wireless communication under large-scale RIS deployment was introduced in [5]. In [6], the optimization of joint beamforming between base station and RIS was studied. In [7], RIS-assisted multiple-input-single-output (MISO) communication was studied. In order to optimize the spectral efficiency, the branch and bound algorithm was proposed to jointly optimize the active beamforming at the base station and the passive beamforming at RIS to obtain the global optimal solution. The author of [8] developed a distributed method for multiple RIS scenarios, which controls each RIS separately by setting circuit switches. This approach has the potential to decrease the energy dissipation of RIS and enhance the overall energy effectiveness of the system. Inspired by [8, 9] jointly optimized the beamforming at the base station and the phase matrix of RIS, and proposed an improved sine and cosine optimization algorithm. Under this algorithm, the optimal phase matrix can be obtained to maximize the EE of single-user MISO systems.

The physical structure and application scenarios of RIS and the specific role of RIS in future wireless communication were clearly introduced in the above literature. However, the above literature did not involve the research on RIS power optimization, and in the RIS-assisted system, the energy consumption of RIS control circuit can not be ignored. Therefore, inspired by the aforementioned study, this article studies and analyzes the EE of the multi-user MISO system in smart grid, by optimizing the beamforming, transmission power and RIS phase matrix of the base station under the perfect channel state information (CSI). Its purpose is to make the RIS-assisted MISO system easier to meet the green energy-saving targets in smart grid.

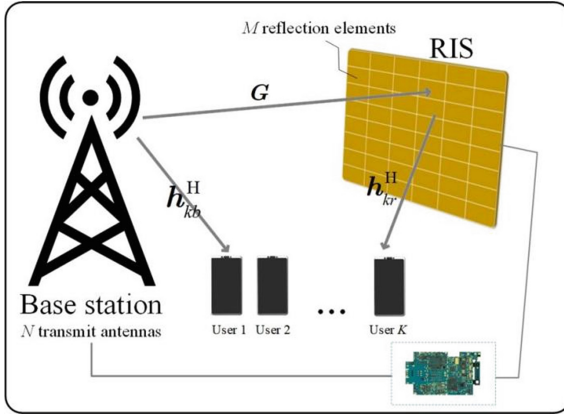


Fig. 1. The RIS-aided multi-user MISO system model

## 2 System Model

As shown in Fig. 1, consider the downlink of a RIS-assisted multiuser MISO transmission system in smart grid, which includes a base station with  $N$  antennas, a RIS with  $M$  reflection units, and  $K$  single antenna users. In addition, all user sets are represented by  $\mathcal{K} = \{1, \dots, K\}$ .

Then the signal received by the  $k$ th user can be expressed as:

$$y_k = \left( \mathbf{h}_{kr}^H \Theta \mathbf{G} + \mathbf{h}_{kb}^H \right) \sum_{i=1}^K \mathbf{w}_i s_i + n_k, k \in \mathcal{K} \tag{1}$$

where  $\mathbf{h}_{kb}^H \in \mathbb{C}^{1 \times N}$  is the channel vector from the base station to the  $k$ th user,  $\mathbf{h}_{kr}^H \in \mathbb{C}^{1 \times M}$  is the channel vector from the RIS to the  $k$ th user,  $\mathbf{G}_l \in \mathbb{C}^{M \times N}$  is the channel matrix from the base station to the RIS,  $\mathbf{w}_i \in \mathbb{C}^{N \times 1}$  represents the beamforming vector at the base station received by the base station except the  $i$ th user,  $i \in \mathcal{K}$  and  $s_i$  represents the signal sent by the base station to the  $i$ th user.  $\Theta = \text{diag}(\beta_1 e^{j\theta_1}, \dots, \beta_M e^{j\theta_M})$ ,  $\theta_{lm} \in [0, 2\pi]$  is the phase angle,  $\beta_m \in [0, 1]$  is the amplitude reflection coefficient,  $\forall m \in \mathcal{M}$ . The general setting is  $\beta_m = 1$ . And  $\sigma^2$  represents the additive white Gaussian noise with power at the  $k$ th user.

Then, the signal-to-interference-to-noise ratio (SINR) at the  $k$ th user can be expressed as:

$$\gamma_k = \frac{|\left( \mathbf{h}_{kr}^H \Theta \mathbf{G} + \mathbf{h}_{kb}^H \right) \mathbf{w}_k|^2}{\sum_{i=1, i \neq k}^K \left| \left( \mathbf{h}_{kr}^H \Theta \mathbf{G} + \mathbf{h}_{kb}^H \right) \mathbf{w}_i \right|^2 + \sigma^2} \tag{2}$$

where  $\left( \mathbf{h}_{kr}^H \Theta \mathbf{G} + \mathbf{h}_{kb}^H \right) \mathbf{w}_i$  represents the interference caused by the other users.

Accordingly, the system's sum rate can be expressed as:

$$R_t = B \sum_{k=1}^K \log_2(1 + \gamma_k) \quad (3)$$

where  $B$  is the channel transmission bandwidth.

The power losses in the multi-user MISO transmission system primarily consist of the base station's transmission power consumption, the base station's fixed power consumption, the user's circuit power consumption, and the RIS's circuit power consumption. Therefore, the total power consumption of the system should be expressed as:

$$P_t = \sum_{k=1}^K \frac{1}{\mu} \mathbf{w}_k^H \mathbf{w}_k + P_{BS} + \sum_{k=1}^K P_{kUE} + P_{RIS} \quad (4)$$

where  $\mu$  is the efficiency of the base station power amplifier,  $P_{BS}$  is the fixed power consumption of the base station itself,  $P_{k,UE}$  is the circuit power consumption of the  $k$ th user, and  $P_{RIS}$  is the power consumption of RIS.

This paper studies the EE maximization of RIS-assisted multi-user MISO system, which is denoted by  $\eta_{EE}$  and expressed as:

$$\eta_{EE} = \frac{B \sum_{k=1}^K \log_2 \left( 1 + \frac{|(\mathbf{h}_{kr}^H \ominus \mathbf{G} + \mathbf{h}_{kb}^H) \mathbf{w}_k|^2}{\sum_{i=1, i \neq k}^K |(\mathbf{h}_{kr}^H \ominus \mathbf{G} + \mathbf{h}_{kb}^H) \mathbf{w}_i|^2 + \sigma^2} \right)}{\sum_{k=1}^K \frac{1}{\mu} \mathbf{w}_k^H \mathbf{w}_k + P_{BS} + \sum_{k=1}^K P_{kUE} + P_{RIS}} \quad (5)$$

By jointly optimizing the base station's beamforming  $\mathbf{w} = \{\mathbf{w}_k, k \in \mathcal{K}\}$  and the RIS's reflection angle  $\theta = \{\theta_m, m \in \mathcal{M}\}$ , the EE is maximized under the constraints of meeting the minimum rate requirements of the system users and the maximum transmission power of the base station [10].

### 3 Problem Formation and Solving

Then, the original optimization problem can be formulated as follows:

$$\begin{aligned} & \max_{\mathbf{w}, \theta} \eta_{EE} \\ & \text{s.t. C1: } \log_2(1 + \gamma_k) \geq R_{k, \min}, \forall k \in \mathcal{K}, \\ & \text{C2: } \sum_{k=1}^K \frac{1}{\mu} \mathbf{w}_k^H \mathbf{w}_k \leq P_{\max}, \\ & \text{C3: } \theta_m \in [0, 2\pi], m \in \mathcal{M}. \end{aligned} \quad (6)$$

where C1 is the minimum rate limit for each user, C2 is the transmission power constraint at the base station, and C3 is the RIS phase angle constraint.

The original problem (6) is a fractional programming problem, which contains discrete variables, so it is non-convex and difficult to solve directly. In order to solve the

non-convex problem, this paper initially breaks down the original problem into two sub-problems: beamforming optimization and reflection phase optimization, then optimizes the individual problem independently and alternately, and finally obtains the optimal solution of the problem. Next, this paper will introduce the algorithm process of two sub-problems optimization.

### 3.1 The Sub-Problem of Beamforming Optimization

To simplify the computational complexity, we make the assumption that the base station employs maximum ratio transmission precoding, that is, under the maximum ratio transmitting (MRT) precoding, the user can obtain the maximum SINR. At this point, the beamforming under multi-user can be expressed as:

$$\mathbf{w}_k = \sqrt{\varepsilon} \cdot \frac{(\mathbf{G}^H \Theta \mathbf{h}_{kr} + \mathbf{h}_{kb})}{\|\mathbf{h}_{kr}^H \Theta \mathbf{G} + \mathbf{h}_{kb}^H\|_2} \quad (7)$$

where  $\varepsilon$  is the transmission power for each user.

Therefore, the EE maximization problem in RIS-aided multiuser MISO systems can be expressed as:

$$\begin{aligned} \max_{\theta} \eta_{EE} &= \frac{B \sum_{k=1}^K \log_2 \left( 1 + \frac{|(\mathbf{h}_{kr}^H \Theta \mathbf{G} + \mathbf{h}_{kb}^H) \mathbf{w}_k|^2}{\sum_{i=1, i \neq k}^K |(\mathbf{h}_{kr}^H \Theta \mathbf{G} + \mathbf{h}_{kb}^H) \mathbf{w}_i|^2 + \sigma^2} \right)}{\sum_{k=1}^K \frac{1}{\mu} \mathbf{w}_k^H \mathbf{w}_k + P_{BS} + \sum_{k=1}^K P_{kUE} + P_{RIS}} \\ \text{s.t. } & B \sum_{k=1}^K \log_2 \left( 1 + \frac{|(\mathbf{h}_{kr}^H \Theta \mathbf{G} + \mathbf{h}_{kb}^H) \mathbf{w}_k|^2}{\sum_{i=1, i \neq k}^K |(\mathbf{h}_{kr}^H \Theta \mathbf{G} + \mathbf{h}_{kb}^H) \mathbf{w}_i|^2 + \sigma^2} \right) \geq R_{k, \min}, \forall k \in \mathcal{K}, \\ & \sum_{k=1}^K \frac{1}{\mu} \mathbf{w}_k^H \mathbf{w}_k \leq P_{\max}, \\ & P_{\min} \leq \varepsilon \leq P_{\max}, \\ & \theta_m \in [0, 2\pi], \forall m \in \mathcal{M}, \end{aligned} \quad (8)$$

where  $P_{\max}$  is the maximum transmission power at the base station, and  $P_{\min}$  is the minimum transmission power at the base station. Because the working state of the reflector is controlled by the switch, the power of the RIS will be changed, thus affecting the total power of the system, so the transmit power  $\varepsilon$  is a real-time change, so the update formula of the power  $\varepsilon$  is expressed as follows:

$$\begin{aligned} \varepsilon &= \frac{g_k P_0 - \frac{1}{\mu}}{\frac{1}{\mu} g_k W \left( \frac{g_k P_0 - 1/\mu}{1/\mu \cdot e} \right)} - \frac{1}{g_k} \\ \text{s.t. } & P_{\min} \leq \varepsilon \leq P_{\max} \end{aligned} \quad (9)$$

where  $g = g_k/\sigma^2$ ,  $P_0 = P_{BS} + \sum_{k=1}^K P_{kUE} + P_{RIS}$ ,  $P_{\min} = (2^{R_{\min}/B} - 1)/g_k$ .

### 3.2 The Sub-problem of Phase Optimization

For the above optimization problem, this paper selects phase  $\theta$  to jointly optimize the phase matrix of RIS and the beamforming emitted by the base station [12]. Therefore, The optimization of phase  $g_k$  is based on the channel gain  $\theta$  under this model.

As (8), the sub-problem of optimizing  $\theta$  can be represented as:

$$\begin{aligned} \max_{\theta} g_k &= \left\| h_{kr}^H \Theta G + h_{kb}^H \right\|_2^2 \\ \text{s.t. } \theta_m &\in [0, 2\pi], m \in \mathcal{M} \end{aligned} \quad (10)$$

Due to the non-convex nature of optimization problem (9), obtaining a closed solution directly is challenging. In order to deal with this problem, an enhanced SCA algorithm is employed to find the optimal solution for the phase matrix. Detailed steps are described as follows.

1. Randomly generate  $I$  individuals  $X_i$ , in which each element of the individuals must meet the unit mode constraint, phase Angle  $\theta \in [0, 2\pi]$ .
2. Formula (8) is utilized to calculate the objection function of each individual, and its maximum value is obtained by finding a locally optimal individual through random generation of individuals.
3. The first  $I/2$  individuals are iteratively upgraded according to Formula (11). During the process, fitness functions of each time were compared and local optimal individuals were updated.

$$\theta^{t+1} = \text{diag}(\mathbf{h}_{kr}^H) \mathbf{G} \cdot \left( \mathbf{h}_{kb} + \left( \text{diag}(\mathbf{h}_{kr}^H) \mathbf{G} \right)^H \cdot \theta^t \right) \quad (11)$$

4. After  $I/2$  individuals are iteratively updated according to formula (12), the local optimal solution at this time is jumped out, and the global optimal solution is developed and explored. In the process, the fitness function of each time is still compared and the optimal individual is updated.

$$x_{ij}^{t+1} = \omega \cdot \begin{cases} w^t \cdot x_{ij}^t + r_1 \cdot \sin r_2 \cdot \left| r_3 p_{gj}^t - x_{ij}^t \right| r_4 < 0.5 \\ w^t \cdot x_{ij}^t + r_1 \cdot \cos r_2 \cdot \left| r_3 p_{gj}^t - x_{ij}^t \right| r_4 \geq 0.5 \end{cases} \quad (12)$$

5. When the iteration is finished and the fitness function reaches convergence, the optimal solution for the given phase is obtained. In case the function does not converge, the number of iterations is increased until convergence is achieved.

In addition,  $r_1$  as a control parameter, mainly controls the amplitudes of sine and cosine functions, and adaptively adjusts by (14).  $T$  represents the maximum number of iterations and remains constant throughout the process. Typically, it has a general value of 2.  $\omega$  updates according to the time-varying weight in the particle swarm.

$$\text{levy}(v) = \left[ \frac{\Gamma(1+v) \cdot \sin(\pi v/2)}{\Gamma[(1+v)/2] \cdot v \cdot 2^{(v-1)/2}} \right]^{1/v} \quad (13)$$

$$r_1 = a \cdot \left(1 - \frac{t}{T}\right) \tag{14}$$

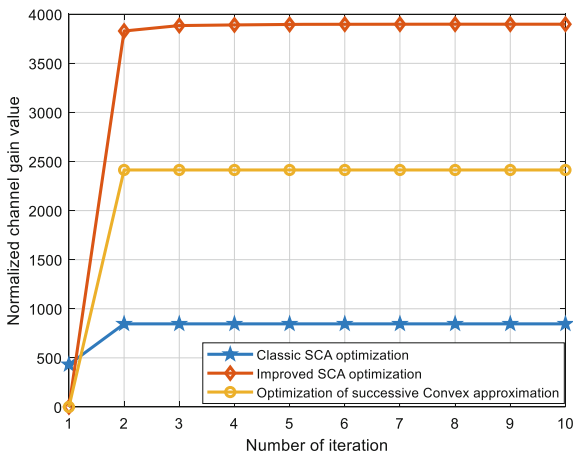
where  $\nu$  is the scaling factor.

### 4 Numerical Results and Discussions

In this section, we utilize MATLAB software to execute simulation experiments and verify the effectiveness of the proposed approach. The system parameters are mainly give as Table 1.

**Table 1.** Simulation parameter setting

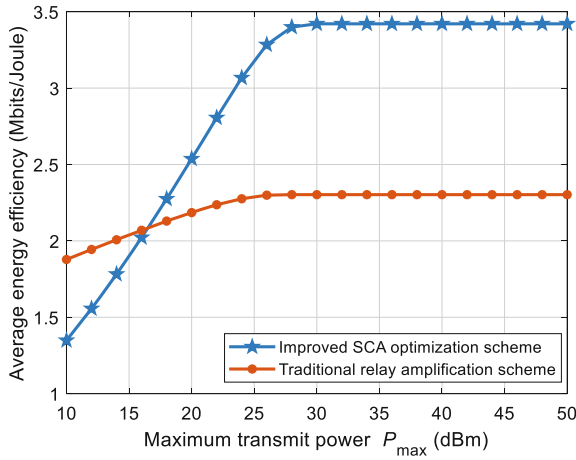
Simulation parameters	Simulation parameters
Transmitting antenna $N$	8
RIS reflecting element $M$	32
Maximum transmit power of base station $P_{I\max}$	30 dBm
Individual dimension $D$	32
Population quantity $I$	100
Number of iteration $T$	100
Levi's flight parameters $\nu$	1.5
Time-varying weight $W_{\min}$	0.2
Time-varying weight $W_{\max}$	0.8



**Fig.2.** Channel gain under three different schemes

Figure 2 displays the convergence characteristics of the enhanced SCA algorithm, illustrating its effectiveness. As shown in Fig. 2, the enhanced SCA algorithm exhibits

approximately a 70% increase in term of channel gain, compared with its original version. This is primarily due to the fact that the original SCA algorithm tends to prematurely converge to a local optimal solution when tackling NP-hard problems. On the other hand, incorporating Levy flight and time-varying weights can overcome this limitation and enhance the algorithm's performance. In addition, compared to the approach described in reference [8], the enhanced SCA algorithm exhibits an approximately 27% increase in channel gain and achieves faster convergence speed. Because by using the optimal phase update formula in the literature, in the SCA algorithm, it is possible to determine the direction of the global optimal solution, combined with the improved SCA algorithm can effectively prevent falling into the local optimal, so we can get a larger channel gain.



**Fig.3.** Variation of EE with  $P_{\max}$  for the two schemes

In order to better illustrate the superiority of the proposed algorithm for the energy efficiency of the system, Fig. 3 illustrates the performance of each scheme in terms of EE (Energy Efficiency) under varying maximum transmission power at the base station. It can be seen that compared with the traditional relay amplification scheme, the improved SCA optimization scheme has achieved about 30% improvement in energy efficiency for the RIS-assisted MISO system. And it can be found in the figure that when  $P_{\max} \leq 25$  dBm, the energy efficiency of each scheme system increases almost linearly with the increase of the maximum transmission power of the base station. However, when  $P_{\max} \geq 25$  dBm, the energy efficiency of each scheme almost tends to be stable and no longer increases. At this time, it can be observed that the EE of the system does not strictly increase as the maximum transmit power of the base station increases. Therefore, this scheme can also be used to obtain the best transmission power of the system, so that the highest energy efficiency of the system can be obtained at the lowest transmission power, which is very consistent with the current green and sustainable performance index of wireless communication.



## 5 Conclusions

This paper studies energy-efficient RIS-aided multi-user MISO systems in integrated power communication networks, and proposes to optimize the RIS's phase matrix of RIS to refine the system's EE performance for information acquisition services. Firstly, the SCA optimization algorithm is introduced to optimize the RIS's phase matrix. Building upon this, an enhanced version of the SCA algorithm is devised to advance the phase matrix further, and the optimal value obtained by this algorithm is more accurate. Secondly, for multi-user beamforming, it is proposed that the base station uses MRT precoding to maximize the SINR received by users. Finally, a scheme is proposed to iterate alternately by using the optimized phase matrix and the power of the system.

**Acknowledgement.** This work was supported by State Grid Jibei Electric Power Co., Ltd. Science and Technology Project (No. SGJBXT00TJJS2200267).

## References

1. Yu, T., Zhang, S., Chen, X., Wang, X.: A novel energy efficiency metric for next-generation green wireless communication network design. *IEEE Internet Things J.* **10**(2), 1746–1760 (2023)
2. Dan, W., Xiaomeng, C., Yongfang, W.: User assignment of wireless communication assisted by reconfigurable intelligent surface. *J. Electron. Inf.* **44**(7), 2425–2430 (2022)
3. Dai, L., Wang, B.C., Wang, M., et al.: Reconfigurable intelligent surface-based wireless communications: antenna design, prototyping, and experimental results. *IEEE Access* **8**, 45913–45923 (2020)
4. Wu, Q., Zhang, R.: Towards smart and reconfigurable environment: intelligent reflecting surface aided wireless network. *IEEE Commun. Mag.* **58**, 106–112 (2020)
5. Shen, D., Dai, L.: Multi-Beam design for extremely large-scale RIS aided near-field wireless communications. In: *Proceedings of 2022 IEEE Global Communications Conference (2022)*
6. Wu, Q., Zhang, R.: Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming. *IEEE Trans. Commun.* **18**(11), 5394–5409 (2019)
7. X. Yu, D. Xu and R. Schober. Optimal beamforming for MISO communications via intelligent reflecting surfaces. *Proc. of 2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2020
8. Yang, Z., et al.: Energy-efficient wireless communications with distributed reconfigurable intelligent surface. *IEEE Trans. Wireless Commun.* **21**(1), 665–679 (2022)
9. Tan, F., Xu, X.: Energy-efficient beamforming optimization for MISO communication based on reconfigurable intelligent surface. *Phys. Commun.* **57**, 1874–4907 (2023)
10. Lin, Y., Yang, Z., Guo, H.: Proportional fairness-based energy-efficient power allocation in downlink MIMO-NOMA systems with statistical CSI. *China Commun.* **16**(12), 47–55 (2019)
11. Liu, Y., Yingyi, S., Yi, W. et al.: Selection scheme for saving transmission power in multi-RIS scenarios. *Electron. Measur. Technol.* **8**, 45 (2022)
12. Lin, S., Zheng, B., Alexandropoulos, G.C., Wen, M., di Renzo, M., Chen, F.: Joint passive beamforming and information transfer for RIS-empowered wireless communications. In: *Proceedings of 2020 IEEE Global Communications Conference (2020)*



# Multi-path Transmission Strategy for Deterministic Networks

Fei Zheng, Kelin Li, Zou Zhou<sup>(✉)</sup>, Yu Hu, and Longjie Chen

Ministry of Education Key Laboratory of Cognitive Radio and Information Processing, Guilin  
University of Electronic Technology, Guilin 541004, China  
zhouzou@guet.edu.cn

**Abstract.** With the rapid growth of internet traffic, network congestion becomes more and more severe, which causes massive packets loss. The reliability and delay of data transmission needs to be guaranteed in real-time applications such as financial transactions and cloud games. Traditional transmission strategies use packet retransmission to ensure data reliability, but the retransmission causes extra delay. The extra delay reduces the quality of service (QoS) for deterministic services. For the above problem, this paper proposes a deterministic network (DetNet)-oriented multipath transmission strategy in the software-defined network (SDN) architecture. The architecture introduces the packet replication and elimination function (PREF) of DetNet to achieve reliable transmission. The strategy establishes a path optimization model with transmission delay and packet loss rate, and then solve the model by the Q-learning algorithm. The delay and packet loss rate of the link construct the reward function. The Q-value table enables to obtain the best combination of paths, and it is gained by the reward function. Simulations show that our strategy have lower packet loss rate and delay jitter than the traditional single-path transmission strategy and the multi-path transmission strategy.

**Keywords:** Software-defined networking (SDN) · Deterministic network · Q-learning algorithm · Packet loss rate · Delay jitter

## 1 Introduction

With the advancement of information technology, the demand for high-reliability and low-delay services continues to grow steadily such as cloud games, internet of vehicles, virtual reality, and industrial automation. These services bring challenges to data transmission. Traditional single-path transmission involves risks such as single-point failures and data loss [1]. To solve these issues, numerous scholars study multi-path transmission control protocol (MPTCP). The protocol establishes multiple transmission paths and optimizes congestion control to meet users' service requirements. Reference [2] introduces multi-path technology to failure recovery. It uses multiple redundant paths for data transmission to reduce data loss. Reference [3] proposes a multi-path transmission selection algorithm based on the immune connectivity model. This algorithm balances the load, extends the life of the network, and ensures reliable data transmission. Reference [4] proposes a multi-path transmission optimization scheme DMPTCP. The

scheme allows the receiver to send negative acknowledgement messages to the sender simultaneously by multiple sub-streams. The sender is able to quickly obtain the packet disorder in the receiver and retransmit packets that are lost.

The multi-path transmission strategy uses the mechanism of packet retransmission to ensure data reliability. However, the mechanism causes extra delay when packet loss occurs. The extra delay reduces the quality of service (QoS) for deterministic services.

High-quality data transmission plays a crucial role in meeting users' service requirements and promoting the future of networking. To ensure high-quality data transmission, Deterministic Networking (DetNet) [5, 6] and Software-Defined Networking (SDN) are regarded as one of the future solutions. DetNet provides the optimal paths for data. DetNet uses the resource reservation, and the packet replication and elimination function (PREF) to achieve high-reliability and low-delay transmission for real-time applications. SDN improves not only the flexibility of the network but also access security and efficiency [7, 8]. The combination of SDN and DetNet has become a hot spot to achieve reliable transmission.

Reference [9] introduces a DetNet service protection architecture based on SRv6. The architecture aims to achieve efficient control and forwarding in DetNet. The paper also proposes a path selection algorithm based on shared protection to improve network resource utilization. Reference [10] puts forward a stream reservation solution with Time Sensitive Network (TSN)-SDN controllers. The approach ensures the utilization of bandwidth. Reference [11] designs a TSNU architecture that guarantees the time slot allocation for scheduling services and alleviates network congestion in industrial IoT. In summary, the combination of SDN and DetNet represents the new trend of network development.

This paper presents a DetNet architecture based on SDN to achieve reliable transmission. This architecture is composed of a network control layer and a data forwarding layer. The SDN controller is composed of three functional modules in the control layer: a path collection module, a path calculation module, and a path assignment module. The path collection module is primarily responsible for gathering information about the network topology and the link resources. The path calculation module performs path calculations. The path assignment module is responsible for sending out flow table. The data forwarding layer is primarily responsible for data transmission and is composed of clients, edge devices, and SDN routers. The edge devices have three major functions: packet ordering, packet replication, and packet elimination.

In Fig. 1, the source sends a DetNet stream to the destination. The source edge device adds each packet in a DetNet stream with a sequence number by the packet ordering function. The source edge device copies the numbered packets by the packet replication function and forwards them through two disjoint paths. When data arrives at the destination edge device, the destination edge device deletes duplicate packets by sequence number. Finally, the destination edge device combines the packets into a DetNet stream and sends it to the receiver based on the sequence number.

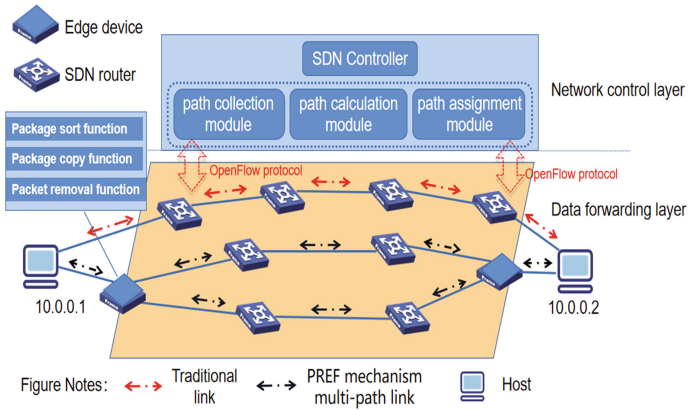


Fig. 1. The SDN-based DetNet architecture

## 2 System Model

### 2.1 Network Topology of SDN

In Fig. 2, the network topology of SDN is described as an undirected graph  $G = (V, E)$ ,  $V = \{v_1, v_2, \dots, v_i, \dots, v_n\}$  represents the set of routing nodes within the network, and  $E = \{e_{i,j} | i, j \in V\}$  denotes the set of links of two neighboring routing nodes in the network.

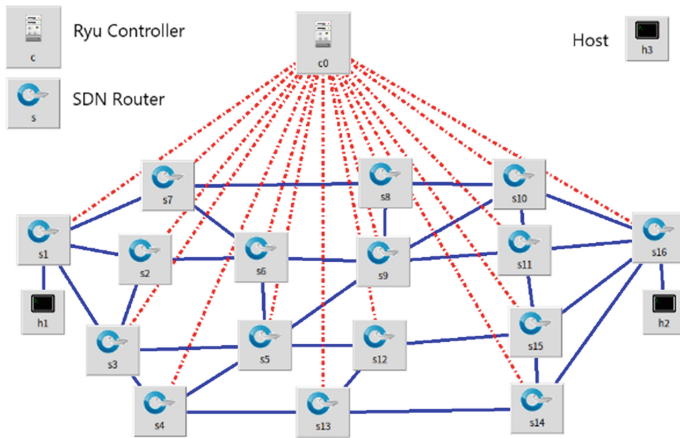


Fig. 2. The network topology of SDN

### 2.2 Queuing Delay

Each routing node has a buffer queue. The queuing delay  $d^{que}(v_i)$  is the waiting delay for packet transmission in the buffer queue. When there are few packets in the buffer queue, the queuing delay will increase.

This paper uses the M / M /1/ N single-service queuing model to simulate a buffer queue in a routing node. In the M / M /1/ N model, the first parameter M represents that the input process of the packets is approximately a Poisson distribution. The second parameter M denotes that the output process of the packets is approximately a negative exponential distribution. 1 represents the number of servers. N represents the system capacity. The queuing delay can be expressed as follows:

$$d^{que}(v_i) = \frac{L_i}{\mu(1 - Q)} \tag{1}$$

where  $L_i = \frac{\rho}{1-\rho} - \frac{(N+1)\rho^{N+1}}{1-\rho^{N+1}}$ ,  $\rho = \frac{\lambda}{\mu}$ ,  $Q = \frac{1-\rho}{1-\rho^{N+1}}$ , and  $\rho$  represents the service intensity,  $\lambda$  denotes the average arrival rate,  $\mu$  represents the average processing rate of the routing node,  $L_i$  represents the expected value of queued packets, and  $Q$  represents the idle probability of the buffer queue.

Packet loss rate and delay jitter are important parameters for measuring DetNet performance. Delay jitter represents the variance of all packets delay on the same path.

$$J = \sqrt{\frac{\sum_{k=1}^{N_{data}} (t_k - \bar{t})^2}{N_{data}}} \tag{2}$$

where  $\bar{t} = \frac{\sum_{k=1}^{N_{data}} t_k}{N_{data}}$ , and  $N_{data}$  represents the total number of packets,  $t_k$  represents the delay of the  $k$ -th packet, and  $\bar{t}$  denotes the average transmission time of the packets.

The packet loss rate represents the percentage of packets loss due to queue buffer overflow. In the M/M/1/N model, the packet loss rate  $l(v_i, v_j)$  can be calculated by the following formula:

$$l(v_i, v_j) = \frac{1 - \rho}{1 - \rho^{N+1}} \cdot \rho^N \tag{3}$$

### 2.3 Transmission Delay

The transmission delay is composed of the queuing delay, the propagation delay, the sending delay, and the processing delay. In DetNets, the queuing delay and the propagation delay are usually in the millisecond range or higher. However, the processing delay of high-speed routers is usually in the microsecond range or lower. This paper only pay attention to the queuing delay and the propagation delay, and it neglects the transmission delay and the processing delay because the sending delay and the processing delay have the same millisecond range. The transmission delay is comprised of the link transmission delay.

$$d(v_i, v_j) = d^{pro}(v_i, v_j) + d^{que}(v_i) \tag{4}$$

Where  $(d^{pro}v_i, v_j)$  represents the link propagation delay from routing node  $v_i$  to routing node  $v_j$ , and  $(d^{que}v_i, v_j)$  denotes the link queuing delay from routing node  $v_i$  to routing node  $v_j$ .

## 2.4 Route Planning

$P(s, d) = \{p_1, \dots, p_r, \dots, p_m\}$  represents the set of all paths from  $s$  to  $d$ . For meeting the requirement of reliable data transmission, we search for the set of paths with better combination of delay and packet loss rate. The paths have a number of constraints:

First, we remove paths with excessive delay:

$$\sum_{\forall (v_i, v_j) \in p_r} d^{\text{pro}}(v_i, v_j) + \sum_{\forall v_i \in p_r} d^{\text{que}}(v_i) < T_{\text{max}}, \forall p_r \in P(s, d) \quad (5)$$

where  $T_{\text{max}}$  represents the threshold of path delay.

$b(v_i, v_j)$  denotes the available bandwidth of the link from routing node  $v_i$  to routing node  $v_j$ .  $b(v_i, v_j)$  is represented as the following formula:

$$\sum_{\forall (v_i, v_j) \in p_r} b(v_i, v_j) > B_{\text{min}}, \forall p_r \in P(s, d) \quad (6)$$

where  $B_{\text{min}}$  represents the required minimum bandwidth for the service.

We need to normalize the link transmission delay and the packet loss rate. The following formulations show the normalized link transmission delay and the packet loss rate:

$$\bar{d}(v_i, v_j) = \frac{d(v_i, v_j) - d(v_i, v_j)_{\text{min}}}{d(v_i, v_j)_{\text{max}} - d(v_i, v_j)_{\text{min}}} \quad (7)$$

$$\bar{l}(v_i, v_j) = \frac{l(v_i, v_j) - l(v_i, v_j)_{\text{min}}}{l(v_i, v_j)_{\text{max}} - l(v_i, v_j)_{\text{min}}} \quad (8)$$

where  $d(v_i, v_j)_{\text{max}}$  is the maximum link transmission delay.  $d(v_i, v_j)_{\text{min}}$  represents the minimum link transmission delay.  $l(v_i, v_j)_{\text{max}}$  denotes the maximum packet loss rate.  $l(v_i, v_j)_{\text{min}}$  is the minimum packet loss rate.

This paper establishes the QoS function  $f(p_r)$  with the link transmission delay  $\bar{d}(v_i, v_j)$  and the packet loss rate  $\bar{l}(v_i, v_j)$ . The QoS function  $f(p_r)$  can be calculated by the following formula:

$$f(p_r) = \theta \sum_{\forall (v_i, v_j) \in p_r} \bar{d}(v_i, v_j) + (1 - \theta) \sum_{\forall (v_i, v_j) \in p_r} \bar{l}(v_i, v_j), \forall p_r \in P(s, d) \quad (9)$$

where  $\theta$  represents the weights of the transmission delay and the packet loss rate.

In summary, we establish a multi-constraint model to solve multi-path problem base on the PREF.

$$\begin{aligned}
 g^* = \arg \min & \sum_{r=1}^u f(p_r), \forall p_r \in P(s, d) \\
 s.t. & \begin{cases} \sum_{\forall (v_i, v_j) \in p_r} d^{\text{pro}}(v_i, v_j) + \sum_{\forall v_i \in p_r} d^{\text{que}}(v_i) < T_{\text{max}} \\ \sum_{\forall (v_i, v_j) \in p_r} b(v_i, v_j) > B_{\text{min}} \\ d^{\text{pro}}(v_i, v_j) \geq 0 \\ d^{\text{que}}(v_i) \geq 0 \end{cases} \tag{10}
 \end{aligned}$$

where  $g^*$  represents the set of paths, which can minimize the transmission delay and the packet loss rate, and  $u$  denotes the number of paths needed for multipath transmission.

### 3 Multi-path Transmission Strategy Base on Q-Learning

This paper solves the multi-constraint model by Q-learning algorithm. The algorithm is a model-free iterative Q-value algorithm:

$$Q(s, a) \leftarrow Q(s_t, a_t) + \alpha [(r(s_t, a_t) + \lambda \max_{a_t} Q(s_{t+1}, a_t) - Q(s_t, a_t))] \tag{11}$$

where  $\alpha$  represents the learning rate,  $\lambda$  is the discount factor,  $s_t$  represents the state at moment  $t$ , and  $a_t$  is the action taken at moment  $t$ .

State-space design: the set of states  $S_t = V = \{v_1, \dots, v_i, \dots, v_n\}$  consists of routing nodes of the SDN network.  $F(v) = \{F(v_1), \dots, F(v_i), \dots, F(v_n)\}$  consists of the set of neighboring nodes of routing node  $i$ .

Action space design: The action space  $A(v) = \{A(v_1), \dots, A(v_i), \dots, A(v_n)\}$  consists of the set of actions of each route node  $i$ . where  $A$  denotes the optional action of routing node  $i$ . The selectable action is represented by the set of neighboring nodes.

Feedback design:  $r(s_t, a_t)$  represents the maximum discount reward.

$$r_{s_t, a_t} = \vartheta r_{\bar{d}(v_i, v_j)} + 1 - \vartheta r_{\bar{l}(v_i, v_j)} + r_{dst} \tag{12}$$

where  $\vartheta$  ( $0 < \vartheta < 1$ ) represents the weights of the delay feedback  $r_{\bar{d}(v_i, v_j)}$  and the packet loss rate feedback  $r_{\bar{l}(v_i, v_j)}$ . The  $r(s_t, a_t)$  consists of the delay feedback  $r_{\bar{d}(v_i, v_j)}$ , the packet loss rate feedback  $r_{\bar{l}(v_i, v_j)}$  and the arrival destination reward  $r_{dst}$ .

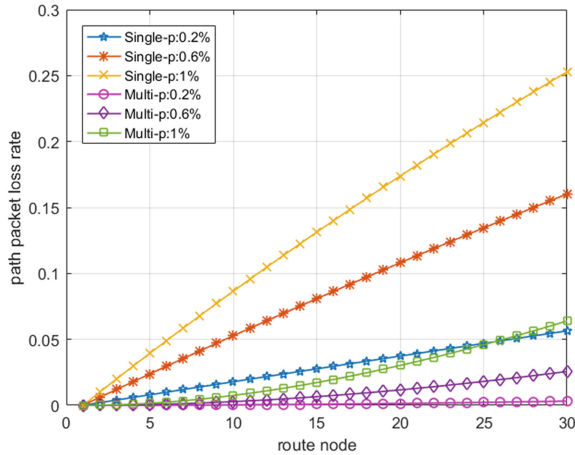
This paper obtains multiple disjoint paths by the Q-value table. We group the found paths in pairs. If we find more than one combination that satisfies the condition, we select the path combination with a close number of hops. If we cannot find a combination that satisfies the condition, the one with the shortest number of hops is chosen as the optimal path. We use the Dijkstra shortest path algorithm for planning the second path after removing the optimal path node in the original SDN topology.

## 4 Experimental Simulation

In this section, we simulate the performance of different transmission strategies in terms of packet loss rate, transmission delay, and delay jitter. The experimental parameters are mainly give as Table 1.

**Table 1.** Experimental parameter setting

Parameter	Value
Simulation time	20 s
Number of packages	10000
Link bandwidth	[0–100] Mbps
Average package size	1024 bit
Service requirements bandwidth $B_{\min}$	10 MB
Learning Rate $\alpha$	0.4
Discount Factor $\lambda$	0.3
Scale factor $\vartheta$	0.4



**Fig. 3.** Comparison of path packet loss between single path and PREF-based multi-path

The experiment sets 2 paths for the PREF multipath transmission strategy. 2 paths of the PREF multipath transmission strategy have the same number of routing nodes as a single path. The link packet loss rate for each path is 0.2%, 0.6%, and 1%.

Figure 3 illustrates an upward trend in the curve of the path packet loss rate with the increase in the number of routing nodes. The path packet loss rate curve of the PREF multipath transmission strategy is greater than a single path. It can be concluded that the PREF multipath transmission strategy has advantages in ensuring data reliability.



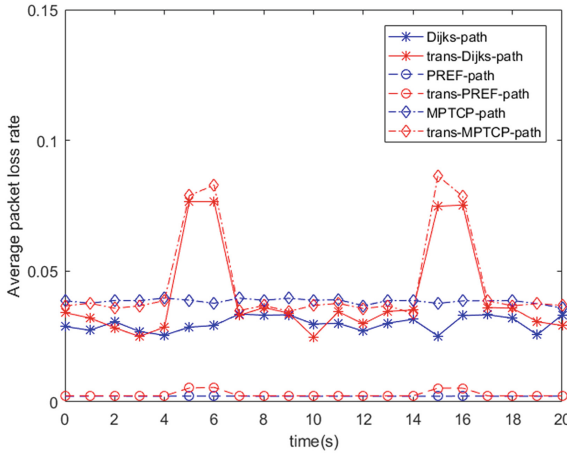


Fig. 4. Average packet loss performance comparison of three transmission strategies

Figure 4 illustrates the performance of three transmission strategies in regard to the average packet loss rate. The PREF multipath transmission strategy has a lower average packet loss rate than the traditional single-path transmission strategy and the multi-path transmission strategy of the MPTCP protocol in 20s. In addition, this paper experiments on link packet loss sudden change. We suddenly increase the packet loss rate of the link at  $t = 5s$ ,  $t = 6s$ ,  $t = 15s$ ,  $t = 16s$ . The experimental result shows that the average packet loss rate curve of the PREF multipath transmission strategy remains stable. It can be concluded that the transmission strategy is able to deal with the sudden situation of link packet loss.

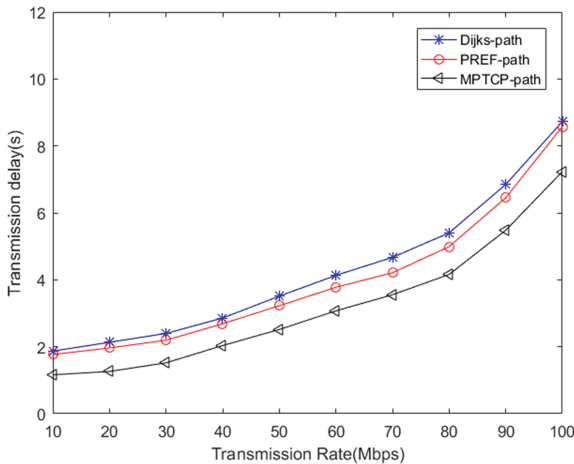


Fig. 5. The relationship between transmission rate and transmission delay

Figure 5 illustrates an upward trend in the curve of the transmission delay with the increase of sending rate. The main reason is that the sending rate exceeds the bandwidth of the path causing an increase in queuing delay. Among the three transmission strategies, the multi-path transmission strategy of the MPTCP protocol has the shortest transmission delay, and the traditional single-path transmission strategy has the longest transmission delay. This is because the multi-path transmission strategy of the MPTCP protocol uses multiple sub-streams transmitted in parallel on different paths, which can reduce data transmission time. The PREF multipath transmission strategy uses packet replication and multiplexing for transmission, resulting in a lower transmission time compared to the traditional single-path transmission strategy.

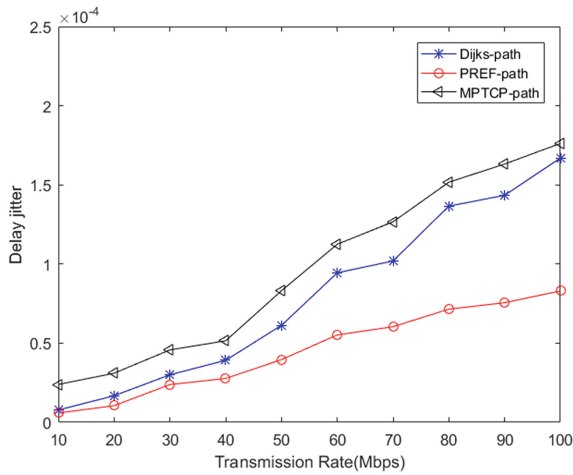


Fig. 6. The relationship between transmission rate and delay jitter

Figure 6 illustrates an upward trend in the curve of the delay jitter with the increase of sending rate. The main reason is that the delay jitter is mainly affected by the queuing delay. The average packet loss rate curve of the PREF multipath transmission strategy is significantly lower than other transmission strategies. The PREF multipath transmission strategy always depends on the path with the minimum delay, thereby reducing the time difference between consecutive packets and consequently reducing delay jitter.

## 5 Conclusions

This paper proposes a DetNet-oriented multipath transmission strategy in the SDN architecture. The architecture introduces the PREF of DetNet to achieve reliable transmission. The strategy establishes a path optimization model with transmission delay and packet loss rate, and then solves the model by the Q-learning algorithm. Simulations show that our strategy have lower packet loss rate and delay jitter than the traditional single-path transmission strategy and the multi-path transmission strategy.

**Acknowledgement.** This work was supported by Dean Project of Key Laboratory of Cognitive Radio and Information Processing Ministry of Education (No. CRKL200107).

## References

1. Memon, S., Wang, J., Bhangwar, A.R., Fati, S.M., Rehman, A., Xu, T., Zhang, L.: Temperature and reliability-aware routing protocol for wireless body area networks. *IEEE Access* **9**, 140413–140423 (2021)
2. Liu, P., Zongpeng, D., Yongjing Li, L., Duan, X.: End-to-end deterministic networking architecture and key technologies. *Telecommun. Sci.* **37**(9), 64–73 (2021)
3. Zhang, Z., Zhang, C., Li, H.: Multipath transmission selection algorithm based on immune connectivity model. *J. Comput. Appl.* **40**(12), 3571 (2020)
4. Jiang, Z., Qian, W., Li, H., Jianpin, W.: Link on-off prediction based multipath transfer optimization for aircraft. *J. Tsinghua Univ. (Sci. Technol.)* **57**(12), 1239–1244 (2017)
5. Nasrallah, A., Alharbi, Z., Wang, C.: Ultra-low latency (ULL) networks: The IEEE TSN and IETF DetNet standards and related 5G ULL research. *IEEE Commun. Surv. Tutor.* **21**(1), 88–145 (2018)
6. Huang, T., Wang, S., Huang, Y., Zheng, Y., Liu, J., Liu, Y.: Survey of the deterministic network. *J. Commun.* **40**(6), 160–176 (2019)
7. Priyadarsini, M., Bera, P.: Software defined networking architecture, traffic management, security, and placement: a survey. *Comput. Netw.* **192**, 108047 (2021)
8. Hakiri, A., Gokhale, A., Berthou, P.: Challenges and research opportunities for Future Internet. *Comput. Netw.* **75**, 453–471 (2014)
9. Li, S., Fang, J., Chen, K.: DetNet service share protection scheme based on SRv6. *J. Commun.* **42**(10), 32–42 (2021)
10. Jianzhong, S., Zhang, H., Zhu, H.: Computing method for periodic stream reservation in TSN combined with SDN controller. *J. Commun.* **42**(10), 23–31 (2021)
11. Venkatraman, B., Moayad, A., Martin, R.: An SDN architecture for time sensitive industrial IoT. *Comput. Netw.* **186**, 107739 (2021)



# SDN-Based Efficient Consortium Blockchain Network Architecture for Grid Information Authentication

Tian Liu, Shuang Yang<sup>(✉)</sup>, Yu Yang, Kelin Yang, Bo Li, Cong Chao, and Bin Sun

State Grid Heze Power Supply Company, Heze, China  
winnie.ys@163.com

**Abstract.** Aiming at the problem of communication redundancy and delay for grid information authentication in the existing consortium blockchain network, a new architecture for optimizing the broadcast path by controlling the topology of the consortium blockchain by software defined networking (SDN) is proposed. First, the SDN controller can collect the information and status of nodes in the consortium blockchain network in real time, and make topology adjustments accordingly. Secondly, some existing practices reduce the redundancy and delay brought by the Gossip protocol, but also bring serious computational burden to the nodes. Therefore, our proposed architecture is divided into two layers. The task of adjusting the topology structure is assigned to the upper-SDN controller layer, and the normal operation of the consortium blockchain network is assigned to the lower-blockchain layer, which not only solves the problem of limited computing power of grid information authentication nodes, but also makes the consortium blockchain network flexible, stable and easy to expand. Finally, the simulation results show that the topology adjustment made by SDN effectively reduces the communication redundancy and delay brought by the Gossip protocol in the consortium blockchain network and improves the consensus efficiency.

**Keywords:** Grid information authentication · Consortium blockchain network · Software defined networking · Gossip protocol

## 1 Introduction

Since the blockchain 1.0 represented by bitcoin [1], blockchain technology has received extensive attention from researchers for its decentralization, tamper-proof and traceability. Up to now, consortium blockchain technology is no longer confined to the financial field, and is gradually applied to the field of Internet of things such as Internet of vehicles [2], smart grid [3], and drug traceability [4]. However, in the process of consortium blockchain for grid information authentication, many problems have also arisen, such as high delay, large communication overhead, low throughput, inflexible network topology, and large resource consumption. These problems are largely directly related to the performance of the consortium blockchain for grid information authentication. Most

of the existing solutions to improve throughput, scalability and reduce resource consumption are by designing more efficient consensus algorithms [5], optimizing message broadcasting [6], optimizing data storage [7] and using side chains [8]. However, the improvement effect of the above scheme is still limited.

To solve these problems, this paper proposes to combine the consortium blockchain architecture based on directed acyclic graph (DAG) with the architecture based on the software defined network (SDN) paradigm [9]. In the graph structure, each block is a vertex, and the blocks are still connected by hash pointers to ensure the traceability and non-tampering of the blockchain. Since blocks can be connected to the graph structure in batches, that is, blocks are generated in parallel, the performance of the consortium blockchain is greatly improved compared to the single chain structure. To determine the order of blocks in a more secure and efficient way and generate blocks in parallel, we adopt the consortium blockchain ordering method based on maximum weight proposed by Li et al. [10], and use SDN to optimize the consortium blockchain network using Gossip protocol. The working principle of the SDN paradigm is to decouple the control plane of the network from the data forwarding plane, and the control function is excluded from the network equipment and aggregated on the SDN controller. Under this architecture, the SDN paradigm improves the control of the consortium blockchain network and provides great flexibility and scalability. By flexibly controlling the topology of the consortium blockchain network, the communication redundancy and delay generated by the Gossip protocol in the network are reduced. The main contributions of this paper are summarized as follows:

- We propose a SDN-assisted consortium blockchain network (SDBN) for grid information authentication, which is a new architecture that uses SDN to provide topology control and optimize broadcast paths in consortium blockchain networks.
- We use SDN to reduce the communication redundancy caused by the random Gossip protocol in the consortium blockchain network.
- In order to improve the stability of the network, we use a distributed SDN controller to avoid encountering single point of failure (SPoF), and also provide higher expansion space for the consortium blockchain network.

The rest of the organization of this paper is as follows. Section 2 summarizes the related work. Section 3 introduces the system model. Section 4 gives the simulation results to illustrate the SDBN environment compared to the ordinary network environment, Gossip protocol brought about by the degree of redundancy changes. Section 5 and Sect. 6 give conclusions and future work.

## 2 Related Work

At present, the number of power IoT devices is growing at an alarming rate. At the same time, most power IoT devices do not have the ability to resist intrusion and malicious attacks. In this case, the security of power IoT devices has become a research hotspot. Blockchain technology based on directed acyclic graph (DAG) has become one of the solutions to this problem with its high concurrency, scalability and security. At the same time, software defined network (SDN) makes the network more flexible and easy to

expand with its management and programmability. Therefore, combining the two has become a new solution for grid information authentication.

Shailendra et al. [11] proposed that the combination of SDN, blockchain technology and mobile edge computing technology provides a architecture for the IoT ecosystem to detect attacks efficiently. Gao et al. [12] designed a system that integrates SDN and blockchain for the Internet of Vehicles. The blockchain is designed at the control layer, and the key data such as identity authentication, data management, access control, and policy management are stored on the chain. Pradip et al. [13] proposed a new blockchain-based distributed SDN architecture, which aims to generate and deploy protection, including threat protection, data protection and access control, to mitigate network attacks such as cache forgery / Address Resolution Protocol (ARP) spoofing, DDoS / DoS attacks, and detect security threats. In addition, the model also focuses on reducing the attack window time, allowing IoT forwarding devices to quickly check and download the latest flow rule table when necessary. However, although all of the above schemes are the integration of blockchain and SDN, they mainly use blockchain technology to enhance the security of SDN architecture, and most of them are attack detection methods. In fact, it is also feasible to apply the advantages of SDN in topology control to blockchain networks, especially in the Internet of Things supported by blockchain.

Varun et al. [14] pointed out that the core of blockchain is P2P networks. Although blockchain technology has improved some aspects of P2P networks, such as providing efficient consensus protocols, identity privacy, and transaction security, distributed topology control in blockchain P2P networks is still one of the focuses of research. In their research, they discussed the constraints and problems of building an optimal P2P network for the blockchain, proposed a scheme for how to use SDN to control the topology of the blockchain network, and conducted modeling analysis and testing. Of course, there are also some other ways to improve the blockchain network. For example, Hao et al. [15] proposed a blockchain P2P topology based on trust enhancement to achieve fast and reliable broadcasting. Li et al. [10] proposed a tree-like blockchain network TBGP based on federated learning, which effectively alleviated the communication redundancy generated by the Gossip protocol during random transmission.

Compared with the above work, we focus on using SDN to regulate the topology of blockchain network for grid information authentication, focusing on solving the problem of insufficient computing power of Gossip protocol in TBGP and redundant communication in hash graph, and improving the scalability and transaction efficiency for grid information authentication.

### 3 System Architecture

In this section, the proposed blockchain network architecture was described. The upper server only controls topology, mainly stores data related to the underlying layer, such as the list and status of nodes, the outbound and inbound links of each node, and does not interfere with other protocols and functions of the underlying blockchain P2P network.

### 3.1 Architecture Overview

As shown in Fig. 1, the proposed network architecture is divided into two layers, namely the upper-SDN controller layer and the lower-blockchain layer. In the lower-blockchain layer, the device acting as a node can not only be a static IoT device, such as smart home, embedded device, desktop computer, disaster warning system, but also a mobile IoT device, such as drone, vehicle electronic control unit, robot, etc. Each node has a node communication with the upper-SDN controller designated as its neighbor. The SDN controller is responsible for collecting information from nodes. According to the state, delay, computing level, probability of being attacked, offline downtime frequency of each node, it can flexibly control the position of each node in the network and build a stable and efficient topology.

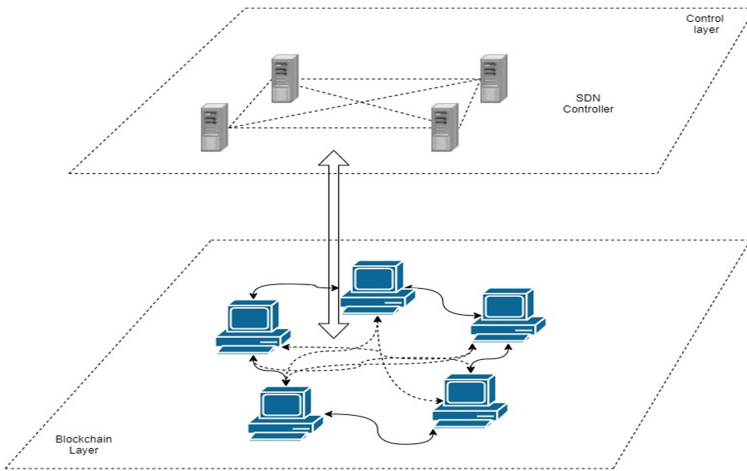


Fig.1. General architecture of the two layers.

### 3.2 Upper Layer – SDN Controller

In this layer, we set up multiple SDN controllers to form a distributed SDN control system. The Raft [16] algorithm is used between controllers to ensure strong consistency. Each controller is in charge of the lower nodes of the corresponding area, and to establish and maintain the topology of the underlying blockchain network. When the nodes in the blockchain network are dynamically added, the controller authenticates them, then collects their status information (computing power, storage, etc.), and then synchronizes the information to other controllers. Finally, the added nodes are arranged to the appropriate location in the lower layer network and the corresponding network topology is updated. If a node in the lower layer exits, it only needs to retain its own information for standby, and when exiting, the controller updates the network topology and synchronizes with other controllers to complete the exit operation.

Each controller has a synchronization view of the lower nodes of other controllers in addition to the lower nodes in its own area. If any controller fails, the node in its managed area will (pseudo-randomly) select one from other controllers as a replacement. If there is a large-scale access of the lower nodes, only the corresponding controller can be added to complete the expansion.

### 3.3 Lower Layer-Blockchain Layer

Our blockchain layer consensus protocol uses the Gossip protocol [17]. Gossip protocol, also known as epidemic protocol, is a protocol for information exchange between nodes or processes based on epidemic transmission. The working principle of the Gossip protocol can be understood as a node can randomly select several neighbors with him to synchronize information, and his neighbors will repeat this work until all nodes know the information. Therefore, the Gossip protocol has final consistency. The Gossip protocol has the characteristics of scalability, natural distributed fault tolerance, decentralization, and fast uniform convergence, and has been applied in many public chains and projects. But it also has its disadvantages. For example, because the coverage of the message needs to be spread gradually, the real-time performance is poor, which will lead to a certain message delay. There are also random selection characteristics of adjacent nodes, which will cause some nodes to receive the same message multiple times, resulting in certain communication redundancy.

In TBGP [10] proposed by Li et al., the random Gossip protocol is optimized. Using the federal learning, a tree-like blockchain network is constructed for the Gossip protocol, which structures the originally disordered network and reduces certain communication redundancy. However, in their work, there are great requirements for the computing power of power IoT nodes, and it is difficult to achieve large-scale popularization. Therefore, we consider that in the lower layer-blockchain layer using the Gossip protocol, only basic operations such as transaction dispersion, virtual voting, consensus synchronization, and block ordering of the blockchain network are performed. The part that needs to be calculated is transferred to the upper-controller layer, and the SDN controller is used to achieve more flexible and real-time topology control. In this way, it not only reduces the computing power demand for power IoT nodes, but also reduces the communication redundancy of the random Gossip protocol.

### 3.4 The Consumption Caused by Topology Control

In our architecture, although the redundancy caused by the Gossip protocol in the blockchain layer is reduced, a certain amount of redundant storage is required in the controller layer. Redundant storage in the controller is necessary to provide resilience and recoverability for the network and avoid network crashes caused by attacks or controller outages.

For the redundant storage part, there are many solutions, such as local / manual backup storage, cloud backup storage, etc. However, in our architecture, the controller layer mainly stores data related to the lower-blockchain, such as the list of nodes and their status, and the outbound / inbound connection of each node. These data are mainly composed of text arranged in simple tables, so the demand level is still low. If you need to



further strengthen the stability of the network, you can choose to add redundant servers in the controller layer, but the cost is relatively high, and the more redundant servers, the higher the cost.

## 4 Simulation Evaluation

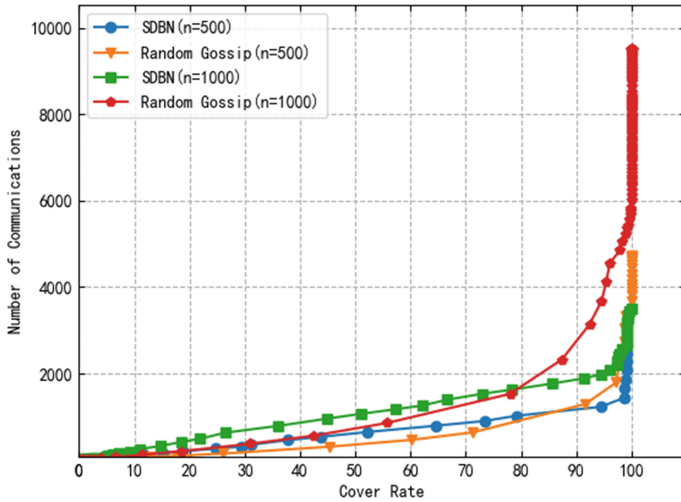
This section introduces the performance of the Gossip protocol under the proposed SDBN architecture and compares it with the performance of the Gossip protocol in the ordinary network environment. To facilitate the evaluation, we fixed the lower layer of the SDBN architecture as a triple tree topology. We use the multi-thread method to simulate the ordinary network environment composed of multiple nodes and the network environment of the triple tree topology. Intel (R) Core (TM) i7-10870H CPU @ 2.20GH x 10 virtual host, 16GB DDR4 memory, Ubuntu20.04LTS operating system. The software uses Golang 1.19.3 Linux/amd64 development environment. The experimental parameters are set as shown in Table 1.

**Table 1.** Experimental parameters.

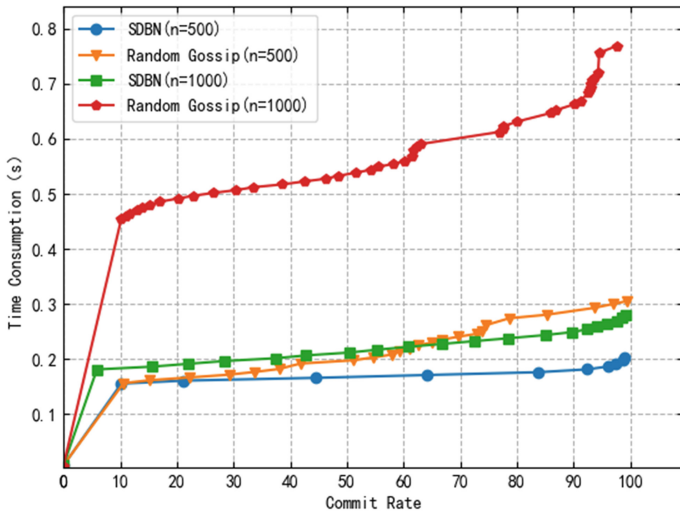
Experimental parameter	Value
Node id	0,1,2, n-1
Number of nodes	[500, 1000]
Min delay	10 ms
Max delay	20 ms
Crash rate of node	[0, 0.01]
Sampling frequency	[10 ms, 20 ms]

Communication delay is generally between the lowest delay and the highest delay. The node crash rate reflects the probability that the node is subjected to a DDoS attack, and this node refuses to respond to any message. Sampling frequency refers to the acquisition frequency of system performance characteristics, such as communication number, coverage, submission rate, time consumption, etc. Coverage refers to the ratio of the number of nodes receiving messages to the total number of nodes during sampling. The submission rate refers to the ratio of the number of synchronized nodes to the total number of nodes when the Gossip protocol submits the synchronization phase sampling.

As shown in Fig. 2, we compare the number of communications required by the Gossip protocol to cover the same proportion of nodes in the SDBN and ordinary network environments when the number of nodes is 500 and the number of nodes is 1000. It can be seen that when the number of nodes is 500, the number of communications required for Gossip protocol to cover all nodes in SDBN environment is only 59.4% of that in ordinary environment. When the number of nodes is extended to 1000, the value is only 58.3%. This shows that only fixing the communication topology of SDBN to a triple tree can effectively reduce the total communication overhead of the system and greatly reduce the communication redundancy generated by the Gossip protocol.



**Fig.2.** Comparing the number of communications required to cover the same proportion of nodes in SDBN and ordinary network environments.



**Fig. 3.** The proportion and total time of consensus confirmation nodes.

Figure 3 shows the total time required for the Gossip protocol to reach a consensus in the SDBN environment and the ordinary network environment. It can be seen that whether the number of nodes is 500 or 1000, or other cases of the same number of nodes, in the ordinary network environment, the Gossip protocol takes longer to reach a consensus. When the number of nodes increases from 500 to 1000, the consensus time also increases. The consensus time in the ordinary network environment increases by 46 ms, and the consensus time in the SDBN environment increases by 10 ms, which

is much lower than that in the ordinary network environment. Therefore, compared with the ordinary network environment, the environment provided by SDBN has lower communication redundancy, higher consensus efficiency and scalability.

## 5 Conclusion

This paper proposes a new architecture that uses SDN to provide topology control and optimize broadcast paths in consortium blockchain networks for grid information authentication. It solves the problem of communication redundancy and delay generated by Gossip protocol as a consensus mechanism in an consortium network environment. At the same time, the introduction of SDN not only solves the problem of insufficient node computing power caused by federated learning in DABG [10], but also strengthens the flexibility, stability and scalability of the network, which is more suitable for the use of the power IoT with insufficient resources. The simulation results show that compared with the ordinary environment, the communication redundancy and delay generated by the Gossip protocol is greatly reduced in the SDBN environment, which improves the transaction efficiency of the blockchain system.

## 6 Future Work

In future work, we will focus on the control and combination of SDN and blockchain networks for grid information authentication, not limited to fixed topologies. We will consider its modeling analysis, find the most suitable topology, study the dynamic control of SDN on the consortium blockchain network topology, and further improve the performance of the consortium blockchain. In addition, we will try to enhance the response speed of SDN for consortium blockchain faulty nodes and enhance the stability of the network.

**Acknowledgment.** This work is supported by State Grid Shandong Electric Power Company Science and Technology Project: “Research on Smart Grid 5G Edge Business Orchestration and Secondary Authentication Technology” (No. 520614220002).

## References

1. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system[R]. (2008–05–19) [2020–08–19]
2. Jiang, T., Fang, H., Wang, H.: Blockchain-based internet of vehicles: distributed network architecture and performance analysis. *IEEE Internet Things J.* **6**(3), 4640–4649 (2018)
3. Mollah, M.B., et al.: Blockchain for future smart grid: a comprehensive survey. *IEEE Internet Things J.* **8**(1), 18–43 (2020)
4. Uddin, M., Salah, K., Jayaraman, R., Pesic, S., Ellahham, S.: Blockchain for drug traceability: architectures and open challenges. *Health Inf. J.* **27**(2), 14604582211011228 (2021)
5. Dongyan, H., Lang, L., Bin, C., Bo, W.: Rbft: Byzantine faulttolerant consensus mechanism based on raft cluster. *J. Commun.* **42**(03), 209–219 (2021)

6. Saad, A., Park, S.Y.: Decentralized directed acyclic graph based DLT network. In: Proceedings of International Conference on Omni-Layer Intelligent Systems, pp. 158–163. IEEE Press, Washington D.C., USA (2019)
7. Fu, X., Wang, H.M., Shi, P.C., et al.: Teegraph: trusted execution environment and directed acyclic graph-based consensus algorithm for IoT blockchains. *Sci. China Inf. Sci.* **65**(3), 1–3 (2021)
8. Musungate, B.N., Candan, B., Abuk, U.C.C., Dalkılıç, G.: Sidechains: Highlights and challenges. In: 2019 Innovations in Intelligent Systems and Applications Conference (ASYU), pp. 1–5. IEEE (2019)
9. Kreutz, D., Ramos, F.M., Verissimo, P.E., Rothenberg, C.E., Azodolmolky, S., Uhlig, S.: Software-defined networking: a comprehensive survey. *Proc. IEEE* **103**(1), 14–76 (2014)
10. Li, L., Huang, D., Zhang, C.: An efficient DAG blockchain architecture for IoT. *IEEE Internet Things J.* **10**(2), 1286–1296 (2022)
11. Rathore, S., Kwon, B.W., Park, J.H.: BlockSecIoTNet: blockchain-based decentralized security architecture for IoT network. *J. Netw. Comput. Appl.* **143**, 167–177 (2019)
12. Gao, J., Agyekum, K.O.B.O., Sifah, E.B., et al.: A blockchain-SDN-enabled Internet of vehicles environment for fog computing and 5G networks. *IEEE Internet Things J.* **7**(5), 4278–4291 (2019)
13. Sharma, P.K., Singh, S., Jeong, Y.S., et al.: Distblocknet: a distributed blockchains-based secure sdn architecture for iot networks. *IEEE Commun. Mag.* **55**(9), 78–85 (2017)
14. Deshpande, V., Badis, H., George, L.: Efficient topology control of blockchain peer to peer network based on SDN paradigm. *Peer-to-Peer Netw. Appl.* **15**(1), 267–289 (2022)
15. Hao, W., Zeng, J., Dai, X., et al.: Towards a trust-enhanced blockchain P2P topology for enabling fast and reliable broadcast. *IEEE Trans. Netw. Serv. Manage.* **17**(2), 904–917 (2020)
16. Ongaro, D., Ousterhout, J.: In search of an understandable consensus algorithm. In: 2014 USENIX Annual Technical Conference (USENIX ATC 14), pp. 305–319 (2014)
17. Demers, A., Greene, D., Hauser, C., Irish, W., Larson, J., Shenker, S., Sturgis, H., Swinehart, D., Terry, D.: Epidemic algorithms for replicated database maintenance. In Proceedings of the Sixth annual ACM Symposium on Principles of Distributed Computing, pp. 1–12 (1987)



# Snowflake Anonymous Network Traffic Identification

Yuying Wang, Guilong Yang, Dawei Xu<sup>(✉)</sup>, Cheng Dai, Tianxin Chen,  
and Yunfan Yang

College of Cybersecurity, Changchun University, Changchun, China  
xudw@ccu.edu.cn

**Abstract.** Tor, as a widely used anonymous communication system, is frequently employed by some users for illegal activities. Snowflake server as a plugin that enables users to connecting to the Tor network, allowing users to evade surveillance by connecting to the Tor network through it. Since Snowflake hides user traffic within regular WebRTC, it becomes challenging for authorities to differentiate and regulate, posing significant difficulties in monitoring efforts. To address these issues, this paper proposes a feature extraction method based on traffic statistical characteristics and a Snowflake traffic identification model based on MLP. We collected traffic datasets in Docker environment, extracted variable-length DTLS handshake sequences, and employed the feature extraction method to extract their statistical characteristics, including packet length, session duration, and average time between sending two packets, among other features. The MLP-based Snowflake traffic identification model can determine whether the traffic belongs to the target traffic based on these features. Moreover, this method can accurately identify traffic even when the traffic fields change. Experimental results demonstrate that this method achieves a 99.83% accuracy rate in identifying Snowflake traffic. Additionally, even when the data distribution in the dataset is altered, although the method requires more training iterations, it still achieves a 99.67% accuracy rate.

**Keywords:** Anonymous communication · Tor network · Traffic identification · MLP · Deep learning

## 1 Background

With the rapid development of the Internet, people's awareness of privacy protection has grown stronger. Various anonymous communication systems have become increasingly popular. According to the CNNIC report on March 2, 2023, as of December 2022, China's online population reached 1.067 billion, with an Internet penetration rate of 75.6%, surpassing over half of the country's population. With such a large user base, anonymous communication systems are often abused by some malicious users, leading to serious cybersecurity incidents [1]. As the most widely anonymous communication system, the Tor system allows users to anonymously access various websites through three-hop relays, without being detected by service providers or intermediaries. The

Tor network has millions of users, and some individuals exploit its anonymity for illicit activities such as drug and firearm trafficking. Researchers have employed traffic identification techniques to identify Tor traffic and block it. In response, the Tor development team introduced Pluggable Transport (PT) [2] technology, which utilizes clients with special protocols as the first hop in the relay chain. These protocols can hide special traffic within normal traffic, making it difficult for censors to discern. Among the most widely used are Obfs4, Meek, and Snowflake. Snowflake primarily evades censorship by concealing traffic within the data channel of WebRTC [3]. WebRTC utilizes DTLS [4] as the underlying protocol for data transmission. Being a widely adopted audio and video technology, WebRTC poses significant challenges to censorship efforts. This paper focuses on identifying the DTLS handshake process within WebRTC. It collects target traffic within Docker environment and employs a feature extraction method based on traffic statistical characteristics to extract features. Finally, a Snowflake traffic identification model based on Multi-Layer Perceptron (MLP) is utilized to determine whether the traffic belongs to the target traffic. If it does, the censoring authority can choose to block the traffic; if not, the traffic is allowed to pass through.

## 2 Related Research

Snowflake [5] is currently one of the most widely used PTs. David et al. [6] conducted a study by collecting a significant amount of application traffic that utilizes WebRTC communication. They manually analyzed the differences between these traffic samples and identified the potential to recognize Snowflake based on certain fields. Additionally, they highlighted the use of WebRTC as a means to evade censorship. Kyle MacMillan et al. [7] conducted a study to evaluate the recognizability of Snowflake. By collecting multiple application traffic samples that utilize WebRTC technology at the underlying level, they analyzed the interaction packets and protocol fields during the DTLS handshake phase. The researchers proposed a method to identify Snowflake traffic based on the DTLS handshake fields. Building upon the research conducted by MacMillan et al., Chen et al. [8] expanded their dataset and proposed a framework for Snowflake traffic identification. This framework utilizes rule matching and DTLS fingerprinting to determine whether user traffic is accessing the Tor network and further classify whether the user is accessing hidden services within the Tor network.

The earlier research primarily focused on the data transmission phase of Snowflake, where WebRTC utilizes the DTLS protocol for initial connection establishment. By extracting specific fields from the protocol and transforming them into features, machine learning algorithms were employed to identify and differentiate between normal WebRTC traffic and abnormal traffic. They primarily focused on the fixed data packets in the DTLS handshake, specifically the Client Hello and Server Hello. However, this approach faces a significant challenge when Snowflake modifies these fields to make them identical to normal WebRTC fields. In such cases, it becomes difficult to distinguish between the two using this method.

### 3 The Fundamental Principles of Snowflake

As a pluggable transport plugin in Tor, Snowflake operates differently from the original Tor network. In the Tor-Meek plugin, the client primarily utilizes a technique called domain fronting [9]. It involves initially connecting to a Content Delivery Network (CDN) provider that supports this technique. The CDN provider then forwards all of the client’s traffic to the next hop node. In this scenario, all client traffic accessing the anonymous system needs to be relayed through the CDN provider, resulting in significant bandwidth overhead.

Snowflake as a new PT consists of the following components, as illustrated in Fig. 1 of the system architecture. The client will first send a proxy request to the broker, and then the broker will create an SDP answer containing information about the proxy and respond to the client. At this point, the client will directly connect to the proxy. When the proxy receives a connection from the client, it first checks if the received request is legitimate, meaning it matches the information it previously sent to the broker. If the information matches, the proxy accepts the client’s connection. The client initiates the DTLS handshake by sending the necessary information to generate a session key. Once the key is generated, both the client and the proxy use it to exchange messages over the WebRTC data channel.

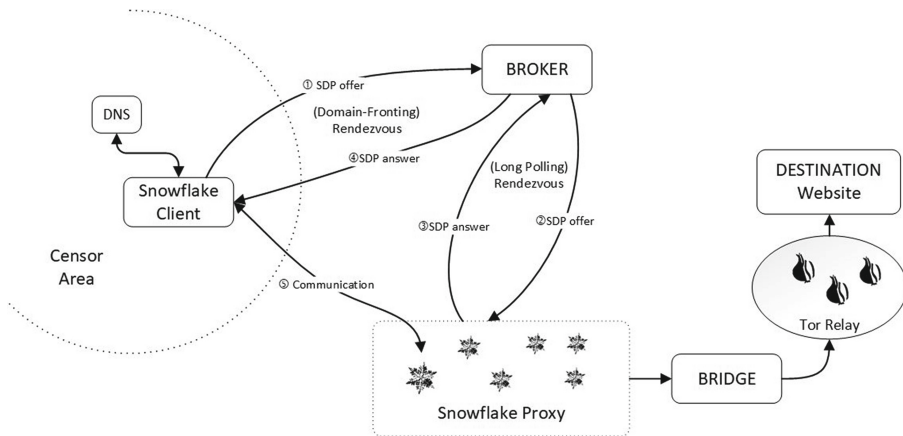


Fig. 1. Snowflake system architecture diagram.

## 4 MLP-Based Snowflake Traffic Identification

### 4.1 Feature Extraction

This paper proposes a method of feature extraction from variable-length traffic sequences using traffic statistical features, primarily based on session-level traffic. Each session-level traffic can be represented as:

$$X_n = \{x_1, x_2, x_3, \dots, x_k\} \tag{1}$$

here,  $x_k$  represents a UDP packet, and  $X_n$  represents all communication traffic between a server and a client, with bidirectional direction.

Since this study focuses on identifying target traffic based on the handshake traffic features between the client and the proxy in WebRTC, the first step is to ensure the complete collection of all handshake traffic. The underlying protocol used for data transmission in WebRTC is DTLS. In a normal DTLS handshake protocol, the client first sends a Client Hello request to the proxy. The proxy then responds with a Server Hello, including its authentication information, such as its public key. After receiving the authentication information from the proxy, the client uses the received public key to encrypt the subsequent information and sends a request. Upon receiving the request, the proxy responds with another data packet. From there, the client can engage in regular encrypted communication with the proxy. This communication process is similar to the communication process in TLS. Under normal circumstances, the handshake traffic between the client and the proxy can be completed with only four data packets. However, due to the diversity of network environments and the use of UDP protocol at the underlying level, which does not guarantee transmission quality, in practical network scenarios, multiple retransmissions are often required. Therefore, capturing only the first four packets of the transmission phase is far from sufficient. It is necessary to capture variable-length traffic sequences from the transmission flow, which can be represented as follows:

$$S_k = \{x_1, x_2, x_3, \dots, x_i\} \quad (2)$$

$x_i$  represents a DTLS handshake data packet, and  $S_k$  represents all the DTLS handshake data packets.

After technical analysis and comparing a large number of data packets, it was determined that when the payload data of the first packet in UDP is 22, the current traffic corresponds to handshake traffic. The traffic that matches this feature is extracted and merged for further feature extraction.

In the traffic feature extraction section, this study primarily analyzes the target traffic using statistical methods. In this regard, we utilized the CICFlowMeter, a feature extraction software, and made certain modifications to it. This software is capable of extracting features from both TCP and UDP traffic. However, in our study, WebRTC utilizes only UDP packets. Therefore, we removed the TCP functionality from the software and incorporated the standard deviation of packet lengths, denoted as:

$$PLS = \sqrt{\frac{\sum_{i=0}^n (Li - \frac{\sum_{i=0}^n Li/n)^2}{N}}{N}} \quad (3)$$

where  $Li$  represents the length of an individual packet and  $N$  represents the number of packets, this feature represents the magnitude of variations in packet sizes during a session. The average length feature of the packets is represented as:

$$PLM = \frac{\sum_{i=0}^n Li}{N} \quad (4)$$

The average time feature between the forward transmission of two packets is represented as:

$$FIM = \frac{\sum_{i=0}^n (T_{i+1} - T_i)}{N} \quad (5)$$



where  $T_i$  represents the time at which the current packet is sent, and  $N$  represents the number of packets. This feature represents the speed of information exchange between the two parties in the session. Additionally, there are other less important features such as data statistics in the reverse flow and session duration, which are not listed here in detail.

Due to the issue of packet retransmission caused by network conditions, we have added the feature of the number of retransmitted packets. This feature can be used to indicate the quality of the network link. If the value is high, it suggests the presence of blocking nodes in the link. The feature extraction algorithm is shown in Table 1. After extracting features from DTLS session traffic, focusing on aspects such as packet size and average transmission rate, a total of 48 flow statistical features are obtained, which can be used for subsequent model training.

**Table 1.** Retransmission packet calculation.

---

**Algorithm 1:** Number characteristic of retransmitted packets

---

**Input:** Session sequence

**Output:** Number of retransmission packets

```

number = 0
packets = []
for packet in sessions:
    if packet in packets:
        number += 1
    else:
        packets.append(packet)

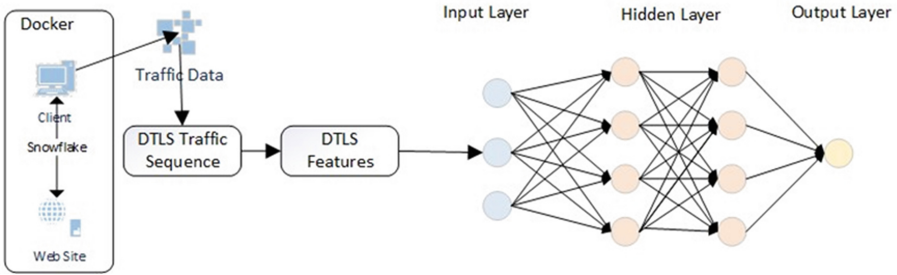
```

---

## 4.2 Model Introduction

Firstly, we need to preprocess the data by normalizing the data. The overall architecture of the model is illustrated in Fig. 2. The first layer is the input layer, which consists of 48 neurons. After preprocessing the data, the dimensionality of the feature vector is 48. The second layer consists of 512 neurons. The input vector dimension is 48, and the output vector dimension is 512. The third layer consists of 64 neurons. The input vector dimension is 512, and the output vector dimension is 64. The fourth layer consists of a single neuron. It is followed by a Sigmoid function. After applying the Sigmoid function, the final output is mapped to the range [0, 1], representing the probability of the input being the target traffic. When the output probability is greater than 0.5, the model classifies the traffic as Snowflake traffic. If the probability is less than 0.5, the traffic is classified as normal WebRTC traffic.

The loss function used in this case is BCELoss, which stands for Binary Cross Entropy Loss. It is a commonly used loss function for binary classification tasks. It measures the difference between the model’s output and the true labels. There are many



**Fig. 2.** Model architecture diagram.

optimization functions available, we have opted to use the Adam algorithm. Adam is an adaptive optimization algorithm that adjusts the learning rate for each parameter. It allows parameters with smaller gradients to have larger learning rates, while parameters with larger gradients have smaller learning rates. This helps improve training efficiency and speed.

## 5 Experiment

### 5.1 Collection and Processing of Traffic

Since Docker provides a closed environment and allows images to be saved in the cloud for easy distribution, the experiments in this study were primarily conducted using Docker. The base image used for the experiments was Ubuntu 20.

The first step is to download the base image and instantiate a container from it. Inside the container, you will install the Python environment, Scapy, and Selenium libraries. Then, you'll install a headless browser that does not require a graphical interface. Next, you'll install the Tor software and Snowflake. Since Snowflake is written in Go, you'll need to install the Go compiler first in order to run the client. Write a script that first uses the Scapy library to listen to the network traffic on a specific network interface. Then, use the Selenium library to write an automation script that allows the browser to visit certain websites automatically. Specify that the traffic should pass through a designated Snowflake proxy port. Finally, when the client enters the anonymous communication network through the proxy, establish a three-hop circuit to access random websites and generate traffic. After the visit, automatically save the traffic data based on the date. To streamline the process and reduce manual efforts, we utilize the Cron software to schedule the program for daily execution. The image can be found at [xinbigworld/ubuntu:1.2](https://github.com/xinbigworld/ubuntu:1.2). Once the image is downloaded, it can be directly run to obtain the aforementioned container environment.

After running the program on two servers for a certain period of time, we consolidate all the Pcap files and merge them into a single file. We then utilize a feature extraction method based on traffic statistics to extract features from the traffic. The extracted features are directly saved to a text file for easy access during the subsequent model training.

By leveraging data from previous papers and combining it with the traffic collected in our Docker environment, we obtained a dataset of size 6477. In this dataset, Snowflake

represents the target traffic, while the traffic collected from the other three software represents normal traffic. Our goal is to achieve high accuracy in identifying the target traffic within this dataset. The distribution of the collected traffic data is shown in Table 2.

**Table 2.** Dataset distribution.

	Snowflake	Facebook messenger	Google hangouts	Discord
Sessions	1386	1584	1539	1968

The term Sessions represents a complete conversation between the client and the server, encompassing bidirectional traffic. It includes the traffic sent from the client to the server as well as the traffic sent back from the server to the client. For example, 1386 indicates that the traffic collection program was executed 1386 times, resulting in the collection of 1386 instances of DTLS handshake information.

The proposed method was utilized to extract DTLS handshake data from a large volume of traffic. The experiments were conducted on a personal computer with an Intel i5-12500H 3.1GHz CPU and 16GB of RAM. Experimental results show that extracting handshake data from a session of length 1383 takes approximately 11ms, with complete packet content including all DTLS handshake information. This demonstrates the feasibility of the proposed method in terms of both efficiency and accuracy. In terms of feature extraction, experiments conducted on a session sequence of length 192 took a total of 381ms for feature extraction.

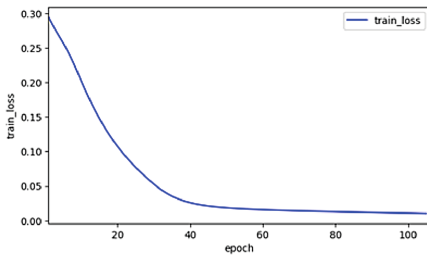
## 5.2 MLP Model Training

The dataset is divided into training and testing sets in a 7:3 ratio. The training set is used to train the model by updating its parameters to establish a classification model. The testing set is used to evaluate the performance of the model and assess its discriminatory power. In this section, we will use accuracy as a metric to measure the model performance.

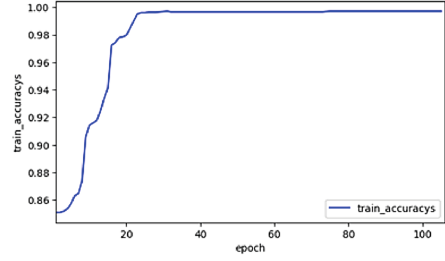
As shown in Fig. 3a, the loss value of the model keeps decreasing as the number of training iterations increases. After 40 training iterations, the loss value reaches a plateau and shows little further improvement. From Fig. 3b, it can be observed that the accuracy of the model on the training set reaches its highest value after 25 training iterations, which is 99.72% for the subsequent iterations. From Fig. 3c, it can be observed that the training performance on the testing set is similar to that on the training set. Both achieve the highest accuracy of 99.83% after 25 training iterations and show little improvement thereafter. This experiment confirms that the proposed method of feature extraction based on flow statistics and the MLP-based Snowflake traffic identification model can effectively recognize the target traffic.

## 5.3 Model Comparison

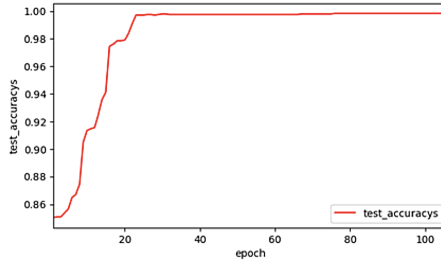
We trained four different models using the same dataset, which was divided into training and testing sets in a 7:3 ratio. We also introduced three additional performance metrics



(a) The loss value of the model



(b) The accuracy of the model on the training set



(c) The accuracy of the model on the test set

**Fig. 3.** Training and evaluation of models.

to evaluate the models. Among them, precision represents the proportion of correct predictions among all positive predictions. Recall represents the proportion of correct predictions among all positive instances. F-score primarily balances precision and recall. The final results are shown in Table 3. From the table, we can see that, in terms of Accuracy, all models except RF achieve relatively high values. However, in terms of precision, MLP significantly outperforms the other models, indicating that the predicted target traffic consists mostly of true target traffic. SVM is able to recall all positive samples in terms of recall, but due to its lower precision, it indicates that there will be a certain number of negative samples predicted as positive, resulting in a higher rate of false positives. In summary, the MLP model demonstrates excellent performance in all aspects of Snowflake traffic identification. Therefore, choosing the MLP model for identifying target traffic is more suitable.

**Table 3.** Model performance comparison

Classifier	Accuracy	Precision	Recall	F1
SVM	0.9855	0.9115	1.0	0.9537
Random Forest	0.9586	0.7892	0.9640	0.8679
MLP	0.9983	0.9916	0.9972	0.9944
Naive Bayes	0.9838	0.9078	0.9925	0.9483

### 5.4 Comparison of the Importance of Traffic Statistical Features

In the experiment, we can use Random Forest (RF) to rank the importance of features and obtain their weights, as shown in Fig. 4. We can observe that the most important feature accounts for 27% of the weight, representing the total time between two forward packets. The second feature occupies 22% of the weight, representing the average length of packets throughout the entire conversation. The third feature represents the duration of the session, i.e., the total time spent by the client and server on DTLS. The cumulative importance of the top three features reaches around 50%. This method involves collecting session packets during the DTLS handshake and extracting statistical features from these packets. Compared to the research presented in the second section, where they directly compare specific fields of the protocol, our method exhibits better robustness. When the protocol fields of the traffic are altered, their method may not achieve the same high accuracy. However, since our method does not rely on using protocol fields as features, it can still effectively identify the target traffic even if the protocol fields are changed.

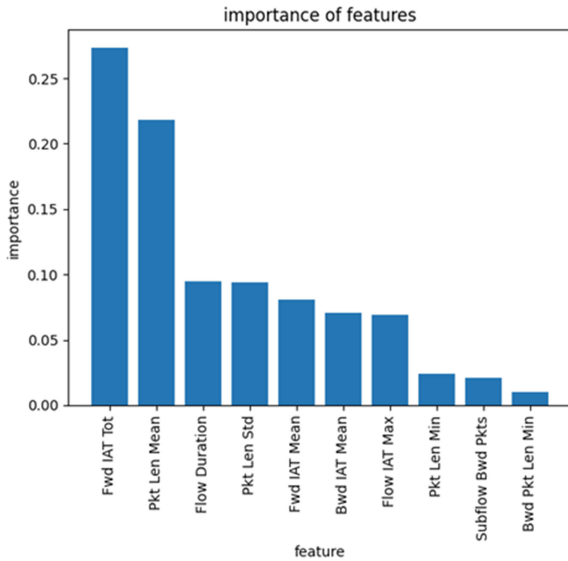


Fig. 4. Feature importance.

### 5.5 The Impact of Data Distribution on Model Performance

As shown in Fig. 5, by varying the proportion of target traffic in the dataset, we simulate the data distribution in real-world scenarios. For example, a ratio of 5:1 represents the size comparison between normal traffic and target traffic datasets. We can observe that the proposed feature extraction method and model still have a high probability of feasibility in real scenarios, achieving an accuracy of 99.67%.

From the figure, we can observe that when the proportion of target traffic in the dataset is higher, the model does not initially achieve a high accuracy. This is because

the dataset is larger, and the model needs multiple iterations to learn the characteristics of the traffic. On the other hand, when the proportion of target traffic decreases in the dataset, although the model initially achieves a high accuracy, it requires more training iterations to reach an accuracy of 99.67%.

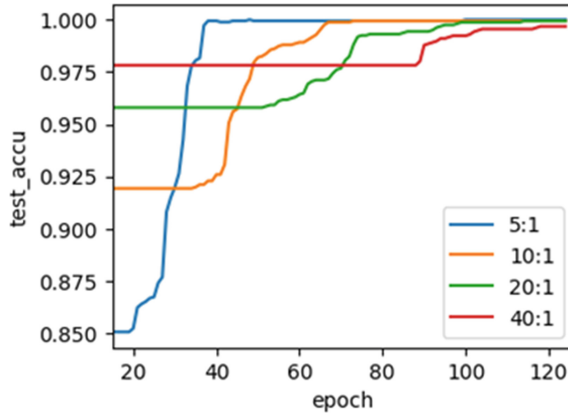


Fig. 5. Target traffic identification with different proportions.

## 6 Conclusion

Many users employ the Tor anonymous communication system to conceal their online activities for the purpose of engaging in illegal activities. While there are numerous methods to identify raw Tor traffic, the difficulty of traffic identification has increased significantly with the use of Tor PT technology, particularly the adoption of Snowflake. In this study, we extract 48 statistical features from DTLS traffic using a flow-based statistical feature extraction method. These features are preprocessed to obtain properly formatted input features in accordance with established standards. The extracted feature data is fed into an MLP model, which can ultimately determine whether the traffic belongs to the target flow. Even if certain fields in the traffic change, this method can still function properly because it primarily relies on the statistical features of the traffic for classification, and changes in protocol fields do not affect its recognition accuracy. Traffic identification is a dynamic process, and as we identify traffic features, Snowflake developers may modify these features to render our model ineffective. This could lead to an ongoing cat-and-mouse situation. It is necessary to continually collect traffic data to maintain a high level of accuracy. In the future, we hope to automate this process to adapt to updates and changes in Snowflake versions.

## References

1. Yannikos, Y., Heeger, J., Steinebach, M.: Scraping and analyzing data of a large darknet marketplace. *J. Cyber Secur. Mob.* 161–186 (2023)
2. Shahbar, K., Zincir-Heywood, A.N.: Traffic flow analysis of tor pluggable transports. In: 2015 11th International Conference on Network and Service Management, pp. 178–181 (2015)
3. Sredojev, B., Samardzija, D., Posarac, D.: WebRTC technology overview and signaling solution design and implementation. In: 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics, pp. 1006–1009 (2015)
4. Shaheen, S.H., Yousaf, M.: Security analysis of dtls structure and its application to secure multicast communication. In: 2014 12th International Conference on Frontiers of Information Technology, pp. 165–168 (2014)
5. The Snowflake, <https://trac.torproject.org/projects/tor/wiki/doc/Snowflake>, last accessed 2023/4/24
6. Fifield, D., Epner, M.G.: Fingerprintability of WebRTC. arXiv preprint arXiv:1605.08805 (2016)
7. MacMillan, K., Holland, J., Mittal, P.: Evaluating snowflake as an indistinguishable censorship circumvention tool. arXiv preprint arXiv:2008.03254 (2020)
8. Chen, J., Cheng, G., Mei, H.: F-ACCUMUL: a protocol fingerprint and accumulative payload length sample-based tor-snowflake traffic-identifying framework. *Appl. Sci.* **13**(1), 622 (2023)
9. Fifield, D., Lan, C., Hynes, R., Wegmann, P., Paxson, V.: Blocking-resistant communication through domain fronting. *Proc. Priv. Enhanc. Technol* **2015**(2), 46–64 (2015)



# Privacy Attacks and Defenses in Machine Learning: A Survey

Wei Liu<sup>1</sup>, Xun Han<sup>2(✉)</sup>, and Meiling He<sup>3</sup>

<sup>1</sup> City University of Macau, Macau, China

<sup>2</sup> Intelligent Policing Key Laboratory of Sichuan Province, Luzhou 646000, Sichuan, China

hldwxhx@163.com

<sup>3</sup> School of Automotive and Traffic Engineering, Jiangsu University, Zhenjiang 212013, Jiangsu, China

hemeiling@ujs.edu.cn

**Abstract.** As machine learning has gradually become an important technology in the field of artificial intelligence, its development is also facing challenges in terms of privacy. This article aims to summarize the attack methods and defense strategies for machine learning models in recent years. Attack methods include embedding inversion attack, attribute inference attack, membership inference attack and model extraction attack, etc. Defense measures include but are not limited to homomorphic encryption, adversarial training, differential privacy, secure multi-party computation, etc., focusing on the analysis of privacy protection issues in machine learning, and providing certain references and references for related research.

**Keywords:** Machine learning model · Means of attack · Defense strategy

## 1 Introduction

This chapter will briefly sort out the background knowledge of machine learning and privacy leakage, and explain the research significance of this paper, as well as the difficulties and challenges in this research direction

### 1.1 Related Work

In the era of big data, massive amounts of information have promoted the development of machine learning, and now it has been widely used in malicious detection (see [33, 37]), computer vision (see [32, 49]), voice command recognition (see [46, 48]), driving system (see [10, 47]), recommendation system (see [36, 56]), medical diagnosis (see [3, 13]) and many other fields. Machine learning can discover patterns and laws from massive data, and apply this knowledge to different tasks, bringing great convenience and benefits to humans. Especially after the



breakthrough development of technologies such as deep learning in [41] and reinforcement learning in [31], it has provided strong support for the application of machine learning in the above fields, and even some performances have been better than humans. In the past, there has been a lot of research work on privacy protection measures in machine learning. Many workers have evaluated and summarized the existing attack and defense work. Reference [5] studies the attack model of machine learning, and uses a Statistical spam classification as an example, and an in-depth analysis is carried out. Reference [2] took cleaning robots as an example to summarize and analyze the problems that may exist in the real work and life of human beings. Reference [4] use a black-box model and a white-box model to conduct targeted research on machine learning adversarial attacks and poisoning attacks. Although Ref. [34] is an article on computer security A comprehensive overview of threats, but it also summarizes some of the content related to machine learning. Reference [35] focuses on the training and prediction phases of the machine learning life cycle. Reference [1] focuses on It is a security issue in the field of computer vision. Reference [18] is based on the machine learning CIA model to investigate and summarize.

This article first explains the development of machine learning and privacy leakage, and then from privacy leakage, attack methods. The three angles of model security systematically and scientifically summarize the existing machine learning attack methods and defense methods, and discuss the limitations of related research. Finally, discuss the challenges faced by machine learning model security and privacy research and Feasible research directions in the future, mainly including contributions

1. Conduct a comprehensive and systematic analysis and summary of attack methods and defense technologies in recent years
2. Present the possible attacks and defense measures of machine learning through the combination of charts, and introduce typical attacks and defense methods
3. According to the characteristics and current situation of machine learning, this paper proposes a multi-faceted summary and outlook.

## 2 Machine Learning Model

The machine learning model in Ref. [30] is a data-driven predictive model, which discovers the relationship and regularity between variables by training the model on a large amount of data, and realizes the prediction or classification of future data.

### 2.1 Model Introduction

This paper uses the Amazon Machine Learning (Amazon ML) model in Ref. [45]. Amazon Machine Learning is a machine learning service provided by Amazon, which aims to help users quickly build and deploy high-quality machine learning models. It provides a series of easy-to-use APIs and tools that enable users to

quickly build, train and test models without requiring extensive machine learning expertise. And it supports a variety of machine learning models, including linear regression, logistic regression, decision trees, support vector machines, and random forests.

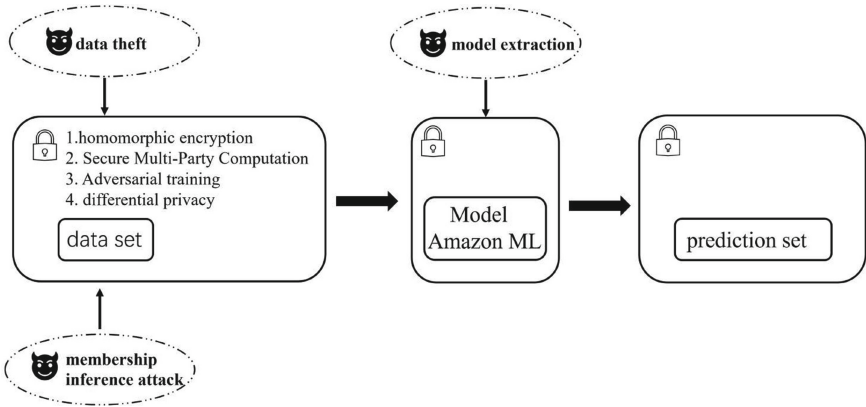


Fig. 1. Machine learning model

### 3 Privacy Leakage

This chapter will briefly explain the background knowledge about privacy leakage. Privacy leakage has always been an important field of machine learning research.

#### 3.1 Background Knowledge on Privacy Leakage

In machine learning, due to specific scenario requirements, its model design is biased towards efficient and accurate prediction output, rather than the ability of the model to resist attacks. Therefore, in the actual application of the model, there will be malicious users attacking various stages of the life cycle of the machine learning model. During the attack process, the risk caused by privacy leakage is particularly prominent.

This paper mainly focuses on attack vectors for data privacy. Most attackers are more inclined to obtain private data of unspecified people, and have developed more attack methods. Therefore, this paper introduces three data-targeted attack methods, involving multiple aspects such as data training, input, and prediction. At the same time, the attack on model privacy is also mainly reflected in the extraction of the model. Regardless of the purpose of the attacker, the leakage of these data will cause considerable damage to the data owner. Therefore, both providers and users of machine learning models should pay more attention to privacy protection and continuously improve their ability to resist attacks.

## 4 Attack Methods That Cause Privacy Leakage

Vulnerabilities in machine learning model algorithms and implementations lead to security risks such as data leakage and loss of model structural parameters. This chapter will introduce three attack methods targeting model data and one attack method targeting the model itself.

### 4.1 Attack Methods Targeting Model Data

Model data is the basis of machine learning models. Model data includes training data, model input and output, etc. Some training data sets that involve privacy, such as shopping records, hospital records, etc., are also related to the issue of personal privacy protection. The following describes three attack methods against machine learning model data.

**4.1.1 Embedding Inversion Attack** Embedding Inversion Attack, also known as embedded inversion attack [14], is an attack method for deep learning semantic embedding models. This attack is often used to infer input text from pre-trained neural language models. In natural language processing, embedding refers to embedding words or phrases into a real vector space using a small fixed-length representation. In text classification tasks, the input text sequence needs to be converted into a sequence of numbers. To do this, word embedding methods can be used to map each word into a vector space of low-dimensional vectors. In this way, a sentence or paragraph can be represented as a matrix of word vectors. This matrix will be fed into a neural network for text classification. At the same time, this matrix can be used as one of the inputs of the deep learning model, and the embedding vector can be used as the context and passed to the neural network for classification, regression and other tasks.

**4.1.2 Attribute Inference Attack** Attribute Inference Attack (see [19,55]) aims to infer private attributes in training data from machine learning models. Attackers do not need to directly access protected personal data, but instead gain private information about personal data by analyzing deployed machine learning models.

**4.1.3 Membership Inference Attack** Member Inference Attack is a privacy attack in machine learning [15,28,38,44,51], which aims to determine whether a given input belongs to the data set by accessing the protected training data set, that is, whether there are members in the data set identity. Membership inference attacks are based on two assumptions, one is that the model is knowable, and the other is that the attacker has access to some sample labels (that is, having membership and corresponding labels in the data set). Then, the attacker specifies some input data and guesses whether it belongs to a specific member in the dataset by tracking the model output.

## 4.2 The Target Is the Attack Method of the Model Itself

There are also attack methods for machine learning models. Attackers can obtain information related to the model by calling APIs related to the machine learning model, and can even disguise or embezzle the model to achieve the purpose of stealing private data.

**4.2.1 Attack Overview** Among them, Model Extraction Attack, [12, 39, 52] has been studied for simple classification tasks, vision tasks, NLP tasks, etc. Typically, model extraction attacks aim to reconstruct a local copy or steal the functionality of a black-box API. If the extraction is successful, the attacker has effectively stolen the intellectual property, i.e. the full details of the model. The work of this attack method mainly focuses on how to imitate a model with performance close to the victim API in the source domain, and a more powerful attacker may even extract a better model than the target victim API [16].

Attackers use this technique to steal model knowledge by accessing the model and its output to deduce sensitive information of the target model. The reason why this attack technique is called model extraction attack is because the attacker can replace the attacked model with a model constructed by himself, and can output the corresponding label in a way consistent with the original model [50].

## 5 Defense Measures Against Privacy Leakage

This chapter will introduce four commonly used schemes in privacy protection, namely homomorphic encryption, secure multi-party computation, confrontation training, and differential privacy.

### 5.1 Homomorphic Encryption

Homomorphic Encryption (HE) refers to satisfying the original file through a specific homomorphic encryption algorithm, the encrypted ciphertext can satisfy the property of homomorphic operation, and the final ciphertext operation result is equivalent to the corresponding homomorphic decryption. The result of performing the same operation directly on the subsequent plaintext can realize the “countable and invisible” data. In the cryptographic system, homomorphic encryption is usually based on computational problems in mathematics, including but not limited to integer decomposition problems, discrete logarithm problems, Determining the remainder of composite numbers, the approximate greatest common factor problem [7, 17, 40], etc.

### 5.2 Secure Multi-party Computation

Secure Multi-Party Computation [6, 11] was proposed by Professor Yao Qizhi, an academician of the Chinese Academy of Sciences, in 1982. For model training,

secure multi-party computation requires the use of cryptographic tools, such as secret sharing [20,21], zero-knowledge proof [26,27], oblivious transmission [8,54], obfuscation circuits [42,53], and in centralized machine learning, secure multi-party The calculation is performed on two non-collusive servers through secret sharing, and the scheme can be extended to the scene of hundreds of users, followed by a large amount of communication overhead . The difference is that the secure multi-party computing scheme based on obfuscated circuit technology can generally only be applied to two to three parties to complete model training. In the joint machine learning model, homomorphic encryption or zero-knowledge proof is more commonly used.

### 5.3 Adversarial Training

Adversarial training [24,25,29] is a defense method in machine learning that aims to improve the resistance of deep neural networks to adversarial attacks. By injecting some perturbations into the original data, the machine learning model is made more robust, thereby reducing the impact of attacks on model data and structural parameters. The method mainly includes the following steps: First, generate adversarial samples. First, some attack algorithm needs to be used to generate adversarial samples and added to the normal training data set to form a new training set. The second is to train the model. The model is retrained using a new training set with adversarial samples in order to enhance the tolerance of the model against noise and improve the robustness of the model. And finally the test model. After the training is completed, the test set is evaluated. If the model shows better robustness, it will have a better ability to deal with raw data and adversarial input than the normal model. If expectations are not met, repeat the first two steps until you are satisfied.

### 5.4 Differential Privacy

Differential privacy is a data protection algorithm with strict mathematical definition and privacy quantification. By perturbing the data, such as adding noise, the attacker cannot deduce the original data, thereby achieving data privacy protection and avoiding the complete destruction of the original data. To ensure the availability of perturbed data . Nowadays, differential privacy technology can be divided into centralized differential privacy [9,23] and localized differential privacy [22,43] according to the processing subject. Among them, centralized differential privacy processes data by a trusted third party, while localized differential privacy The data is privately processed locally by the user, and the more mainstream method is localized differential privacy.

## 6 Summary and Outlook

This article introduces the leakage risks and defenses of machine learning models, describes four attack methods and introduces four defense measures. It can be seen that whether it is aimed at the model training data or the attack method against the model itself, it is applicable to most of today's machine learning models. It can be seen that these models have a certain risk of leakage. With the deepening of machine learning and artificial intelligence research, the application of machine learning models has become more and more extensive, and it has become more and more deeply involved in all aspects of people's lives. A large amount of personal privacy data is applied to the training of the model to improve the humanity and intelligence of the model. However, this trend increases the danger caused by privacy leaks. After mastering relevant data, attackers can rely on the performance of private data to profile people, and may target potential advertisements, data collection, and even targeted telecommunications. Provide convenience for online fraud and theft of private property.

**Acknowledgement.** The Opening Project of Intelligent Policing Key Laboratory of Sichuan Province, No. ZNJW2023KFMS004.

## References

1. Akhtar, N., Mian, A.: Threat of adversarial attacks on deep learning in computer vision: a survey. *IEEE Access* **6**, 14410–14430 (2018)
2. Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., Mané, D.: Concrete problems in ai safety (2016). [arXiv:1606.06565](https://arxiv.org/abs/1606.06565)
3. Arumugam, K., Naved, M., Shinde, P.P., Leiva-Chauca, O., Huaman-Osorio, A., Gonzales-Yanac, T.: Multiple disease prediction using machine learning algorithms. *Mater. Today Proc.* **80**, 3682–3685 (2023)
4. Bae, H., Jang, J., Jung, D., Jang, H., Ha, H., Lee, H., Yoon, S.: Security and privacy issues in deep learning (2018). [arXiv:1807.11655](https://arxiv.org/abs/1807.11655)
5. Barreno, M., Nelson, B., Joseph, A.D., Tygar, J.D.: The security of machine learning. *Mach. Learn.* **81**, 121–148 (2010)
6. Braun, L., Huppert, M., Khayata, N., Schneider, T., Tkachenko, O.: Fuse–flexible file format and intermediate representation for secure multi-party computation. *Cryptology ePrint Archive* (2023)
7. Doan, T.V.T., Messai, M.L., Gavin, G., Darmont, J.: A survey on implementations of homomorphic encryption schemes. *J. Supercomput.* 1–42 (2023)
8. Fan, C., Jia, P., Lin, M., Wei, L., Guo, P., Zhao, X., Liu, X.: Cloud-assisted private set intersection via multi-key fully homomorphic encryption. *Mathematics* **11**(8), 1784 (2023)
9. Feldman, V., McMillan, A., Talwar, K.: Stronger privacy amplification by shuffling for rényi and approximate differential privacy. In: *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pp. 4966–4981. SIAM (2023)
10. Flores Fernández, A., Sánchez Morales, E., Botsch, M., Facchi, C., García Higuera, A.: Generation of correction data for autonomous driving by means of machine learning and on-board diagnostics. *Sensors* **23**(1), 159 (2023)

11. Gao, C., Yu, J.: Securerc: a system for privacy-preserving relation classification using secure multi-party computation. *Comput. Secur.* **128**, 103, 142 (2023)
12. Gong, X., Wang, Q., Chen, Y., Yang, W., Jiang, X.: Model extraction attacks and defenses on cloud-based machine learning models. *IEEE Commun. Mag.* **58**(12), 83–89 (2020)
13. Haug, C.J., Drazen, J.M.: Artificial intelligence and machine learning in clinical medicine, 2023. *N. Engl. J. Med.* **388**(13), 1201–1208 (2023)
14. Hayet, I., Yao, Z., Luo, B.: Invernet: An inversion attack framework to infer fine-tuning datasets through word embeddings. In: *Findings of the Association for Computational Linguistics: EMNLP 2022*, pp. 5009–5018 (2022)
15. Hu, H., Salcic, Z., Sun, L., Dobbie, G., Yu, P.S., Zhang, X.: Membership inference attacks on machine learning: a survey. *ACM Comput. Surv. (CSUR)* **54**(11s), 1–37 (2022)
16. Jagielski, M., Carlini, N., Berthelot, D., Kurakin, A., Papernot, N.: High accuracy and high fidelity extraction of neural networks. In: *Proceedings of the 29th USENIX Conference on Security Symposium*, pp. 1345–1362 (2020)
17. Jain, N., Pal, S.K., Upadhyay, D.K.: Implementation and analysis of homomorphic encryption schemes. *Int. J. Cryptogr. Inf. Secur. (IJCIS)* **2**(2), 27–44 (2012)
18. Ji, S., Du, T., Li, J., Shen, C., Li, B.: Security and privacy of machine learning models: a survey. *Ruan Jian Xue Bao/J. Softw.* **32**(1), 41–67 (2021)
19. Jia, J., Gong, N.Z.: Attriguard: A practical defense against attribute inference attacks via adversarial machine learning. In: *27th {USENIX} security symposium ({USENIX} security 18)*, pp. 513–529 (2018)
20. Kamal, A.A.A.M., Iwamura, K.: Privacy preserving multi-party multiplication of polynomials based on  $(k, n)$  threshold secret sharing. *ICT Express* (2023)
21. Li, F., Chen, T., Zhu, S.: A  $(t, n)$  threshold quantum secret sharing scheme with fairness. *Int. J. Theor. Phys.* **62**(6), 119 (2023)
22. Li, M., Tian, Z., Du, X., Yuan, X., Shan, C., Guizani, M.: Power normalized cepstral robust features of deep neural networks in a cloud computing data privacy protection scheme. *Neurocomputing* **518**, 165–173 (2023)
23. Li, Y., Wang, R., Li, Y., Zhang, M., Long, C.: Wind power forecasting considering data privacy protection: A federated deep reinforcement learning approach. *Appl. Energy* **329**, 120, 291 (2023)
24. Lin, T.H., Lee, Y.S., Chang, F.C., Chang, J.M., Wu, P.Y.: Protecting sensitive attributes by adversarial training through class-overlapping techniques. *IEEE Trans. Inf. Forensics Secur.* (2023)
25. Liu, J., Lau, C.P., Chellappa, R.: Diffprotect: generate adversarial examples with diffusion models for facial privacy protection (2023). [arXiv:2305.13625](https://arxiv.org/abs/2305.13625)
26. Liu, X., Tu, X.F., Luo, D., Xu, G., Xiong, N.N., Chen, X.B.: Secure multi-party computation of graphs' intersection and union under the malicious model. *Electronics* **12**(2), 258 (2023)
27. Liu, Y., Feng, Q., Peng, C., Luo, M., He, D.: Asymmetric secure multi-party signing protocol for the identity-based signature scheme in the IEEE p1363 standard for public key cryptography. In: *Emerging Information Security and Applications: Third International Conference, EISA 2022, Wuhan, China, October 29–30, 2022, Proceedings*, pp. 1–20. Springer (2023)
28. Liu, Y., Wen, R., He, X., Salem, A., Zhang, Z., Backes, M., De Cristofaro, E., Fritz, M., Zhang, Y.: {ML-Doctor}: Holistic risk assessment of inference attacks against machine learning models. In: *31st USENIX Security Symposium (USENIX Security 22)*, pp. 4525–4542 (2022)

29. Luo, X., Chen, Z., Tao, M., Yang, F.: Encrypted semantic communication using adversarial training for privacy preserving. *IEEE Commun. Lett.* (2023)
30. Mahesh, B.: Machine learning algorithms-a review. *Int. J. Sci. Res. (IJSR)*. [Internet] **9**, 381–386 (2020)
31. Moerland, T.M., Broekens, J., Plaat, A., Jonker, C.M., et al.: Model-based reinforcement learning: a survey. *Found. Trends® Mach. Learn.* **16**(1), 1–118 (2023)
32. Ning, X., Tian, W., He, F., Bai, X., Sun, L., Li, W.: Hyper-sausage coverage function neuron model and learning algorithm for image classification. *Pattern Recognit.* **136**, 109, 216 (2023)
33. Nouman, M., Qasim, U., Nasir, H., Almasoud, A., Imran, M., Javaid, N.: Malicious node detection using machine learning and distributed data storage using blockchain in wsns. *IEEE Access* (2023)
34. Papernot, N., McDaniel, P., Sinha, A., Wellman, M.: Towards the science of security and privacy in machine learning (2016). [arXiv:1611.03814](https://arxiv.org/abs/1611.03814)
35. Papernot, N., McDaniel, P., Sinha, A., Wellman, M.P.: Sok: security and privacy in machine learning. In: 2018 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 399–414. IEEE (2018)
36. Pawase, A.D., Mandage, V.T., Panchal, S.S., Patil, S.Y., Deokar, P.: A shop recommendation system to empower retailers using machine learning
37. Rashid, K., Saeed, Y., Ali, A., Jamil, F., Alkanhel, R., Muthanna, A.: An adaptive real-time malicious node detection framework using machine learning in vehicular ad-hoc networks (vanets). *Sensors* **23**(5), 2594 (2023)
38. Salem, A., Zhang, Y., Humbert, M., Berrang, P., Fritz, M., Backes, M.: MI-leaks: model and data independent membership inference attacks and defenses on machine learning models (2018). [arXiv:1806.01246](https://arxiv.org/abs/1806.01246)
39. Salih, A., Zeebaree, S.T., Ameen, S., Alkhyyat, A., Shukur, H.M.: A survey on the role of artificial intelligence, machine learning and deep learning for cybersecurity attack detection. In: 2021 7th International Engineering Conference “Research & Innovation amid Global Pandemic” (IEC), pp. 61–66. IEEE (2021)
40. Sen, J.: Homomorphic encryption-theory and application. In: *Theory and Practice of Cryptography and Network Security Protocols and Technologies*, vol. 31 (2013)
41. Sharifani, K., Amini, M.: Machine learning and deep learning: a review of methods and applications. *World Inf. Technol. Eng. J.* **10**(07), 3897–3904 (2023)
42. Song, C., Huang, R.: Secure convolution neural network inference based on homomorphic encryption. *Appl. Sci.* **13**(10), 6117 (2023)
43. Sun, S., Huang, H., Peng, T., Shen, C., Wang, D.: A data privacy protection diagnosis framework for multiple machines vibration signals based on a swarm learning algorithm. *IEEE Trans. Instrum. Meas.* **72**, 1–9 (2023)
44. Truex, S., Liu, L., Gursoy, M.E., Yu, L., Wei, W.: Towards demystifying membership inference attacks (2018). [arXiv:1807.09173](https://arxiv.org/abs/1807.09173)
45. Venkateswar, K.: *Using Amazon Sagemaker to Operationalize Machine Learning*. Santa Clara, CA. USENIX Association (2019)
46. Weng, Z., Qin, Z., Tao, X., Pan, C., Liu, G., Li, G.Y.: Deep learning enabled semantic communications with speech recognition and synthesis. *IEEE Trans. Wirel. Commun.* (2023)
47. Wu, J., Huang, Z., Hu, Z., Lv, C.: Toward human-in-the-loop ai: enhancing deep reinforcement learning via real-time human guidance for autonomous driving. *Engineering* **21**, 75–91 (2023)
48. Xin, J., Lyu, X., Ma, J.: Natural backdoor attacks on speech recognition models. In: *Machine Learning for Cyber Security: 4th International Conference, ML4CS*



- 2022, Guangzhou, China, December 2–4, 2022, Proceedings, Part I, pp. 597–610. Springer (2023)
49. Xu, M., Yoon, S., Fuentes, A., Park, D.S.: A comprehensive survey of image augmentation techniques for deep learning. *Pattern Recognit.* 109347 (2023)
  50. Xu, Q., He, X., Lyu, L., Qu, L., Haffari, G.: Beyond model extraction: imitation attack for black-box nlp apis. *arXiv e-prints* pp. arXiv–2108 (2021)
  51. Ye, J., Maddi, A., Murakonda, S.K., Bindschaedler, V., Shokri, R.: Enhanced membership inference attacks against machine learning models. In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pp. 3093–3106 (2022)
  52. Yi, T., Chen, X., Zhu, Y., Ge, W., Han, Z.: Review on the application of deep learning in network attack detection. *J. Netw. Comput. Appl.* **212**, 103,580 (2023)
  53. Yu, Y., Li, Z., Tu, Y., Yuan, Y., Li, Y., Pang, Z.: Blockchain-based distributed identity cryptography key management. In: *2023 15th International Conference on Computer Research and Development (ICCRD)*, pp. 236–240. IEEE (2023)
  54. Zhang, J., Tian, H., Xiong, K., Tang, Y.L., Yang, L.: Fair multi-party private set intersection protocol based on cloud server. *J. Comput. Appl.* 0 (2023)
  55. Zhao, B.Z.H., Agrawal, A., Coburn, C., Asghar, H.J., Bhaskar, R., Kaafar, M.A., Webb, D., Dickinson, P.: On the (in) feasibility of attribute inference attacks on machine learning models. In: *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 232–251. IEEE (2021)
  56. Zheng, R., Qu, L., Cui, B., Shi, Y., Yin, H.: Automl for deep recommender systems: a survey. *ACM Trans. Inf. Syst.* (2023)



# Metaverse Security and Forensic Research

Manxuan Wang<sup>1</sup>, Guangjun Liang<sup>1,2,3(✉)</sup>, Meng Li<sup>4</sup>, and Siyi Cao<sup>1</sup>

<sup>1</sup> Department of Computer Information and Cyber Security, Jiangsu Police Institute, Nanjing, China

lianggjun@126.com

<sup>2</sup> Engineering Research Center of Electronic Data Forensics Analysis, Nanjing, China

<sup>3</sup> Key Laboratory of Digital Forensics, Department of Public Security of Jiangsu Province, Nanjing, China

<sup>4</sup> Basic Course Teaching and Research Department, Jiangsu Police Institute, Nanjing, China

**Abstract.** Metaverse is the advanced form of Internet technology development and the expansion and extension of cyberspace in the era of digital economy. In the meta-universe, data, computing power, algorithms and other elements integrate and promote each other, giving birth to new business models and application scenarios, changing people's production and life style and social governance model. In this paper, the concept, characteristics and development history of the meta-universe security and forensics are described, and the application scenarios and technical framework of the meta-universe are introduced. At the same time, this paper takes the forensics of meta-universe devices smart bracelet and smart TV as an example, analyzes the current problems of meta-universe security and forensics, and puts forward corresponding countermeasures for the current security problems of meta-universe forensics.

**Keywords:** Metaverse · Smart wearable device · Electronic data forensics

## 1 Introduction

Metaverse technology is committed to creating a virtual world that is parallel to the real world and interactively integrated. It is an advanced form of Internet technology development and has broad application prospects. It will definitely lead to major changes in social and cultural life [1, 2]. Metaverse Technology will develop and comprehensively integrate VR, AR, XR, AI, game engine, blockchain, cloud computing and many other high-tech achievements, and rapidly iteratively upgrade, thereby giving birth to and driving the rapid development of related technical science fields, and the two interact and advance side by side. At present, the metaverse has become a new highland for strategic layout of countries all over the world, and related technologies and industries are developing rapidly. However, the Metaverse is still in its infancy, and its development and application are immature. Due to its more complex information technology integration, its security issues are more diverse, and it faces risks and challenges. The construction of the metaverse may also produce a large number of spillover effects and induce a series

of severe social and cultural problems. Scholars conduct related research on metaverse security and forensics in response to existing problems, which can support and guide the steady and long-term development of metaverse technology research and development and industrialization, and continue to make new achievements and new progress.

In 2020, human society will reach the critical point of virtualization. The COVID-19 pandemic has swept across most of the world, forcing people to change their traditional contact-based social activities to non-contact ones. 2021 is known as the “first year of the metaverse”. Various Internet industry giants have aimed at the bright prospects of their development and announced their company’s future transformation plans. In order to catch the “high-speed train” of the metaverse, the famous social network company Facebook has announced to the society that it will complete the transformation into a metaverse company within the next five years. At the same time, “ByteDance” spent more than 9 billion yuan to acquire a VR hardware manufacturer. Once the game platform “roblox” was launched, its market value skyrocketed, showing infinite possible future prospects. On different tracks, different types of industries are taking steps to explore the Metaverse industry together and growing rapidly [3].

In terms of work and social interaction, Nvidia has established an industrial-grade metaverse, and employees’ production and social interactions are all carried out in a virtual space using network avatars. In the field of entertainment, virtual idols take advantage of the development of the metaverse to take advantage of the momentum. DOTA2 official virtual idol dodo, Tsinghua University virtual student Hua Zhibing, iQiyi virtual idol program “Interdimensional Rising Star” and so on have entered the public eye. In the cultural tourism industry, a new model of online activities integrating culture, scenes, and consumption has entered the construction stage [4]. While ensuring the effect of epidemic prevention and anti-epidemic, it can effectively promote the digital and intelligent development of the cultural tourism industry. The future of metaverse forensics is endowed with more possibilities. This new form of digital media integrates a variety of materials, which not only relies on the material world, but also transcends the material world. This kind of decentralized dissemination accelerates the dissemination process of cultural globalization and contributes to the collaborative innovation and development of multiple industries.

## 2 The Concept and Research Progress of the Metaverse

### 2.1 The Concept of the Metaverse

In the science fiction novel “Avalanche” published by American writer Neil Stephenson in 1992, the concept of metaverse first appeared in people’s field of vision. The novel builds a virtual digital world called “Metaverse” that is completely parallel to the real world. In the virtual world, people use virtual identities to socialize, work, compete and realize their own value.

What exactly is the metaverse? The connotation of the “Metaverse” concept, which was born in science fiction literature, seems to have an explanation of “thousands of people and thousands of faces”. The word “meta” often has two translations, namely “meta” and “super”. When translated as “meta”, it is a description of the essence of things, such as the familiar “meta-data”, which exists as a simplification of the entire

web page data. When translated into “chao”, it is the knowledge of transcendence. However, the author believes that when understanding the “meta-verse”, both translations are acceptable. Because it is not only a parallel universe related to the essence of the universe, but also a universe beyond the real world. It is not only a new starting point for research, but also a kind of transcendence [5, 6].

## 2.2 Research Progress of Metaverse

It is often said that the publication of the science fiction novel “Avalanche” in 1992 ushered in a new era for the development of foreign metaverses. In fact, “Avalanche” describes an advanced future world. The origin of the idea of the metaverse is generally considered to be in the novel “True Names and Surnames” written by the American professor Vernovitch published in 1981. This book creatively conceives a virtual world that can be entered and obtained sensory experience through a brain-computer interface. Since then, Metaverse has started its rapid development abroad. According to the analysis of the time zone map of foreign metaverse research (as shown in Fig. 1) and the number of foreign metaverse research publications, it can be seen that foreign metaverse research includes four stages, namely the initial exploration stage, rapid development stage, heat fading stage, and explosive development stage.

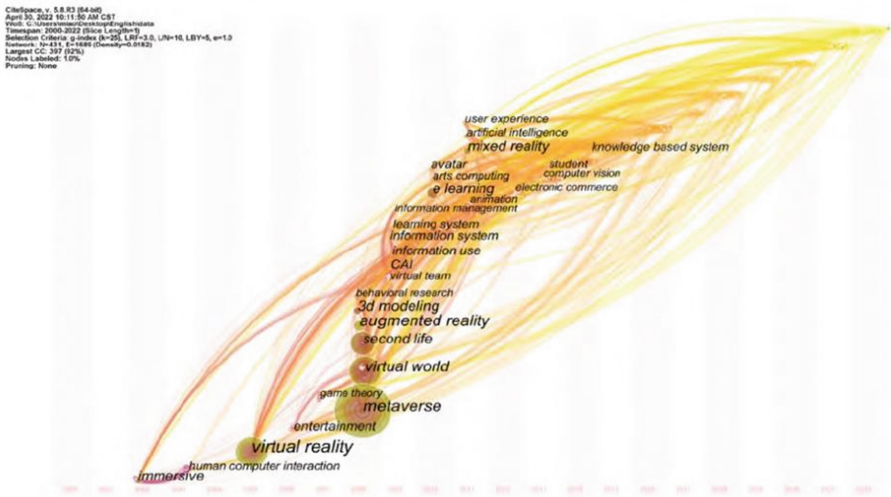


Fig. 1. Time zone map of foreign metaverse research from 2000 to 2022

The first stage is the initial exploration stage from 2000 to 2007. During this period, although many foreign scholars conducted related research on “Metaverse”, “Meta-verse” did not appear in the keywords. However, keywords such as “immersive”, “Virtual Reality”, and “entertainment” gradually emerged. At this time, most metaverses studied abroad are supported by virtual reality technology to study the environmental characteristics and realization of the metaverse. The metaverse at this time is actually

synonymous with various games, such as World of Warcraft, Second Life, etc., which has great limitations and is somewhat different from the current metaverse.

The second stage is the rapid development stage from 2008 to 2014. As the game “Second Life” that was born in the first stage became popular abroad, foreign metaverse research also ushered in a small peak. The research is not limited to the ontology of the metaverse, but extends to the application of the metaverse, including education, consumption, cultural tourism and other industries. Among them, the research in the field of education is more abundant. Metaverse can create a virtual learning environment at this stage, and make learning courses and conduct virtual experiments in this learning environment. In the consumer sector, sales venues have shifted from offline supermarkets to online. In the cultural tourism industry, such as the museum field, Metaverse can infer the exhibits that users have viewed from the museum’s access logs, and generate adjustment plans based on the user’s experience to bring a better tour experience.

The third stage is the heat subside stage from 2015 to 2020. Compared with the previous stage, at this stage, the research began to focus on the privacy issues within the metaverse, and gradually discovered problems with the universe. Foreign scholars such as Ben believe that user privacy includes three types: personal information privacy, behavioral privacy, and communication privacy. In the metaverse space, users are easily tracked and cause privacy leaks. At the same time, scholars have also proposed that user privacy can be protected by creating a “private copy”.

The last stage is the explosive development stage from 2021 to today. With the rapid development of information technology, the commercial field has also begun to intervene, and the Metaverse has quickly attracted the attention of economic, social, educational, medical and other fields, and research has entered a peak period of explosion. At this time, metaverse research presents a diverse situation. Correspondingly, the research content of the first three stages, such as the application, security, ethics, and technical support of the metaverse, is still the focus, but it is more specific and in-depth than the previous research. For example, the birth of the SimuMan framework can express the facial expressions and body language of virtual avatars. The framework that can support the six expressions of sadness, surprise, happiness, anger, enjoyment and neutral and can follow the user’s natural and smooth changes has greatly stimulated the enthusiasm of foreign metaverse research. In addition, foreign researchers have also conducted research on how to enhance the sense of belonging of vulnerable groups and help them socialize [7, 8].

### **3 Cyberspace Security and the Police Metaverse**

The core connotation of cyberspace security is information security, without information security, there will be no cyberspace security. Cyberspace security includes information security, network security, and data security. Metaverse is a typical digital information system and the future of cyberspace digitization. The police metaverse is supported by technologies such as blockchain, interaction, video games, artificial intelligence, network and computing, and the Internet of Things. Integrate and connect the virtual and real policing worlds to promote a new ecology and new style of global police interconnection, comprehensive interweaving, and collaborative operation.

In essence, the “Police Metaverse” is not a policing application scenario, nor is it a policing technical means, but a complete policing ecosystem. Cloud computing, digital twins, etc.) as the carrier, can realize the seamless connection among police officers, police machines, police environment, and police systems. The Police Metaverse aims to break the limitations of time, space, and resources in police governance, and realize the “presence” of police officers’ multi-sensory senses such as hearing, sight, taste, touch, and smell, so as to realize the “presence” of police services and crime governance. The goal of diachronic integration, synchronous sharing, and real-time interaction”. Its appearance marks that the digitalization of police affairs is moving towards a meta-cosmos that interweaves virtual and real collaboration, highly interactive structures, and comprehensive human-machine connections. Its system architecture diagram is shown in Fig. 2.

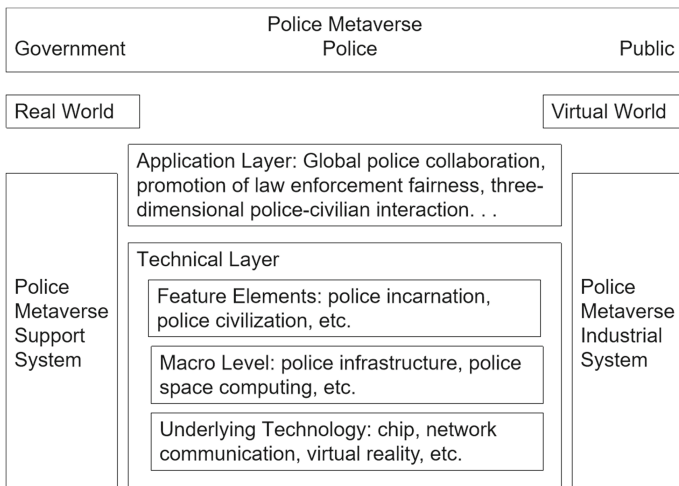


Fig. 2. Schematic diagram of the police metaverse system architecture

## 4 Smart Bracelet Forensic Example

### 4.1 Smart Bracelet Data Acquisition

As a metaverse device, the smart bracelet is also one of the important components of the Internet of Things. Therefore, for the forensics of smart bracelet data, we need to use the software “Internet of Things Forensic Analysis”. First, create a case. This case will be the carrier of the data extracted in the future. After creating the case, select the model of the smart bracelet and add it to the inspection materials. And follow the prompts to extract the data in the smart bracelet. After opening the official website of Mi Band, enter and click Export Data, a risk warning will pop up on the web page, warning users who extract the data that there is a risk of leakage. According to the data classification given by the official website, this forensics can extract personal data, activity data, sleep, heart

rate, body fat, exercise data and other private information of bracelet users, and can even be specific to detailed information such as rapid eye movement time during sleep and calorie consumption during exercise. After selecting the desired data, the official website will automatically package the data and send the compressed package to the mailbox specified by the user. The user only needs to log in to the mailbox to easily download the compressed package containing the bracelet data. Through the steps given by the software, we can find that for the smart bracelet branded as Xiaomi, its official website provides the function of exporting all the data of the bracelet, and it will be encrypted and compressed and sent to the designated mailbox. To complete the whole process, the user only needs to provide an account number and password, and there is no second layer of barriers. Although there will be a warning that there is a risk of leakage in the middle of the evidence collection, it is not enough to send a strong enough reminder to the user, and the identity information of the person who extracted the data will not be further confirmed. After downloading and opening the compressed package, it is found that the data has been divided into different categories, such as user information, sleep information, heart rate detection information, exercise information, etc., which are placed in different folders, and finally presented in the form of a table, which is simple and clear, and easy for users to understand and use. The final data presentation form is shown in Fig. 3.

📁 ACTIVITY	2023/4/25 11:53
📁 ACTIVITY_MINUTE	2023/4/25 11:53
📁 ACTIVITY_STAGE	2023/4/25 11:53
📁 BODY	2023/4/25 11:53
📁 HEARTRATE	2023/4/25 11:53
📁 HEARTRATE_AUTO	2023/4/25 11:53
📁 SLEEP	2023/4/25 11:53
📁 SPORT	2023/4/25 11:53
📁 USER	2023/4/25 11:53

**Fig. 3.** The final presentation form of the data

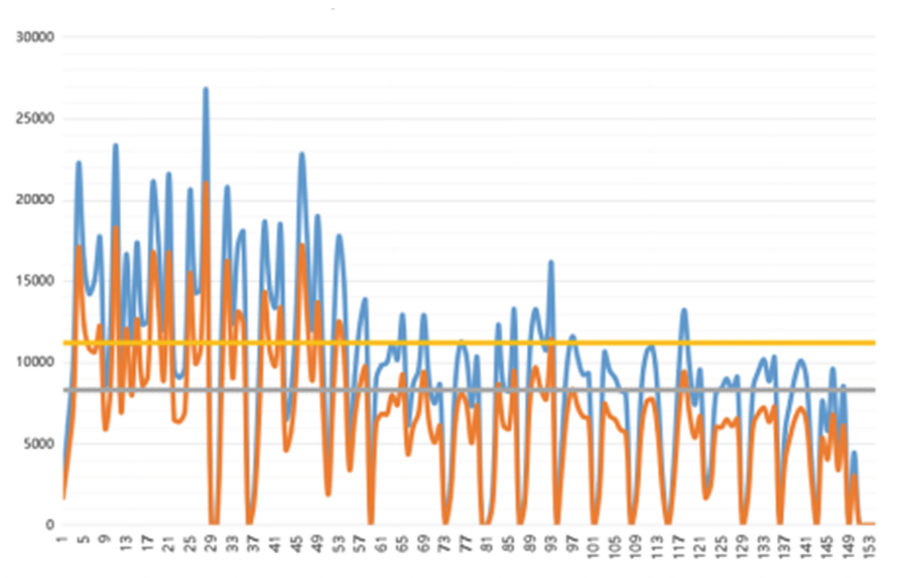
Through the acquisition and analysis of these data, using visualization and corresponding algorithms, we can obtain the personality tags of each user who uses Metaverse smart wearable devices, and adjust real-world behaviors through tags to obtain better physical conditions. However, there are pros and cons. The easy and successful extraction of data can not help but cause reasonable concerns. Metaverse wearable devices contain a lot of useful information, many of which are relatively private secrets, and their leakage may have a very large impact on users, and even affect the behavior of the real world. Leakage of trajectory information may lead to tracking violations, sleep information leakage may cause health care product companies to take advantage of it, and WeChat message information connected to mobile phones is a great challenge to

personal privacy violations, and so on. The one-level checkpoint that only needs to enter the account password undoubtedly poses a greater risk of leakage.

## 4.2 Data Analysis of Smart Bracelets

### 4.2.1 Daily Steps Analysis

Studies have shown that when the number of daily steps is 8300–11200 steps, as the number of daily steps increases, the improvement effect of body fat mass and body fat percentage also increases. For every 1,000 steps per day, the body fat loss increased by 1.09 kg. However, when the daily step count is greater than 11400–14700 steps, the improvement effect will decrease with the increase of the step count. Therefore, only when the number of daily steps is increased or decreased within an appropriate range can effective fat loss be achieved.



**Fig. 4.** Changes in daily steps and walking distance

The daily steps and walking distance extracted from the bracelet are made into a line graph (as shown in Fig. 4), and the following analysis can be performed. Among them, the gray and yellow lines represent the number of steps that can achieve the best fat-reducing effect. It can be seen from the figure that in the 153 days recorded by the bracelet, the user's step changes are quite extreme. The general rule is that the number of steps exceeds 15,000 or even 20,000 on weekdays, while it is less than 8,000 steps on weekends. It can be inferred that most of the user's commuting on weekdays is by walking, or he pays more attention to exercise, while on weekends he will choose to "walk or not walk if he can", staying at home, and the number of steps will be reduced accordingly. Data that deviates from the standard number of steps can also be analyzed



to show that the user has not carried out scientific and effective fat loss activities. In order to achieve better results, manual intervention can be used to adjust the number of daily steps, such as changing the travel mode when necessary on weekdays, using battery cars, cars and other means of transportation, and participating in outdoor sports on weekends.

If the security of this information cannot be guaranteed, it will be stolen and used by people with intentions, and sold to unscrupulous merchants, and the user's mobile phone will not be safe. Numerous sales calls of "fat loss training camp" and "recommendation of transportation tools" aimed at business opportunities, pervasive, and targeted the pain points of users, so as to earn more benefits. Merchants have obtained high profits, but the lives of users of Metaverse devices have been disturbed, and they may even consume impulsively, causing their own economic losses.

#### 4.2.2 Heart Rate Analysis

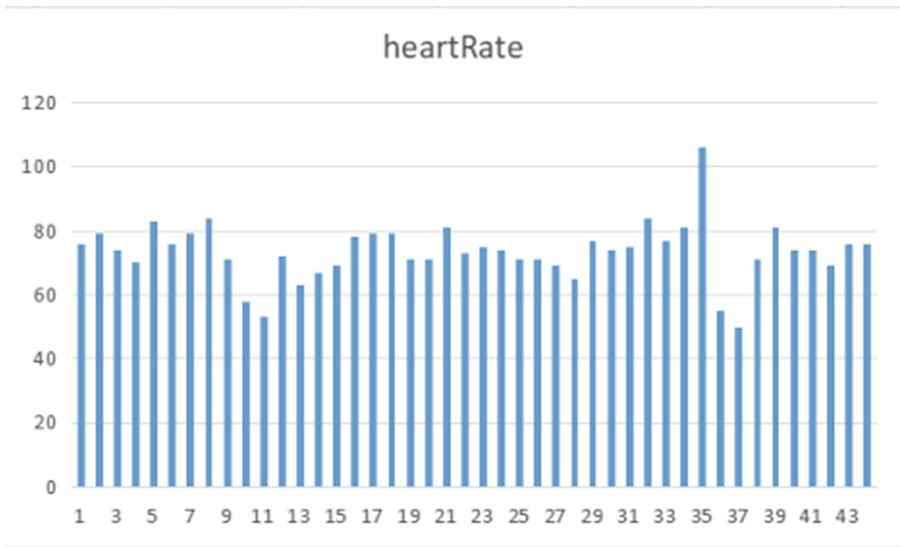
Medical personnel can better grasp the patient's daily life activities and health status based on the mobility, behavior and functional ability recorded on the patient's bracelet. Therefore, the heart rate monitoring of the bracelet can effectively improve the compliance of aerobic activities in patients with chronic heart failure, allowing patients to obtain greater benefits. With the increasing incidence of stroke year by year, more and more attention has been paid to blood pressure management in clinical practice. Heart rate is an important factor in the prognosis evaluation of hypertensive stroke patients, and it is very easy to monitor at the same time. Smart bracelets play a vital role in hypertensive stroke.

Slow heart rate is a positive factor for the improvement of high blood pressure. The improvement of high blood pressure is more obvious in patients with a resting heart rate of less than 70 beats. According to the heart rate results monitored by this bracelet, the probability of the user suffering from hypertensive stroke can be predicted. (as shown in Fig. 5).

The international verapamil sustained-release trandolapril study showed that the relationship between heart rate and mortality was a U-shaped curve, and the mortality rate was the lowest in patients with a heart rate of 55–75 beats/min. It can be seen from the figure that the user's heart rate is basically in the range of 70–80, and there are also relatively unstable situations. It can be deduced that the possibility of the user suffering from high blood pressure still cannot reach the minimum. At the same time, the user's heart rate fluctuates greatly, and the possibility that the heart rate and blood pressure may be easily affected by the surrounding environment cannot be ruled out.

According to the results of the analysis, it is necessary to take measures to reduce the user's heart rate and take targeted heart rate management to reduce the risk of hypertensive stroke. Based on the data analysis of the smart bracelet, suggestions can be made for the user to increase the amount of exercise appropriately, and if necessary, use drug intervention to reduce the oxygen consumption of the heart and weaken the stress of the heart.

Of course, heart rate monitoring can timely feed back the abnormal information of the user's heart to the user of the bracelet, so that he can adjust his living habits and make necessary countermeasures. However, under Xiaomi's incomplete security protection



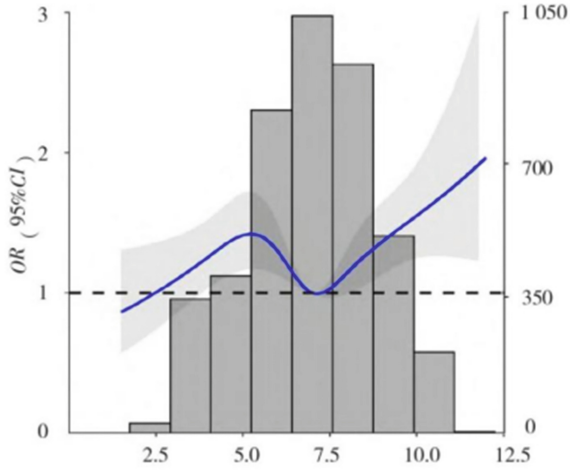
**Fig. 5.** User's heart rate

measures, heart rate and movement trajectory, once leaked, criminals will regard it as a “secret recipe” for tracking users. They can easily infer the user's physical condition and use it as a blackmail method to blackmail the user. They can also obtain the user's daily habits and route trajectory, which can easily cause damage to the user's property and personal life. And so on, people can't help but put a big question mark on the forensics security of metaverse equipment.

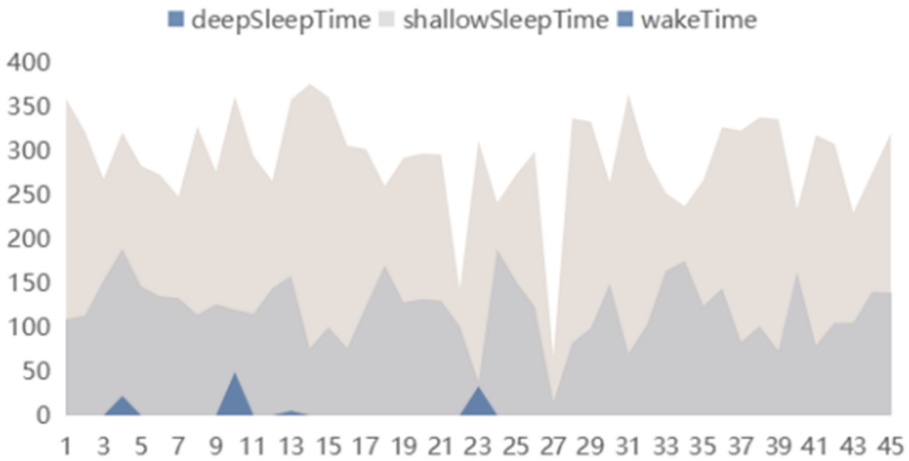
### 4.2.3 Sleep Monitoring

With the rapid aging of my country's population, cognitive dysfunction in the elderly is increasingly becoming a prominent public health problem. Given that there is no effective treatment, identifying risk factors to prevent or delay their occurrence is the main strategy and initiative. There is a statistical relationship between nighttime sleep duration and cognitive impairment in the elderly (Fig. 6). The probability of cognitive impairment in the elderly who sleep less than 6 h and more than 8 h is 1.24 times and 1.33 times that of the elderly who sleep more than 6–8 h. Both short sleep duration and long sleep duration increase the risk of cognitive impairment in the elderly. Insufficient sleep will increase inflammatory response factors, and longer sleep will accelerate the atrophy of frontotemporal gray matter in the elderly, damage memory, and lead to cognitive dysfunction. Referring to the model in Fig. 5, the sleep time of the user of the wristband can be analyzed. The sleep time of the bracelet user is visualized as follows (as shown in Fig. 7).

The smart bracelet can not only record the total time of the user's sleep, but can even distinguish between the user's deep and light sleep, and record the corresponding time. It can be found that the user's sleep time is generally within the “golden sleep time” of 6 to 8 h, and there is no big problem. But the duration of deep sleep is shorter. In response



**Fig. 6.** The relationship model between nighttime sleep time and cognitive impairment in the elderly in a community



**Fig. 7.** Changes in sleep time

to this situation, the user can change his diet structure and consume more high-protein foods, such as milk, wild jujube seed soup, and the like. You can also create a very quiet environment before going to bed to increase the duration of deep sleep.

Similarly, the sleep time recorded by the bracelet can certainly help users understand their sleep status and adjust their work and rest, but if it is used by someone with a heart, it will also become a sharp knife in the hands of criminals. After knowing the user's sleep time and duration, it is more convenient to commit criminal acts when no one is paying attention, such as burglary, etc., which greatly threatens the safety of Metaverse device users.

## 5 The Risk Challenge of Metaverse Security

### 5.1 Cyber Attack Threat

Among the main threats to the digital ecosystem, cyber attacks account for the main part. Obviously, the metaverse cannot be the “exception” that escapes the sword of cyber attack. Moreover, “the height of the Tao is one foot, and the height of the devil is one foot.” With the continuous development of metaverse technology, the types and forms of cyber attacks are also constantly updated. New cyber attacks are likely to target equipment terminals and end users in the metaverse, and operators and key service providers may also become their criminal targets. The advantage of the metaverse itself—the fusion of virtual and real worlds will also raise the danger of cyber attacks to a new level. The cyber attack at this time will not only attack the property and data in the virtual world, but may also affect the lives and health of citizens in the real world. Cyber security policing also needs to target more targets in the preventive link. It is necessary to continuously update the attack methods and increase the attack surface, which makes the precious police force more dispersed, and the concentrated attack is not as effective as before.

To address the threat of cyber attacks, we need to make full use of the significant advantages of new technologies, such as big data, cloud computing, and the Internet of Things. Even if the data is large, complex, and dynamic, it can be processed quickly and effectively, and a real-time updated intelligent processing system can be built. Network security knowledge system can improve the defense ability of network attack threats.

### 5.2 Technical Security Flaws

There may be more design flaws in the metaverse’s integration model of technology that are not even realized. These design loopholes are like time bombs, which are likely to be targeted by cunning cyber attackers, and are likely to explode suddenly when the system itself is running, affecting the operation of the system. Moreover, the Metaverse tries to permanently preserve online information and also hopes to ensure the integrity of the system. Therefore, the cost of system upgrades and repairs is extremely high, and some hidden loopholes are difficult to discover in time. This gives criminals an opportunity to take advantage of the loopholes to invade the system and seek illegitimate benefits without anyone noticing. Once the criminal system matures, it will be more difficult for the cyber security department to crack down on it, and it will take more time and effort.

To solve the technical security flaws of Metaverse technology, it is necessary to train a large number of professional and technical personnel. To have a more specific understanding of Metaverse technology from a theoretical perspective, we can not only avoid possible problems when designing Metaverse equipment, but also provide practical solutions for future problems. Pave the way for possible network security issues.

### 5.3 Critical Infrastructure

The Metaverse relies on the normal operation of critical infrastructure, and once it is attacked or fails, its negative impact is likely to be beyond the control of capabilities. For example, if the information storage system in the Metaverse is attacked, the value of the

Metaverse will be severely reduced, and the resulting economic losses will be huge. The protection of critical infrastructure will also present additional challenges for forensics.

Complementary devices must follow suit, keeping pace with software development. Metaverse technology is not just a technology. When problems arise, all levels need to cooperate with each other to solve the problem. Perfect supporting facilities are the key to dealing with security issues. Without supporting infrastructure, security issues will break out sooner or later. Therefore, strengthening the construction of supporting facilities is also a top priority.

#### **5.4 Data Breach**

The designers of the Metaverse hope to use the blockchain technology to put a layer of protection on the information security of users in the Metaverse, but the blockchain technology may still be attacked by cyber attackers. If the assets and information of virtual identities in the Metaverse are stolen, their user value will instantly return to zero. The huge profits made hackers all over the world aim at the “meat and potatoes” of the Metaverse. The next big target for cybercriminals will also be the Metaverse. How to avoid the leakage of information and property, how to obtain evidence, track and protect after leakage has also become an important topic.

The victims of these information leaks have a wide range of subjects, various types of information, and negative impacts. Therefore, we need to improve the laws and regulations on the large-scale leakage of Metaverse information and property as soon as possible, and build a comprehensive Metaverse information protection legal system to prevent criminals from taking advantage of legal loopholes and causing avoidable losses. Secondly, strengthen the main responsibility of operators, increase the cost of crime, restrain the behavior of operators from the inside, and prevent them from actively leaking information.

#### **5.5 Digital Data Forensic Difficulties**

The metaverse will lead to differences in the extraction and fixation of electronic evidence from the present, and the types of electronic data will be more extensive. U disk, cloud disk, and hard disk are no longer the only types of storage devices; in order to keep up with the development of the metaverse, the database will increase accordingly; the display of data is no longer limited to APPs, browsers, etc.; Not only based on the existing operating system to run. These new possibilities have also brought new and huge challenges to police forensics personnel.

The actual work of electronic forensics requires not only important legal support, but also the formulation of comprehensive electronic forensics management measures in combination with existing online fraud cases. Only in this way can the security of the network environment be maintained to the greatest extent.

## **6 Conclusion**

Metaverse is an advanced form of Internet technology development, and it is the expansion and extension of cyberspace in the era of digital economy. By studying the security of metaverse forensics, it is expected to improve the efficiency of metaverse equipment

forensics and improve the security of metaverse equipment. The metaverse equipment is widely used, and the technology is constantly advancing, but there are still some problems that need to be solved urgently. The actual work of electronic forensics requires not only important legal support, but also the formulation of comprehensive electronic forensics management measures in combination with existing online fraud cases. Only in this way can the security of the network environment be maintained to the greatest extent.

## References

1. Bolu, W.: Comments on the ambitions and concerns of metaverse technology. *J. Univ. Electron. Sci. Technol. China (Soc. Sci. Ed.)* **25**(01), 11–16+51 (2023). [https://doi.org/10.14071/j.1008-8105\(2022\)-4011](https://doi.org/10.14071/j.1008-8105(2022)-4011)
2. Min, S., Feng, X.: Confusion after metaverse “became popular”. *Procurat. Situati.* **659**(15), 64–66 (2022)
3. Shenyang.: The three transformations, three and three energies of metaverse. *Media* **379**(14), 21–22 (2022)
4. Xinju, H., Rui, D., Huaqing, W.: The development and governance of the chinese metaverse—comparing the history of internet development in China. *Indust. Econ. Rev.* (2023)
5. Yanan, H., Tao, A.: Duan Xinxin and so on. Research hotspots and trends of Metaverse at home and abroad—Based on CiteSpace visualization analysis. *Southeast Commun.* (2022)
6. Lin, W.: The development of metaverse abroad and its enlightenment to our country. *Shanghai Inf.* **209**(03), 54–56 (2022)
7. Yong, P.: Prevention and governance of new cybercrime. *Crime Res.* **249**(06), 11–17 (2021)
8. Zekai, C., Lin, Z., Zhanquan, L.: Dose-effect relationship between daily steps and fat loss in obese children and adolescents. *Chinese School Health* **43**(09), 1329–1332 (2022)



# A Survey of Security Vulnerabilities and Detection Methods for Smart Contracts

Jingqi Zhang<sup>1</sup>, Xin Zhang<sup>1</sup>, Zhaojun Liu<sup>1</sup>, Fa Fu<sup>1(✉)</sup>, Jianyu Nie<sup>2</sup>, Jianqiang Huang<sup>3</sup>, and Thomas Dreibholz<sup>4</sup>

<sup>1</sup> Hainan University, Haikou, China  
fufa@hainanu.edu.cn

<sup>2</sup> International Business Beijing Foreign Studies University, Beijing, China

<sup>3</sup> China Telecom Corporation Limited Hainan Branch, Haikou, China

<sup>4</sup> Simula Metropolitan Centre for Digital Engineering, Oslo, Norway  
dreibh@simula.no

**Abstract.** At present, smart contracts cannot guarantee absolute security, and they have exposed many security issues and caused incalculable losses. Due to the existence of these security vulnerabilities, researchers have designed many detection and classification tools to identify and discover them. In this article, we present a classification of smart contract security vulnerabilities based on a large number of detailed articles. Then, we introduce the latest smart contract vulnerability detection methods, summarize the process model of detection tools based on artificial intelligence methods, and compare and analyze various detection tools. Finally, we provide an outlook on future research directions based on the current status of smart contract security.

**Keywords:** Blockchain · Smart contracts · Detection methods · Security vulnerabilities

## 1 Introduction

Smart contracts are a special protocol used in the development of contracts within the blockchain. It allows for trusted transactions without a third party and ensures that these transactions are traceable and irreversible. The idea of Smart Contracts were introduced and defined by Szabo [1]. Although smart contracts have a high level of security, there are still unscrupulous individuals who exploit the vulnerabilities of smart contracts to gain illegal benefits. For example, there is a case of an attack in 2021, Hackers have stolen some \$600 million in cryptocurrency from the decentralized finance platform Poly Network<sup>1</sup>. This study explores the latest methods and tools for blockchain-based smart contract vulnerability detection. In addition, we analyze the features of these detection tools and compare them. Finally, based on the analysis, we discuss the research directions about the future security of smart contracts.

<sup>1</sup> Poly Network: <https://edition.cnn.com/2021/08/11/tech/crypto-hack/index.html>.

## 2 Security Issues

### 2.1 Smart Contract Platform Vulnerability

**Oracle** Oracle's security problem lies in the fact that its nodes are responsible for critical data stored securely on the blockchain. However, Oracle nodes are the only source of real data and are susceptible to attacks, manipulation, and compromise, so it is also a security issue for smart contracts [2].

**IOTA** (Internet of Things Application) is a distributed ledger technology (DLT) specifically designed for the Internet of Things (IoT). But it still carries the risk of being attacked, as well as its custom hashing algorithms. Some researchers found that there were collision issues with it. Bitcoin has Transaction malleability, and other popular platforms will be attacked as they get more activity [3].

### 2.2 Smart Contract Code Vulnerability

**Unchecked Return Value** In solidity language, some functions will generate unreasonable return values when executed or called, and these wrong return values will lead to logical errors in the operation of smart contracts.

**tx.origin** It is a solidity global variable that contains the address of the originator of the current transaction. However, using tx.origin may pose security issues. One potential security threat is spoofing smart contracts by spoofing the sender address of a transaction. If the smart contract relies on tx.origin to determine the sender of the transaction, this vulnerability can be exploited by the attacker [4].

**Integer Overflow and Underflow** Integer overflows are relatively common security vulnerability. If the integer variable exceeds the valid range during operation, an integer overflow error will occur. Among them, arithmetic, truncation, and signed overflow are the main problems of smart contracts [5].

### 2.3 Blockchain Vulnerability

**Reentrancy Vulnerability** It is a type of security vulnerability that can occur in smart contracts. It happens when an attacker exploits a contract's method that calls another contract without completing its own internal processing [6].

**Timestamp Dependency** Miners can manipulate the timestamps of transactions to exploit vulnerabilities. In order to benefit from transactions, miners can change the timestamps that are most favorable to their operations, so the different benefits for miners can lead to security issues [7].

**Time Constraints** In general, time constraints are implemented through timestamps, which require the consent of all miners. At the same time, all transactions within a block share the same timestamp. This mechanism enables all contracts to maintain a consistent state, but it also risks being attacked. Because the miner creating a new block can choose either timestamp, when the miner holds shares [8].

**Generating Randomness** Generating random numbers are intended to increase the security of smart contracts, but even then, there are still some



problems of security vulnerabilities. The security issue of generating random numbers in smart contracts is of great importance, because the predictability of random numbers may leave vulnerabilities for hacking attacks [9].

### 3 Security Vulnerability Analysis Tools in Smart Contracts

The tamper-evident nature of smart contracts has both advantages and disadvantages. We analyze the security vulnerability analysis tools of smart contracts into two categories, static analysis methods [10–20] and dynamic analysis methods [21–29]. In addition, this paper also analyzes the dynamic static combined detection tool [30] was analyzed in this paper. The latest detection results are also summarized and analyzed according to this classification.

#### 3.1 Static Analysis

Traditional smart contract vulnerability detection tools are basically based on fixed inspection rules [12], at the same time, traditional detection tools also have numerous problems. Therefore, in following search, a large proportion of tools using deep learning methods for vulnerability detection which can avoid this problem.

Xuesen Zhang et al. proposed a Bi-LSTM (Bi-directional Long Short-Term Memory) neural network based approach [10]. This method vectorizes the code of the smart contract and uses it as input for vulnerability detection. As LSTM is a forward network, the authors add backpropagation operators to obtain Bi-LSTM neural network operators. However, for new types of defects, the neural network needs to be retrained. On the other hand, Huiwen Yang et al. proposed a detection method [11] which is based on abstract syntax trees (AST). It extracts the features of smart contracts from AST, divides an AST into multiple ASTs based on the types of functions, state variables, and function modifiers, and then trains the model to detect vulnerabilities in smart contracts.

An approach to use graph neural networks (GNN) for smart contract vulnerability detection is suggested by Zhuang et al. [12], they proposed a degree-free graph convolutional neural network (DR-GCN) and a new temporal message propagation function (TMP) that learns from the normalized graph to vulnerability detection.

In contrast, Ziling Wang et al. proposed the GVD-net (Graph embedding-based Machine Learning Model for Smart Contract Vulnerability Detection) model [13] to detect vulnerabilities in smart contracts. The whole GVD-net is divided into a preprocessing part, a backbone network and a detection part. But it can only detect three types of vulnerabilities, namely arithmetic problems, access control and asset freezing.

There are still some methods proposed by researchers. Ran Guo et al. proposed a model based on twin networks (SCVSN) [14] for smart contract vulnerability detection. SCVSN combines twin networks with deep learning models

and has a high level of accuracy for reentrant vulnerabilities. But it only uses reentrant vulnerabilities as case study, and it does not have the ability to detect integer overflow vulnerabilities and timestamp vulnerabilities.

Lejun Zhang et al. proposed a serial-parallel convolutional bidirectional gated recurrent network model (SPCBIG-EC) fusion integrated classifier [15] that can show excellent performance advantages in multi-task vulnerability detection. Meanwhile, the authors propose a CNN structure, string-parallel CNN (SPCNN), applicable to the above serial hybrid model. However, when the vulnerabilities are mixed, the accuracy is lower and the sensitivity is bad. They also proposed a hybrid model-based model called CBGRU [16], which combines different word embeddings and different deep learning methods to detect smart contract vulnerabilities. In the experiments, CBGRU performed excellent in detecting infinite loop vulnerabilities and so on. But the accuracy of the model in detecting smart contract vulnerabilities with obvious features is significantly higher than that of vulnerabilities with less obvious features.

Zhipeng Gao proposed a deep learning method called SmartEmbed [17] for detecting vulnerabilities in smart contracts, which detects code clones and problem points in smart contracts. In SmartEmbed, the information retrieval process has been accelerated in matrix computation, code embedding, and database access.

In Ethereum and some blockchain networks, the gas in smart contracts acts as an indicator to measure the computational effort and resource consumption. It ensures fair compensation for miners and helps maintain network security and efficiency. Asem Ghaleb et al. proposed a bytecode-based taint tracking detection tool, eTainter [18], which is a static analyzer that specifically targets gas-related vulnerabilities in smart contracts. But this tool has some limitations, as it cannot detect unbounded loop vulnerabilities that depend on data items, and some contracts have timeout issues.

Clara Schneidewind et al. proposed a tool called eThor [19], the first well-established automated static analyzer based on EVM (Ethereum Virtual Machine) bytecode. eThor takes as input the bytecode and contract-parameterized HoRSt specification, which is a framework for the specification and implementation of static analyses based on Horn clause resolution. And later goes through several stages of analysis to measure vulnerabilities.

Weimin Chen proposed a semantic-awareness-based tool, SADPonzi [20], to identify Ponzi schemes in Ether smart contracts. It uses a heuristic-guided symbolic execution technique. Experimental tests show that SADPonzi outperforms the current so method with 100% accuracy and recall, but it also has the limitation that it cannot be used to detect new Ponzi smart contracts or less popular Ponzi schemes.

## 3.2 Dynamic Analysis

Dynamic analysis is used to detect, track, and analyze the running kind of smart contracts to understand their behavior, performance, and security. Common

dynamic vulnerability detection methods are mainly dynamic symbolic execution, fuzzy testing, dynamic taint, etc. In recent years, with the development of deep learning, tools for detecting smart contract vulnerabilities using machine learning have also gradually emerged. In the following research, we will analyze and introduce several common dynamic detection tools as well as the latest detection tools.

A tool called Oyente is proposed by Luet al. [21], which uses symbolic execution for the detection of smart contract security vulnerabilities. This tool follows a modular design, which consists of four main components, CFGbuilder (Control Flow Graph), Explorer, CoreAnalysis, and Validator. It does not fully mimic the execution environment of Ether, so it does not yet reach the expected level.

Bo Jiang et al. proposed a tool called ContractFuzzer [22], which is the tool that first uses fuzzy testing to test the security vulnerabilities of Ethereum smart contracts. Compared with the Oyente, this tool can detect 7 types of vulnerabilities and its leakage rate is relatively reduced.

Another tool called EasyFlow [23] is a smart contract vulnerability detection tool based on taint analysis proposed by Jianbo Gao et al. It focuses on such vulnerabilities as integer overflows. It can not only classify smart contracts into secure contracts and contracts with overflows, but also automatically generate transactions that trigger overflows.

Besides, Yuhe Huang et al. proposed a tool called EOSFuzzer [24], a generic black-box fuzz testing framework, which is the first fuzzing framework for detecting vulnerabilities in EOSIO (Enterprise Operation System Input Output) smart contracts.

Mojtaba Eshghie et al. proposed a monitoring framework Dynamit, which is a tool that first uses machine learning to analyze the dynamic execution of smart contracts [25]. The tool consists of a monitor and a detector, where the monitor is used to collect information about the transaction and to discern whether the transaction is harmful or not. As the same time, Mengjie Ding et al. proposed HFContractFuzzer [26], a tool based on fuzzy technique for testing Hyperledger Fabric smart contracts. HFContractFuzzer is effective, but it still has drawbacks and limitations, such as performance degradation problems, inability to verify its superiority, etc.

Except for all the tools mentioned above, a novel reinforcement learning-based vulnerability guided fuzzifier RLF [27] was proposed by Jianzhong Su et al. , which is used to motivate vulnerable transaction sequences to detect vulnerabilities in smart contracts. Meanwhile, the Park [28], a tool first using general framework for parallel forked symbolic execution of smart contracts, was proposed by Peilin Zheng et al. It proposes the use of multiple CPU cores to improve symbol execution efficiency based on symbol tools. And WASAI [29], a new concolic fuzzer for discovering vulnerabilities in Wasm (WebAssembly) smart contracts proposed by Weimin Chen et al. has been tested as a state-of-the-art tool, but it still has some shortcomings, such as the trade-off between

scalability and efficiency, the seeds chosen by WASAI are not the most suitable, the benchmarks need to be improved, etc.

### 3.3 Dynamic and Static Combined Analysis

Currently, there are few tools that can combine static analysis with dynamic analysis, but HFCCT (Hyperledger Fabric Chaincodes Test) [30] is one of them. Peiru Li et al. proposed HFCCT, a vulnerability detection tool that combines dynamic symbolic execution and static abstract syntax trees for detecting Golang chain code vulnerabilities. After testing, HFCCT is significantly more efficient than HFContractFuzzer. HFCCT can detect more vulnerabilities compared to HFContractFuzzer, but it still has two kinds of vulnerabilities that cannot be detected, they are Reified Object Addresses and Cross Channel Chaincode Invocation. Besides, further optimization is needed to be improved.

### 3.4 Comprehensive Comparison

We conducted a comparative analysis of the detection tools mentioned above and found that the use of deep learning methods for smart contract security vulnerability detection has been increasing in recent years, and we summarized all the tools.

**Table 1.** Experimental data based on artificial intelligence detectors

Tool	Analysis method	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)
Detection based on Bi-LSTM Neural Network [10]	Machine learning	81.4	100	41.	58.3
Detection based on abstract syntax tree [11]	Abstract syntax tree (AST)	99.6	98.8	90.4	94.4
Detection using graph neural networks [12]	Machine learning	84.4	74.1	82.6	78.1
SCVSN [14]	Deep learning	96.0	94.2	96.0	94.8
SPCBIG-EC [15]	Deep learning	96.7	94.6	–	96.74
CBGRU [16]	Deep learning	93.3	96.3	86.0	90.9
Dynamit [25]	Machine learning	94.0	–	94.0	93.0

About 70% of the static analysis tools in our survey are based on machine learning or deep learning. We summarize the model of smart contract vulnerability detection tools using artificial intelligence technology, as shown in Fig. 1. And we summarize the data of AI-based detection tools. All data are compared with the reentrancy vulnerability as the detection object, and the detection indicators include: Accuracy, Precision, Recall, and F1 as shown in Table 1.

First, these methods using artificial intelligence technology clean the source code of smart contracts, segment words, and convert the code into vectors to build a dataset. Then, the dataset is divided into training set and test set by labeling. Finally, the training set was used to train the constructed model, and the test set was used to obtain the analysis report.

References [11, 13] improved the part of converting the code into vectors. Detection based on AST [11] improved the word embedding. The AST is divided

into state variables, function modifiers, and functions, and all of them are converted into vectors for model training to obtain better training results. GVD-net [13] is an improvement on word embedding. The authors treat the variables and relationships of solidity code as a non-Euclidean graph, and use the Node2Vec [31] algorithm to construct vectors.

References [10, 14, 15, 17] improved the detection part. The Detection based on Bi-LSTM Neural Network [10] built their model based on Bi-LSTM network. SCVSN [14] improves the network structure and combines two networks to train the model. The SCVSN Siamese network structure is the combination of Siamese network and LSTM neural network. SPCBIG-EC [15] improves the network structure, combines the serial hybrid model of CNN and RNN, and combines the feature extraction advantages of CNN and the characteristics of RNN emphasizing the time dimension. In the detection part of the network, SmartEmbed [17] uses deep learning and similarity checking technology to unify clone detection and bug detection efficiently and accurately, so as to improve the efficiency and accuracy.

References [12, 16] have improved the overall model. Detection Using Graph Neural Networks [12] made changes to word embeddings, The authors use a graph generation phase, which extracts the control flow and data flow semantics from the source code and explicitly models the fallback mechanism. Besides, they use a graph normalization phase inspired by k-partite graph. At the same time, they use graph neural networks for vulnerability detection to replace traditional neural networks such as CNNs. CBGRU [16] improves both the word embedding model and the detection model. The word embedding model uses Word2Vec and FastText, and the detection model combines five deep models CNN, LSTM, GRU, BiGRU and BiLSTM for detection, making full use of the advantages of five networks to improve its vulnerability detection ability.

In terms of dynamic analysis tools [21–23, 25, 27, 28], there is no unified process. The dynamic analysis method detects the contract in the execution process, so some dynamic analysis methods do not require source code [25]. EOSIO is a typical public blockchain platform. WASAI [29] and EOSFuzzer [24] analyzed EOSIO.

HFCContractFuzzer [26] HFCCT [30] is aimed at Hyperledger Fabric platform for vulnerability detection, and HFCCT adopts the way of dynamic and static collection. In HFCCT, the authors used 15 chain codes to compare with HFCContractFuzzer. The test results show that the vulnerability detection efficiency of HFCCT is higher than that of HFCContractFuzzer, and the display of errors is clearer. We can see that the dynamic and static analysis method is more efficient than the single analysis method.

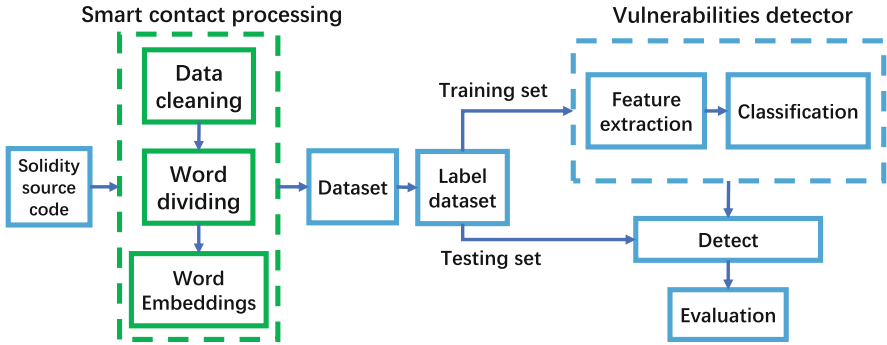


Fig. 1. Model of smart contract vulnerability detection tools using artificial intelligence

## 4 Development Direction

From the perspective of whether to run the contract, we divide all smart contract vulnerability detection tools into three categories. Through analysis and comparison, we draw the following conclusions:

### 4.1 Deep Learning

At present, machine learning and deep learning are increasingly used in vulnerability detection. In the future, Chat-GPT may be a powerful assistant for future smart contract vulnerability detection. However, a common drawback of these detection tools [13–15, 17] is that they detect fewer kinds of vulnerabilities, which may be related to the small number of existing large standard datasets.

### 4.2 Combination of Static and Dynamic Analysis

When the contract is complex, dynamic analysis has more advantages than static analysis, because the relationship between many vulnerabilities is complex, which can not be easily analyzed by simply inspecting the code files. Moreover, the coverage of dynamic analysis tools is not high. Therefore, how to improve the coverage of dynamic analysis tools is a big problem.

### 4.3 Platform and Language

Most of the current detection tools are aimed at the Ethereum platform and Solidity language. The running platform such as EOS, Hyperledger Fabric, etc., and the programming language such as Vyper language, etc. The smart contract security vulnerability of these platforms and languages are less studied, so it is also the direction of future research.

## 5 Conclusion

In the era when blockchain is more popular, smart contracts provide security for blockchain, but security of vulnerabilities in smart contracts cannot be ignored. We hope that the re-classification and summary of security vulnerabilities can also make people have a better understanding of the security issues in smart contracts. Through the analysis and comparison of detection tools, we believe that the security detection technology of smart contracts will become more and more mature, and they can also have higher efficiency and better vulnerability detection ability. Therefore, with the update and progress of technology, the security problem of blockchain will be more and more guaranteed.

**Acknowledgment.** This work was funded by Haikou Science and Technology Plan Project (2022-007).

## References

1. Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., Wang, F.-Y.: Blockchain-enabled smart contracts: architecture, applications, and future trends. *IEEE Trans. Syst., Man, Cybern.: Syst.* 49(11), 2266–2277 (2019)
2. Pise, R., Patil, S.: A deep dive into blockchain-based smart contract-specific security vulnerabilities. In: 2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), pp. 1–6. IEEE (2022)
3. Praitheeshan, P., Pan, L., Yu, J., Liu, J., Doss, R.: Security analysis methods on ethereum smart contract vulnerabilities: a survey. arXiv preprint [arXiv:1908.08605](https://arxiv.org/abs/1908.08605) (2019)
4. Kado, C., Yanai, N., Cruz, J.P., Okamura, S.: An empirical study of impact of solidity compiler updates on vulnerabilities. In: 2023 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), pp. 92–97. IEEE (2023)
5. Sun, J., Huang, S., Zheng, C., Wang, T., Zong, C., Hui, Z.: Mutation testing for integer overflow in ethereum smart contracts. *Tsinghua Sci. Technol.* 27(1), 27–40 (2021)
6. Kun, H., Bo, W., Dan, X.: A return-value-unchecked vulnerability detection method based on property graph. In: Recent Developments in Intelligent Systems and Interactive Applications: Proceedings of the International Conference on Intelligent and Interactive Systems and Applications (IISA2016), pp. 114–123. Springer (2017)
7. Mense, A., Flatscher, M.: Security vulnerabilities in ethereum smart contracts. In: Proceedings of the 20th International Conference on Information Integration and Web-Based Applications and Services, pp. 375–380 (2018)
8. Bartoletti, M., Pompianu, L.: An empirical analysis of smart contracts: platforms, applications, and design patterns. In: Financial Cryptography and Data Security: FC 2017 International Workshops, WAHC, BITCOIN, VOTING, WTSC, and TA, Sliema, Malta, April 7, 2017, Revised Selected Papers 21, pp. 494–509. Springer (2017)
9. Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., Imran, M.: An overview on smart contracts: Challenges, advances and platforms. *Futur. Gener. Comput. Syst.* 105, 475–491 (2020)

10. Zhang, X., Li, J., Wang, X.: Smart contract vulnerability detection method based on bi-lstm neural network. In: 2022 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA), pp. 38–41. IEEE (2022)
11. Yang, H., Zhang, J., Gu, X., Cui, Z.: Smart contract vulnerability detection based on abstract syntax tree. In: 2022 8th International Symposium on System Security, Safety, and Reliability (ISSSR), pp. 169–170. IEEE (2022)
12. Zhuang, Y., Liu, Z., Qian, P., Liu, Q., Wang, X., He, Q.: Smart contract vulnerability detection using graph neural networks. In: Proceedings of the Twenty-Ninth International Conference on International Joint Conferences on Artificial Intelligence, pp. 3283–3290 (2021)
13. Wang, Z., Zheng, Q., Sun, Y.: Gvd-net: graph embedding-based machine learning model for smart contract vulnerability detection. In: 2022 International Conference on Algorithms, Data Mining, and Information Technology (ADMIT), pp. 99–103. IEEE (2022)
14. Chen, W., Guo, R., Wang, G., Zhang, L., Qiu, J., Su, S., Liu, Y., Xu, G., Chen, H.: Smart contract vulnerability detection model based on siamese network. In: International Conference on Smart Computing and Communication, pp. 639–648. Springer (2022)
15. Zhang, L., Li, Y., Jin, T., Wang, W., Jin, Z., Zhao, C., Cai, Z., Chen, H.: Spcbig-ec: a robust serial hybrid model for smart contract vulnerability detection. *Sensors* **22**(12), 4621 (2022)
16. Zhang, L., Chen, W., Wang, W., Jin, Z., Zhao, C., Cai, Z., Chen, H.: Cbgru: a detection method of smart contract vulnerability based on a hybrid model. *Sensors* **22**(9), 3577 (2022)
17. Zhipeng Gao. When deep learning meets smart contracts. In: Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering, pp. 1400–1402, 2020
18. Ghaleb, A., Rubin, J., Pattabiraman, K.: etainter: detecting gas-related vulnerabilities in smart contracts. In: Proceedings of the 31st ACM SIGSOFT International Symposium on Software Testing and Analysis, pp. 728–739 (2022)
19. Schneidewind, C., Grishchenko, I., Scherer, M., Maffei, M.: Ethor: practical and provably sound static analysis of ethereum smart contracts. In: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, pp. 621–640 (2020)
20. Chen, W., Li, X., Sui, Y., He, N., Wang, H., Lei, W., Luo, X.: Sadponzi: Detecting and characterizing ponzi schemes in ethereum smart contracts. *Proc. ACM Measur. Anal. Comput. Syst.* **5**(2), 1–30 (2021)
21. Luu, L., Chu, D.H., Olickel, H., Saxena, P., Hobor, A.: Making smart contracts smarter. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 254–269 (2016)
22. Jiang, B., Liu, Y., Chan, W.K.: Contractfuzzer: Fuzzing smart contracts for vulnerability detection. In: Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering, pp. 259–269 (2018)
23. Gao, J., Liu, H., Liu, C., Li, Q., Guan, Z., Chen, Z.: Easyflow: Keep ethereum away from overflow. In: 2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion), pp. 23–26. IEEE (2019)
24. Huang, Y., Jiang, B., Chan, W.K.: Eosfuzzer: Fuzzing eosio smart contracts for vulnerability detection. In: Proceedings of the 12th Asia-Pacific Symposium on Internetworking, pp. 99–109 (2020)



25. Eshghie, M., Artho, C., Gurov, D.: Dynamic vulnerability detection on smart contracts using machine learning. In: Proceedings of the 25th International Conference on Evaluation and Assessment in Software Engineering, EASE '21, pp. 305–312. Association for Computing Machinery, New York (2021)
26. Ding, M., Li, P., Li, S., Zhang, H.: Hfcontractfuzzer: fuzzing hyperledger fabric smart contracts for vulnerability detection. In: Proceedings of the 25th International Conference on Evaluation and Assessment in Software Engineering, EASE '21, pp. 321–328. Association for Computing Machinery, New York (2021)
27. Su, J., Dai, H.N., Zhao, L., Zheng, Z., Luo, X.: Effectively generating vulnerable transaction sequences in smart contracts with reinforcement learning-guided fuzzing. In: Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering, pp. 1–12 (2022)
28. Zheng, P., Zheng, Z., Luo, X.: Park: accelerating smart contract vulnerability detection via parallel-fork symbolic execution. In: Proceedings of the 31st ACM SIGSOFT International Symposium on Software Testing and Analysis, pp. 740–751 (2022)
29. Chen, W., Sun, Z., Wang, H., Luo, X., Cai, H., Wu, L.: Wasai: uncovering vulnerabilities in wasm smart contracts. In: Proceedings of the 31st ACM SIGSOFT International Symposium on Software Testing and Analysis, pp. 703–715 (2022)
30. Li, P., Li, S., Ding, M., Yu, J., Zhang, H., Zhou, X., Li, J.: A vulnerability detection framework for hyperledger fabric smart contracts based on dynamic and static analysis. In: Proceedings of the 26th International Conference on Evaluation and Assessment in Software Engineering, pp. 366–374 (2022)
31. Grover, A., Leskovec, J.: Node2vec: scalable feature learning for networks. In: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD '16, pp. 855–864. New York, Association for Computing Machinery (2016)



# A Survey of Blockchain-Based Identity Anonymity Research

Fa Fu<sup>1</sup>(✉), Gaoshang Lu<sup>1</sup>, Jianqiang Huang<sup>2</sup>, and Thomas Dreibholz<sup>3</sup>

<sup>1</sup> Hainan University, Haikou Hainan 570228, China  
fufa@hainanu.edu.cn

<sup>2</sup> Telecom Corporation Limited Hainan Branch, Haikou Hainan 570125, China

<sup>3</sup> Simula Metropolitan Centre for Digital Engineering A/S, Pilestredet 52, 0167 Oslo, Norway

**Abstract.** With the booming development of blockchain technology, blockchain-based data transactions have been applied in many fields such as finance, healthcare and logistics. It can help users to realize data transactions and management more conveniently, securely, transparently and efficiently. However, there is a certain problem of identity privacy leakage when data transactions are conducted on blockchain. Therefore, the issue of user identity privacy protection has become the core issue of data transactions on the blockchain, which is crucial to the sustainable development and wide application of the blockchain. This paper discusses the privacy protection in the process of data transactions on blockchain in terms of user identity anonymity, introduces and analyzes in detail the current research status and implementation technologies for realizing identity anonymity on blockchain, explains the threats and challenges for realizing identity anonymity, analyzes the existing problems, and gives an outlook and summary of the future research directions for realizing identity anonymity on blockchain.

**Keywords:** Blockchain · Identity anonymous · Data transaction

## 1 Introduction

A key feature of blockchain technology is decentralization, which allows participants to conduct transactions without a central control authority and also means that transactions and data records are open and transparent to all node chains, participants' identity data may be exposed to others. However, since some private information may be involved, such as transaction amounts, medical consultation records, and trade secrets, such users want to protect their identity information from disclosure. However, when using blockchain addresses to participate in blockchain business, users need to frequently perform input and output operations. Analyzing this information can indirectly associate the true user identity of the account address, which poses a threat to privacy leakage for blockchain participants' accounts. Therefore, there is still a risk of leaking sensitive user identity information in blockchain transactions, such as the propagation trajectory of the transaction at the network layer, this information may be used to infer the true identity of the blockchain address. Therefore, how to protect user identity privacy data, prevent

user identity information from being identified and leaked, and achieve identity privacy to protect users' real identity and private information is crucial for the sustainability and wide application of the blockchain.

## **2 Blockchain Technology**

### **2.1 Blockchain**

User identity privacy refers to mapping the real-world user's real identity to his or her address information on the blockchain [1], which contains personal information such as the user's identity and address that are recorded in detail and not publicly available. Among them, the user identity information refers to the basic personal information entered by the user when applying for access to the blockchain [2], while the user address information refers to the place where the individual belongs when participating in the blockchain data storage and transmission, and usually contains two accounts used for input and output in transactions. To protect identity anonymity, users usually use random addresses or pseudonyms for transactions in the blockchain [3]. A blockchain address is a pseudonym used by users in the blockchain system and is usually used as an account number for input and output during transactions. Compared to traditional account numbers, blockchain addresses are superior in concealing the user's identity [4].

### **2.2 Smart Contracts**

Smart contracts are automated contracts that enable the signing and execution of contracts on the blockchain, a concept first introduced by Nick Szabo in 1996 in his paper "Smart Contracts: Building Blocks for Digital Markets". In Szabo's definition, a smart contract is an automatically executed contract based on a computer protocol that represents and enforces the terms of the contract in digital code. These codes allow for automated and decentralized execution of the contract and protect the security and privacy of the contract through encryption. However, in the late 1990s, computer technology was not mature enough to implement the concept of smart contracts. It was not until 2009 that the advent of Bitcoin made smart contracts possible. Born in 2013, Ether has revolutionized the face of smart contracts. Ether introduced a high-level programming language called Solidity, making it easier for developers to write more complex smart contracts and implement more features on the Ether blockchain. Since the birth of Ether, the applications of smart contracts have been expanding. Smart contracts have also become one of the most representative blockchain technologies.

## **3 Research and Analysis of Identity Anonymization Techniques**

Currently, the main technologies applied in blockchain to achieve identity anonymity include blind signature, group signature, and aggregate signature technologies. In this section, we will comprehensively analyze the advantages and disadvantages of the main signature technologies in the blockchain.

### 3.1 Blind Signature Technology

Blind signature is a digital signature technique that allows a signer to sign a message without knowing its content [5]. It has a wide range of applications in privacy protection and authentication authorization, especially in electronic cash, digital certificates, and anonymity networks. Rivest, R. L. proposed the RSA blind signature scheme in 1978 [6], which is an implementation of blind signatures based on the RSA cryptographic algorithm with better security and efficiency. This is another important contribution of the blind signature technique. Chaum, D. proposed the original blind signature scheme [7] in 1983, i.e., using a randomization technique so that the signer cannot know the content of the signature, thus enabling untraceable payments. This is one of the seminal works in blind signature techniques.

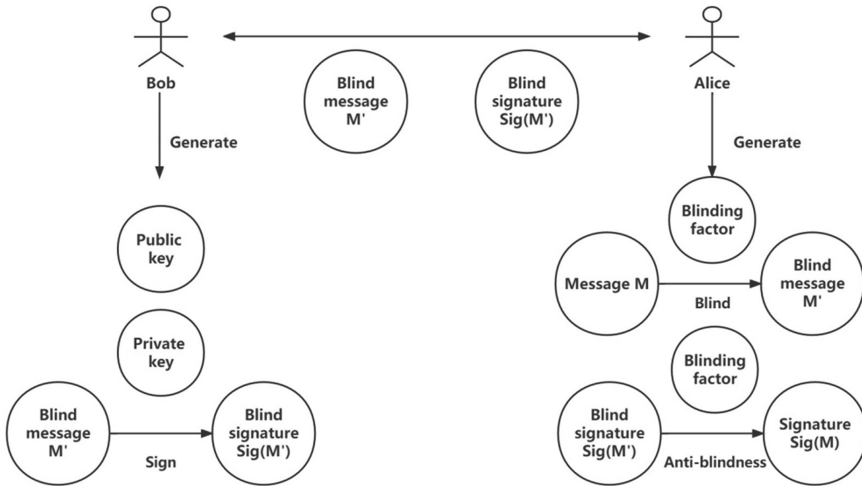
The basic principle of blind signature is that first, the signer Bob generates a pair of public and private keys [8] and publishes the public keys. Then, user Alice generates a random number as a “blind factor”, and the message  $M$  to be signed is blinded using the blind factor, the message  $M$  is multiplied by the blind factor to obtain a blind message  $M'$ . The signer Bob signs the blind message  $M'$  with his private key to get a blind signature  $\text{Sig}(M')$ , and sends the blind signature  $\text{Sig}(M')$  to Alice. to obtain the signer’s signature  $\text{Sig}(M)$  for the original message [9]. Since the blind signature process does not require the original message to be revealed to the signer, the privacy of the message can be guaranteed. The flowchart of the blind signature is shown in Fig. 1.

First, blind signatures have strong privacy; during the blind signature process, the signer does not know the specific content of the message, and thus the privacy of the message can be guaranteed [10]. Second, blind signatures have strong anonymity, and users can obtain the signer’s signature without revealing their identity, thus achieving anonymous authentication authorization. Finally, blind signatures also have high security; blind signatures have the same security as ordinary digital signatures [11], i.e., they prevent forgery and tampering. However, in addition to this, blind signatures also have some disadvantages, such as slow processing speed, blind signature processing requires blind and anti-blind operations, and thus is slower compared to ordinary digital signatures. Secondly, the complexity of the blind signature operation is high, and blind signature technology is more complex than other digital signature technologies, requiring more calculations and communications. Finally, blind signatures are irrevocable, i.e., once the signer signs, the signature cannot be revoked. If the identity of the user is exposed, the reputation of the signer may be damaged.

### 3.2 Group Signature Technology

A group signature is a digital signature mechanism used to verify the integrity and origin of a message and to prove that a particular signer belongs to a specific group. Unlike ordinary digital signatures, group signatures allow any member of a group to sign a message [12] while maintaining individual privacy. In simple terms, a group signature is a digital signature scheme that decouples the signature of a group from the identity information of a single individual.

David Chaum first introduced the concept of group signatures in 1991 [13] and introduced a cryptography-based group signature scheme that allows a group of members



**Fig. 1.** Schematic diagram of the blind signature process

to publish a message using a group signature without revealing the identity of the individual. The scheme also has a revocation function, i.e., the signer's signature can be revoked when necessary. Ronald Cramer proposed a multi-authority election scheme based on group signatures in 1997 [14], which employs multiple authorities to enhance the security and reliability of the scheme. Jan Camenisch proposed an efficient group signature scheme based on cryptography in 2004 [15], where the signature length of the scheme is independent of the swarm size and is only related to the security parameters. The scheme is efficient and secure and supports the revocation of the signature function.

A group contains multiple members, who together form the group. A member of the group signs the message, and members outside the group can verify that the message has been signed by the group, but they do not know exactly which member has signed it. This approach conceals the true signature identity and achieves the unity of anonymity and super visibility. The signature process of the group signature is shown in Fig. 2.

Group signature techniques have strong anonymity and do not require the identity of the signer to be revealed, so the signer can remain anonymous, which is important in cases where privacy needs to be protected. Group signature techniques have verifiability, i.e., the recipient can verify that the signature belongs to the group and verify the integrity and origin of the message, which ensures the authenticity and trustworthiness of the message. And finally, group signature techniques have non-repudiation i.e., signers cannot deny the messages they sign [16]. This is because the signature mechanism makes the signature unforgeable and the signers cannot claim that they did not sign the message. In addition to this, group signature techniques have some disadvantages, such as the possibility of abuse, as group signatures can be used for criminal activities or other unethical practices due to the anonymity of the signers. The signers need to be trusted, and the validity of group signatures depends on the trust of the signers. If one or more of the signers behave maliciously, it may negatively affect the validity of the signature. It is difficult to revoke. Unlike ordinary digital signatures, group signature technology is difficult to be revoked

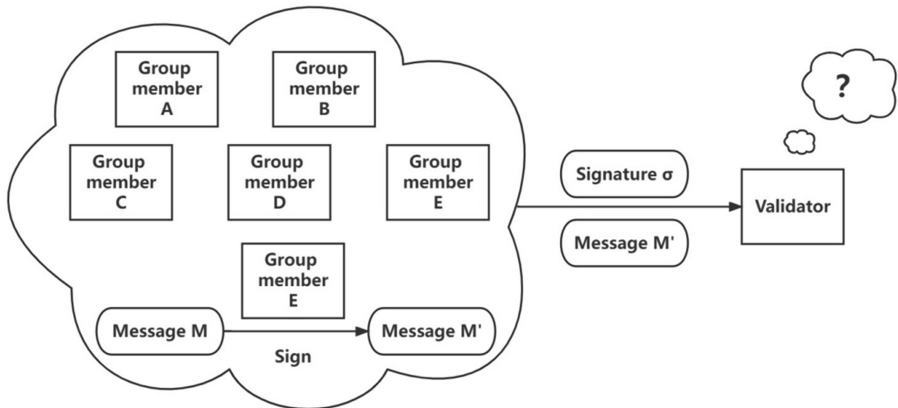


Fig. 2. Schematic diagram of the group signature process

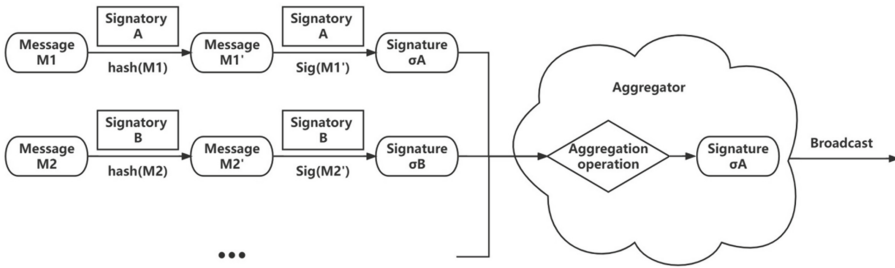
because the identity of the signer is anonymous, and if malicious behavior occurs among the signers, it is difficult to find the responsible person and revoke the signature.

### 3.3 Aggregate Signature Technology

Aggregate signature is a digital signature mechanism that can significantly reduce transaction storage space and transmission costs, and improve verification efficiency. Careful consideration needs to be given to usage scenarios and signer trust when using this technology. It allows multiple signers to sign the same message and aggregates these signatures into a single signature. In simple terms, aggregated signatures are digital signature schemes that aggregate multiple signatures into a single signature [17] and are mainly used to achieve bulk verification of transactions. Dan Boneh et al. proposed a bilinear mapping-based aggregated signature scheme [18] in 2003, which is not only efficient but also verifies the signer identity and signature integrity.

Signer A first hashes the message  $M$  to get the message digest  $M'$ , and then signs the message digest  $M'$  with his private key to get the signature  $\sigma_A$ , other signers also hash and sign their respective messages in this way to get the signature  $\sigma_B$ , signature  $\sigma_C$ , etc. All signers send their signatures to a centralized aggregator. The Aggregator combines all signatures into one signature and makes the signature public. The flowchart of aggregated signatures is shown in Fig. 3.

The aggregated signatures have some advantages. Firstly, it can reduce transaction storage space and transmission costs. Aggregated signatures allow multiple signers to aggregate their signatures into a single signature, which greatly reduces the storage space and transmission costs of the transaction. Secondly, aggregated signature technology also improves verification efficiency. A single signature of an aggregated signature can reduce the verification workload because the verifier only needs to verify one signature instead of verifying multiple. Finally, the aggregated signature technique increases privacy protection, as aggregated signatures can add anonymity and privacy protection to the signer since they can aggregate multiple signatures into a single signature. In



**Fig. 3.** Schematic diagram of the aggregated signature process

addition, aggregated signatures rely on the trust of all signers, and their validity depends on the integrity and security of all signers. If one of the signers acts maliciously, it may negatively affect the validity of the entire signature. Unlike traditional digital signatures, aggregated signatures are difficult to be revoked, because signers cannot revoke their signatures individually, if one of the signers behaves maliciously, revoking the entire signature may be very difficult. Finally, aggregated signatures may require more complex implementations and higher computational costs, and therefore may not be suitable for use in certain scenarios. According to the above analysis, the advantages and disadvantages of the three signature technologies are summarized in Table 1.

**Table 1.** Comparison of advantages and disadvantages of three technologies.

	Advantages	Deficiencies
Blind signature	High privacy Strong anonymity High security	Slow speed High complexity Irrevocable
Group signature	Strong anonymity Verifiability Non-deniability	Slow speed Unprecedented overheads Large signature length
Aggregate signature	Reduce transaction storage space and transmission costs Improve validation efficiency Increase privacy protection	Potential for abuse Signers need to be trusted Difficult to revoke

### 4 Future Research Directions

Through the comparative analysis of different blockchain identity anonymity technologies, we can see that many researchers have proposed various identity anonymity technologies on the blockchain to guarantee the privacy and security of users, but there are still several aspects that need further research.

- (A) Performance problem: Since all data on the blockchain is public, achieving anonymity requires broadcasting encrypted transactions in the network and waiting for some time for each identity verification, which can increase the burden of network transmission and computation and lead to performance degradation. As proposed in the literature [19] based on homomorphic encryption, each participant in this scheme needs to perform a large number of encryption and decryption operations, which also affects the performance of the system due to the slow encryption and decryption speed of homomorphic encryption. Then there is a scheme based on the obfuscation technique proposed in the literature [20], in this scheme, all participants need to perform obfuscation operations, and the obfuscation operations consume a large amount of computational resources, which also affects the performance of the system. Therefore future research work needs to seek more efficient anonymity guarantee schemes and explore more efficient consensus algorithms to improve transaction processing speed. For example, using zero-knowledge proofs to protect privacy [21] without using homomorphic encryption or obfuscation techniques can achieve efficient privacy protection with high performance, and using cryptographic multi-party computation to protect privacy [22] can compute the corresponding results without exposing the original data, and the performance can be improved by parallel computation. More research is still needed on performance optimization and evaluation methods.
- (B) Implementing identity anonymity may involve legal compliance issues and anonymous identities may be used for illegal activities. Therefore, to achieve sustainable development of blockchain, future research efforts need to target technical means and solutions to achieve privacy protection while achieving technical controllability, such as using identity to authenticate and authorize participants, using traceability to track participants' behavior, and helping regulators identify illegal activities through ways and means such as government certification and blockchain identity certification agencies. Thus, how to develop regulatory standards to further ensure the legitimacy and transparency of data usage to avoid data misuse and mishandling is an important research issue.
- (C) Compatibility issues: Implementing anonymity protection in current blockchain technologies may encounter compatibility issues. Public data on the blockchain can improve transparency and trust, but some sensitive data, just like the privacy of users need to be protected. This requires appropriate encryption measures to ensure data security and privacy protection while keeping the data open. Therefore, future research work needs to develop more compatible blockchain technologies to solve this problem, such as promoting trusted blockchain technologies, such as federated chains and side chains, to meet the demand for identity anonymity in different scenarios.

## 5 Summary

This paper compares and contrasts different technologies of protecting identity anonymity for data transactions on the blockchain, analyzes the advantages and disadvantages of each technology and the applicable environment, and provides an outlook on the future direction of implementing identity anonymity for data transactions on



the blockchain, to help researchers quickly and comprehensively understand the basic content and development trend of blockchain identity anonymity technology and future research directions. With the maturity of blockchain technology and its wide application in various industries, the realization of identity anonymity is of great research significance for the sustainable development of blockchain, and we still need to continue to study this area and create a more perfect and practical identity anonymity solution.

**Acknowledgment.** This research was funded by Haikou Science and Technology Plan Project (2022–007).

## References

1. Yu, X.: Blockchain privacy protection key technology research and application. *Inf. Technol.* **3**(5), 36–50 (2020)
2. Liu, H.O., Zhou, Y.Y., Zhou, X., et al.: A review of blockchain privacy threats and protection mechanisms research. *Comput. Integrat. Manufact. Syst.* **3**(9), 1–25 (2023)
3. Yu, P.: Blockchain-based research on privacy data protection and sharing of electronic medical records. *Inf. Technol.* **1**(8), 25–41 (2020)
4. Song, Y.C., Ning, X.Y.: Blockchain technology risk assessment and control. *Financ. Account. Mon.* **14**(9), 124–140 (2021)
5. Wu, Y.X.: Research on group blind signature and multi-bank electronic cash system. *Inf. Technol.* **11**(2), 31–45 (2014)
6. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**(2), 120–126 (1978)
7. Chaum, D.: Blind Signatures for Untraceable Payments. *Adv. Cryptol.* **15**(2), 19–22 (1983)
8. Wang, Y.: Research on automatic trust negotiation protocol based on secure multi-party computation. *Inf. Technol.* **6**(1), 49–65 (2012)
9. Liu, D.: A blind signature based on combined public key cryptography. *Fujian Comput.* **31**(2), 21–32 (2015)
10. Gong, Z.Y.: IoT privacy protection based on partial blind signature algorithm. *Modern Trade Ind.* **41**(25), 111–123 (2020)
11. He, B.: A study of forward-secure proxy blind signature scheme. *Inf. Technol.* **3**(2), 23–39 (2014)
12. Lei, Y.C.: Blockchain privacy protection scheme based on group signature. *Inf. Technol.* **5**(3), 42–58 (2020)
13. Chaum, D., Heyst, E.V.: Group signatures. In: *Advances in Cryptology - EUROCRYPT '91, Lecture Notes in Computer Science*, vol. 547, pp. 257–265 (1991)
14. Cramer, R., Gennaro, R., Schoenmakers, B.: A secure and optimally efficient multi-authority election scheme. *Trans. Emerg. Telecommun. Technol.* **8**(5), 481–490 (1997)
15. Camenisch, J.: Efficient group signature schemes for large group. In: *Advances in Cryptology - CRYPTO'97, Lecture Notes in Computer Science*, vol. 1294, pp. 410–424 (1997)
16. Lu, D.J., Wang, Y.: An identity-based gated proxy signature scheme. *Basic Sci.* **26**(01), 1–14 (2010)
17. An, T.: Research and application of data security privacy protection methods in cloud environment. *Inf. Technol.* **5**(9), 22–38 (2020)
18. Boneh, D., Gentry, C., Lynn, B., et al.: Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In: Biham, E. (ed.) *EUROCRYPT 2003, LNCS*, vol. 2656, pp. 416–432. Springer, Heidelberg (2003)

19. Miers, I., Garman, C., Green, M., et al.: Zerocoin: anonymous distributed E-cash from bitcoin. In: Symposium on Security and Privacy, pp. 397–411. IEEE, San Francisco (2013)
20. Bonneau, J., Narayanan, A., Miller, A., et al.: Mixcoin: Anonymity for Bitcoin with accountable mixes. In: Christin, N., Safavi-Naini, R. (eds.) International Financial Cryptography Association 2014, LNCS, vol. 8437, pp. 486–504. Springer, Berlin (2014)
21. Bowe, S., Chiesa, A., Green, M., et al.: ZEXE: enabling decentralized private computation. In: Symposium on Security and Privacy, pp. 947–964. IEEE, San Francisco (2020)
22. Damgård, I., Keller, M., Larraia, E., et al.: Practical covertly secure MPC for dishonest majority – or: breaking the SPDZ limits. In: Advances in Cryptology - EUROCRYPT 2013, Lecture Notes in Computer Science, vol. 7887, pp. 463–480 (2013)



# Blockchain-Based Central Bank Digital Currencies: A Comprehensive Survey

Shuo Chen<sup>1</sup>, Zhiwei Liu<sup>1,2</sup>, Xiang Xu<sup>1</sup>, Haoyu Gao<sup>1,2</sup>, Hong Lei<sup>1,4(✉)</sup>, and Chao Liu<sup>3</sup>

<sup>1</sup> School of Cyberspace Security, Hainan University, Haikou 570228, China  
1434801240@qq.com, liuzhiwei@hainanu.edu.cn, xuxiangoc@163.com,  
1095055672@qq.com, leiluono1@163.com

<sup>2</sup> Oxford-Hainan Blockchain Research Institute, Chengmai 571924, China

<sup>3</sup> The Blockhouse Technology Limited, Oxford OX2 6XJ, UK

liuchao@tbtl.com

<sup>4</sup> SSC Holding Company Ltd, Chengmai 571924, China

**Abstract.** In this information age, real currency is transitioning to digital currency. Blockchain technology has introduced smart contracts and distributed ledger technology, leading to new research directions in various fields including finance, the Internet of Things, and energy. Central Bank Digital Currency (CBDC) based on blockchain has been incorporated into the technical choices of central banks in various countries. This paper examines the current research and implementation of central bank digital currency by various central banks worldwide. It provides an overview of CBDC's definition, operational status, and technical characteristics. Additionally, this paper highlights the challenges and issues associated with CBDC systems in the current environment. These problems include security issues, performance issues, privacy protection issues, and legal issues. In this regard, some literature has proposed solutions, which are analyzed and summarized in this paper. We classify and summarize the existing problems and propose effective solutions, including using fragmentation technology to increase transaction throughput and implementing corresponding regulatory measures to strengthen supervision.

**Keywords:** Central bank digital currency · Blockchain · Smart contract · Distributed ledger technology

## 1 Introduction

Today, in the era of electronic currency innovation, the modern monetary economy has gradually entered the era of digital currencies. The decreasing use of physical cash around the world and the development of private digital currencies such as Bitcoin have sparked interest among central banks in Central Bank Digital Currency (CBDC), and banks such as the Bank of Canada, Deutsche Bank, Banque de France, and the Bank of Japan (BOJ) have launched digital currency-related projects [1]. The research focus in the field of digital currency is gradually shifting from decentralized encrypted digital currency to legal digital currency based on the central bank of the country.

The Bank for International Settlements (BIS) and the central banks of China, the European Union, the United States, and other countries put forward the definition of CBDC based on research and practice. (Table 1) [2, 3].

According to survey data from the BIS, central banks around the world generally hold an optimistic outlook on the prospects of CBDC. The main goals of CBDC are to improve delivery security, robustness, and transaction efficiency, reduce issuance costs, and increase transaction convenience. Many central banks worldwide are actively exploring CBDC issuance and implementation to adapt to the digital age's economic advancements [4].

The classification of currency is based on the following attributes: (1) issuing subject (central bank currency or commercial bank currency); (2) form (digital or physical); (3) value attribute (standard currency or credit currency); (4) circulation method (cash or non-cash currency). By definition, CBDC is a digital currency issued by a central bank. According to its scope and purpose of use, CBDC can be divided into retail and wholesale types.

**Retail CBDC.** Retail CBDC refers to the digital currency issued directly to the public by the central bank, similar to the current paper money and coins, which can be used to purchase goods and services. Retail CBDC is issued to the general public, so the technical design and distribution methods need to take into account the extensive use and safety [5].

**Wholesale CBDC.** Wholesale CBDC refers to the digital currency issued by the central bank to financial institutions and large enterprises, which is mainly used for settlement and clearing transactions between institutions. The wholesale CBDC is issued to financial institutions, so the technical design and distribution methods must consider efficiency and security [6].

The main difference between retail and wholesale distribution is the object and the purpose of distribution. The main difference between retail distribution and wholesale distribution is the object and purpose of distribution. The wholesale type is mainly issued for financial institutions, and the main purpose is to carry out large-scale transactions between institutions, while the retail type is for the public, and the main purpose is daily consumption and wage payment.

In 2018, the BIS and the Committee on Payment and Market Infrastructure (CPMI) released a report [2] that highlighted the varying motivations and priorities of major countries or economies when it comes to developing CBDC. Table 1 summarizes the definition of CBDC by mainstream economies. The report showed that emerging market economies are more inclined to promote retail CBDC compared to developed economies [7]. Retail CBDC has a stronger research motivation than wholesale CBDC, and emerging market economies have a stronger research motivation for CBDC than developed economies. For emerging market economies, improving domestic payment efficiency, payment security, and financial stability is crucial, as many smaller economies do not have a real-time full settlement system for their currencies. In contrast, improving cross-border payment efficiency is one of the most important motives for developed economies.

CBDC can use blockchain technology to achieve transaction security and transparency. By writing transaction records into the blockchain, the security and non-tamperability of transactions can be guaranteed. At the same time, blockchain technology

**Table 1.** Comparison of CBDC definitions by major financial institutions worldwide.

Institution	Definition
BIS	BIS believes that the central bank digital currency is a digital form of cash issued by the central bank, which can be used for payment and settlement on different technology platforms, and needs to take into account its impact on financial stability and privacy protection
European Central Bank	The ECB believes that CBDC should be a tool to supplement existing payment methods, rather than an alternative, and its impact on financial stability and monetary policy needs to be taken into account
Federal Reserve System	The Fed believes that the issuance of CBDC needs to consider its impact on financial stability, monetary policy, and privacy protection. The Fed also points out that the design of CBDC should fully consider interoperability with existing payment systems
People's Bank of China	The PBOC has initiated testing of the digital Renminbi, which is the central bank digital currency of China. The PBOC believes that the digital renminbi will enhance payment efficiency, foster financial innovation, and uphold national monetary sovereignty
Bank of Japan	BOJ believes that the issuance of CBDC needs to take into account its impact on financial stability and payment systems. It is also necessary to fully consider its interoperability with existing payment systems and user privacy protection

can also reduce the cost of CBDC issuance, improve the efficiency of transactions, [8, 9] and gain incomparable advantages over traditional currencies.

Centralized CBDC uses decentralized blockchain technology to improve security and reliability. Blockchain technology solves the problem of single point of failure and central server risk that is easy to occur in centralized systems and improves the robustness of CBDC. However, the use of decentralized technology does not mean that CBDC is completely decentralized. For Internet products with financial attributes, strict supervision and review by government agencies are needed to prevent the emergence and proliferation of criminal acts.

The rest of this paper is organized as follows. The second section introduces the related concepts of blockchain and CBDC. The third section summarizes the current academic research and ideas. The fourth section summarizes the existing problems and challenges of CBDC and puts forward some suggestions for these problems. The fifth section summarizes the paper.

## 2 Background

### 2.1 Blockchain Technology

The blockchain is a special data structure composed of a series of blocks, each of which can store some information. The information that needs to be stored on the chain is packaged into blocks, and the blocks are linked to each other to form an orderly, non-tamperable chain event, which is stored on each node. This information is permanently stored in a peer-to-peer (P2P) network composed of independent participant nodes [10]. Blockchain is a decentralized, secure, reliable, transparent technology that can be used in various application scenarios, including digital currency, the Internet of Things, and supply chain management.

**Account Balance Model and Unspent Transaction Output Model (UTXO).** The balance model is a simple payment system where user accounts store identifiers for authorization management, while the UTXO model tracks unpaid funds with a ledger of accounting entries [11]. Users must authenticate themselves to access their accounts and authorize transactions in the balance model, while the UTXO model involves creating and authorizing transactions that balance input values with output values. Ethereum and some digital currencies use the balance model, while the UTXO model is used in Bitcoin and other cryptocurrencies.

**Smart Contract.** Ethereum is an open blockchain platform that allows anyone to establish and use decentralized applications through blockchain technology. It is controlled and owned by no one, and its design is flexible and adaptable. Ethereum has Turing completeness, allowing it to implement smart contracts which are not possible in Bitcoin. Smart contracts are programs stored on the blockchain that can automate protocols and trigger the next operations when conditions are met, without any mediation involvement or time loss.

**Access Mechanism.** Blockchain can be divided into three categories: Consortium Chain, Public Chain, and Private Chain from the access mechanism. The public chain refers to an open network in which anyone can participate, create blocks, and verify transactions in the network at any time. The public chain is characterized by decentralization, and high safety performance, but weak performance. The Consortium chain refers to a blockchain network formed by an alliance of multiple organizations or enterprises. Only verified members can join the network. The characteristics of the alliance chain are high efficiency and good privacy. A private chain is a blockchain network controlled by a single subject, which is extremely centralized and more often used within a single enterprise. Different forms of blockchain technology, each with its characteristics, have different applications in different scenarios.

The data on the blockchain is transparent, tamper-proof, and can be permanently saved. Smart contracts provide transparency and efficiency to transactions, as encrypted records of transactions are shared among participants without third-party involvement.

### 2.2 Cbdc

**Distribution and Operation Structure.** CBDC represents the central bank's digital currency, and its issuance and operation structure is completely managed by the central

bank. This process usually includes the following aspects [12]: the issuance of CBDC, storage of CBDC, CBDC transaction, risk management of CBDC, and regulation of CBDC.

The distribution and structure of CBDC depend on the objectives and capabilities of the central bank and need to be considered comprehensively [13]. Cooperation with other institutions can also play a role in promoting the development of CBDC.

**CBDC Design Features.** In the design of CBDC, several aspects need to pay attention to. (1) How to calculate interest, different central banks have different approaches to designing interest rates for their CBDC [14]. (2) Off-line function, offline functionality has been challenging to implement in practice, with varying definitions of what constitutes an offline transaction. While offline typically means disconnected from the internet but still relying on local networks like Bluetooth, events like power outages or electromagnetic interference can also disrupt local networks. (3) In terms of technology selection, a centralized network or distributed network has its advantages and disadvantages. The centralized network has better risk control and management efficiency, but the problems of private security and single point of failure are more serious. Which technology to use needs to be carefully selected [15]. (4) Anonymity, the degree of anonymity relates to the difficulty of promotion. (5) In cross-border payments, central bank e-money has natural advantages in cross-border transactions. For example, compared with traditional currency systems, central bank digital currency is faster and more efficient in completing cross-border payments, and the whole process is traceable. This can be promoted as an advantage of CBDC [16].

### 2.3 Summary of the Current Status of CBDC Operations

Table 2 shows the summary information of CBDC that has been released so far by major economies around the world [17–25]. This table shows that governments led by China are actively promoting the work of CBDC. Some countries such as Russia, and the United Kingdom have been promoting CBDC for several years, and China has carried out pilot testing work many times, from which we can see that the international community has a high degree of recognition of CBDC.

In addition, the United States and the European Union are paying more and more attention to the central bank's digital currency in related fields, and relevant departments are also actively preparing for the issuance of CBDC.

## 3 Existing Literature Review

The emergence of blockchain technology has brought distributed ledger technology and smart contract technology, which provides a new solution to solve the problems of CBDC supervision, risk control, and operational efficiency. At present, many central banks are exploring the application of blockchain technology in CBDC, and the academic community has conducted a lot of research and ideas on CBDC based on blockchain.

About the confusion of CBDC types between different organizations, Hyunjun Jung proposed a method to realize the interoperability between different CBDCs by using

**Table 2.** CBDC project information summary.

Name	Technical feature	Operation situation
Digital currency electronic payment	Double-Layer structure	The promotion will start in 2021 and is being promoted in pilot cities
Digital cash	Know Your Customer and Anti-Money Laundering, Multifactor Authentication	In the pilot use, it is constantly improving
Petro	Linked to oil, using POS incentives and a certain amount of money	Affected by the government, the acceptance is limited
Dinero electrónico	New coins are obtained by algorithm mining, completely decentralized	Stopped running
E-krona	Asset Guarantee, centralized management, and Supervision	It is still in the development stage
Restricted access coin	Centralized ledger, highly scalable, consensus algorithm without workload proof	Market acceptance is not clear, still need to observe
Digital ruble	Anti-counterfeiting technology to protect monetary sovereignty and data privacy	Has not yet begun to promote

blockchain and cross-chain technology. This method uses the existing cross-chain protocol to realize the interoperability between different CBDCs and improve the circulation of CBDCs [26]. Sushil Kumar proposed a CBDC architecture based on a consortium blockchain. The system is divided into the distribution layer and the user layer. The wholesale CBDC and retail CBDC are implemented in different layers, which provides an idea for the implementation of CBDC [27].

According to Reference [28], this paper proposes a CBDC framework based on blockchain, including three layers: regulatory layer, network layer, and user layer, which consists of a core module, transaction module, and identity authentication module. The alliance chain technology is used to realize the comprehensive management of CBDC, and the privacy and security of CBDC are guaranteed by zero-knowledge proof and smart contract technology. The framework provides a safe, efficient, and comprehensive digital currency management platform, improves the efficiency of payment, and provides regulatory and compliance review tools. According to Reference [29], a CBDC design and implementation scheme based on the Consortium Chain and Proof of Authority consensus mechanism is proposed, which is divided into three modules: account module, transaction module, and supervision module. The payment function of the transaction module is based on the smart contract of the Cosmos blockchain, which can automatically execute, settle and verify the transaction's legitimacy and effectiveness, and avoid malicious operations. The supervision module consists of smart contracts and supervision



nodes. Through the cooperation of smart contracts and regulatory nodes, CBDC accounts and transaction information are automatically audited and supervised. The supervision module can use smart contracts and algorithms to automatically identify and process risk events, statistically analyze transaction data, conduct data audits, etc., to achieve efficient and accurate supervision. The adjustment of authentication and authorization and regulatory strategies, require the personnel of the regulatory agency to operate and make decisions to ensure the effective and compliant operation of the regulatory module.

J. Zhang proposes a new operation mode is proposed, which uses KYC/AML verification, transaction restrictions, transaction records, and risk management to control risks. The account module of CBDC adopts the KYC/AML mechanism, and the transaction module uses smart contract technology [30]. The transaction records are traceable and transparent. The design also includes risk management and emergency response mechanisms to achieve comprehensive supervision of CBDC. The use of smart contract technology and blockchain technology has improved the efficiency of supervision. Regarding privacy issues, according to a survey by Abdul Jabbar, consumers have a negative attitude toward the privacy leaks that CBDC may cause. However, if the use of CBDC can bring obvious benefits, most people are willing to accept these risks [31].

Finally, aiming at the problem of insufficient performance, J. Xu proposed a series of optimization methods for CBDC [32], including the use of parallel distributed architecture, fast and efficient POS consensus mechanism [33], and hash-based data compression technology [34]. These methods can improve the processing speed and throughput of CBDC while ensuring its security and reducing the demand for storage space and bandwidth.

## 4 Challenge and Future Directions

CBDC, like traditional currency, is an officially recognized legal currency and an upgrade of traditional currency in the digital age. However, as a new technology, although all sectors of society are optimistic about it, there are still many challenges to be solved to truly apply it on a large scale. This part summarizes the challenges and problems encountered by CBDC and looks forward to the future research direction.

### 4.1 Challenge

The current challenges of CBDC are mainly focused on the following aspects.

**Technology Selection Issues.** Due to financial supervision and expansion requirements, CBDC mostly adopts the alliance chain rather than the fully decentralized public chain. Although a few organizations have developed CBDC based on bitcoin networks, such as Wrapped Bitcoin, and Liquid Network. Most countries have chosen an alliance chain. Choosing the appropriate underlying network is of great significance to the promotion of CBDC. Central banks need to choose the appropriate network structure according to their situation.

**Scalability.** The financial system needs the ability to have high concurrency and secure transactions. Compared with the existing financial system, the TPS of the blockchain network is far from enough. Although some scholars have proposed some

optimization schemes to increase the TPS of the blockchain to thousands, there are many limitations of these schemes and further experiments are needed [35]. The existing financial system usually requires thousands of TPS to meet demand [36].

**Working Environment.** The use of CBDC also needs to be discussed. The payment method using the Internet is not as easy to be accepted as paper money. For example, there is a conflict between electronic payment and cash payment on the Internet in China, electronic payment has a technical threshold for some elderly people. As an official currency, CBDC should be free for all people to use, but there is no difference between the current CBDC payment and electronic payment, so we need a more understandable and acceptable means of payment.

**Privacy and Regulation.** Legal and regulatory issues for digital currency need to be unified. Electronic money has anonymity, but too much anonymity can make it difficult to supervise. Legislation on the legal status of digital currency issuance is important. Privacy and data issues for users of digital currency must also be considered, with a need to balance regulatory and privacy concerns while paying attention to security issues [37–40].

**Integration with Existing Systems.** The integration of CBDC and the existing financial system needs more consideration. At present, the world financial system tends to be stable, and the addition of CBDC may have some impact on the current situation [41]. Although the central bank's digital currency has a positive effect on the financial system, there will be many problems in the process of integration [42]. For example, how to guide users to start using the central bank digital currency, who will supervise the central bank digital currency, and how to define the power of the currency-issuing department. Although these problems will not hinder the final realization of CBDC, they will have an impact on the speed of CBDC.

## 4.2 Future Directions

Although many scholars have improved and optimized the blockchain technology and CBDC scheme, more efforts are still needed to promote CBDC on a global scale. Future research should deepen the application of blockchain technology in CBDC, closely link the non-tampering, traceability, transparent process, and other characteristics of blockchain with CBDC, improve the privacy security and system stability of CBDC, improve the scalability of the system, improve the user's acceptance of CBDC, and reduce the risk challenges that CBDC may face. The central bank needs to carefully choose the technology suitable for the development of CBDC according to its specific situation. The public blockchain provides higher decentralization and transparency, but requires higher security and scalability, while the consortium blockchain provides better security and transaction speed. To improve the performance of CBDC, blockchain fragmentation technology [43] and side chain technology [44] can be applied to the blockchain. The central bank's testing and review process of CBDC should be thorough to identify and reduce CBDC-related risks. CBDC should be easy to use and interoperable with existing payment systems. The government should introduce laws and regulations to protect users and strengthen supervision.

## 5 Conclusion

Since the advent of blockchain technology in 2008, its distribution, security, transparency, and non-tampering technical characteristics have attracted wide attention. Due to the shortcomings of Bitcoin, such as high volatility, high energy consumption, and difficulty in supervision, governments tend to use blockchain technology to issue their CBDC. This paper first summarizes the current definition of CBDC by mainstream organizations and countries, introduces the views of central banks on CBDC, and then analyzes some improvement schemes of CBDC and blockchain technology in academia. At present, CBDC is still in the testing stage on the whole, and the CBDC of major central banks has not yet been formally promoted on a large scale. The reason is that CBDC has many problems and challenges to be solved, such as insufficient scalability, unclear technical options, and insufficient system ease of use. Finally, this paper proposes effective solutions to these problems and provides direction and guidance for subsequent research.

**Acknowledgments.** This work was supported in part by the National Key R&D Program of China (No. 2021YFB2700600); in part by the Finance Science and Technology Project of Hainan Province (No. ZDKJ2020009); in part by the National Natural Science Foundation of China (No. 62163011); in part by the Research Startup Fund of Hainan University under Grant KYQD(ZR)-21071.

## References

1. Duffie, D.: Building a stronger financial system: opportunities for a digital dollar. In: Central Bank Digital Currency Considerations, Projects, Outlook (2021)
2. Central bank digital currencies: foundational principles and core features, <https://www.bis.org/publ/othp33.htm>, last accessed 2021/3/12
3. Ozili, P.K.: Central bank digital currency research around the world: a review of the literature. *J. Money Launder. Control* **26**(2), 215–226 (2023)
4. Li, J., Yuan, Y., Wang, F.: The development status and prospect of digital currency based on blockchain. *Autom. Sin. (JAS)* **47**(4), 715–729 (2021)
5. Kiff, J., et al.: A survey of research on retail central bank digital currency (2020)
6. Opore, E.A., Kim, K.: Design practices for wholesale central bank digital currencies from the world. In: Symposium on Cryptography and Information Security, Japan (2020)
7. Results of the 2021 BIS survey on central bank digital currencies, Bank for International Settlements, <https://www.bis.org/publ/bisbull33.htm>, last accessed 2021/9/1
8. Javarone, M.A., Wright, C.S.: From Bitcoin to Bitcoin cash: a network analysis. In: 1st Workshop Proceedings on Cryptocurrencies and Blockchains for Distributed Systems, pp. 77–81 (2018)
9. Tschorsch, F., Scheuermann, B.: Bitcoin and beyond: a technical survey on decentralized digital currencies. *IEEE Commun. Surv. Tutor.* **18**(3), 2084–2123 (2016)
10. Nakamoto, S., Bitcoin, A.: A peer-to-peer electronic cash system **4**(2), 15 (2008). <https://bitcoin.org/bitcoin.pdf>
11. Nagayama, R., Banno, R., Shudo, K.: Trail: An architecture for compact UTXO-based blockchain and smart contract. *IEICE Trans. Inf. Syst.* **105**(2), 333–343 (2022)

12. Li, D., Wong, W.E., Pan, S., et al.: Design principles and best practices of central bank digital currency. *Int. J. Perform. Engin.* **17**(5), 411 (2021)
13. Yao, Q.: A systematic framework to understand central bank digital currency. *Sci. China Inf. Sci.* **61**, 1–8 (2018)
14. Zhang, T., Huang, Z.: Blockchain and central bank digital currency. *ICT Express* **8**(2), 264–270 (2022)
15. Soltani, R., Zaman, M., Joshi, R., et al.: Distributed ledger technologies and their applications: a review. *Appl. Sci.* **12**(15), 7898 (2022)
16. Opare, E.A., Kim, K.: A compendium of practices for central bank digital currencies for multinational financial infrastructures. *IEEE Access* **8**, 110810–110847 (2020)
17. Bhattacharya, D.: Digital Yuan (e-CNY): China’s official digital currency. *Strat. Anal.* **46**(1), 93–99 (2022)
18. Auer, R., Frost, J., Gambacorta, L., et al.: Central bank digital currencies: motives, economic implications, and the research frontier. *Ann. Rev. Econ.* **14**, 697–721 (2022)
19. Ometov, A., Bezzateev, S., Mäkitalo, N., et al.: Multi-factor authentication: a survey. *Cryptography* **2**(1), 1 (2018)
20. Bouchaud, M., Lyons, T., Saint Olive, M., et al.: Central banks and the future of digital money. *ConsenSys AG Whitepaper 01–20* (2020)
21. Söderberg, G.: The e-krona—Now and for the future. *Sveriges Riksbank Econ. Comment.* (8) (2019)
22. Danezis, G., Meiklejohn, S.: Centrally banked cryptocurrencies. arXiv preprint [arXiv:1505.06895](https://arxiv.org/abs/1505.06895), 25–51 (2015)
23. Blakstad, S., Allen, R., Blakstad, S., et al.: Central bank digital currencies and cryptocurrencies. In: *FinTech Revolution: Universal Inclusion in the New Financial Ecosystem*, pp. 87–112 (2018)
24. Shirai, S.: *Money and Central Bank Digital Currency* (2019)
25. Zohar, A.: Bitcoin: under the hood. *Commun. ACM* **58**(9), 104–113 (2015)
26. Jung, H., Jeong, D.: Blockchain implementation method for interoperability between CBDCs. *Future Internet* **13**(5), 133 (2021)
27. Kumar, S.: Permission blockchain network based central bank digital currency. In: *2021 IEEE 4th International Conference on Computing*, pp. 1–6 (2021)
28. Han, X., Yuan, Y., Wang, F.Y.: A blockchain-based framework for central bank digital currency. In: *2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, pp. 263–268 (2019)
29. Han, J.: Cos-CBDC.: Design and Implementation of CBDC on cosmos blockchain. In: *2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pp. 303–308 (2021)
30. Zhang, J., Tian, R., Cao, Y., et al.: A hybrid model for central bank digital currency based on blockchain. *IEEE Access* **9**, 53589–53601 (2021)
31. Jabbar, A., Geebren, A., Hussain, Z., et al.: Investigating individual privacy within CBDC: a privacy calculus perspective. *Res. Int. Bus. Financ.* **64**, 101826 (2023)
32. Cao, Y., Zhang, J., Yuan, X., et al.: A hybrid blockchain system based on parallel distributed architecture for central bank digital currency. In: *International Conference on Fuzzy Systems and Data Mining*, pp. 1138–1145 (2019)
33. King, S., Ppcoin, N.S.: Peer-to-peer crypto-currency with proof-of-stake. *Self-Publish. Paper* **19**(1) (2012)
34. Sundaeswaran, N., Sasirekha, S., Paul, I.J.L., et al.: Optimised KYC blockchain system. In: *2020 International Conference on Innovative Trends in Information Technology (ICITIIT)*, pp. 1–6 (2020)
35. Lee, Y.: A survey on security and privacy in blockchain-based Central Bank Digital Currencies. *J. Internet Serv. Inf. Secur.* **11**(3), 16–29 (2021)

36. Hong, Z., Guo, S., Li, P.: Scaling blockchain via layered sharding. *IEEE J. Sel. Areas Commun.* **40**(12), 3575–3588 (2022)
37. Barrdear, J., Kumhof, M.: The macroeconomics of central bank digital currencies. *J. Econ. Dyn. Control* **142**, 104148 (2022)
38. Nabilou, H.: Testing the waters of the Rubicon: the European central bank and central bank digital currencies. *J. Bank. Regul.* **21**, 299–314 (2020)
39. Belke, A., Beretta, E.: From cash to central bank digital currencies and cryptocurrencies: a balancing act between modernity and monetary stability. *J. Econ. Stud.* **47**(4), 911–938 (2020)
40. Khan, J., Abbas, H., Al-Muhtadi, J.: Survey on mobile user's data privacy threats and defense mechanisms. *Proc. Comput. Sci.* **56**, 376–383 (2015)
41. Ozili, P.K.: Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Rev.* **18**(4), 329–340 (2018)
42. Qian, Y.: Central Bank Digital Currency.: optimization of the currency system and its issuance design. *China Econ. J.* **12**(1), 1–15 (2019)
43. Wang, J., Chenchen, H., Xiaofeng, Y., et al.: Distributed secure storage scheme based on sharding blockchain. *Comput., Mater. Contin.* **70**(3), 4485–4502 (2022)
44. Singh, A., Click, K., Parizi, R.M., et al.: Sidechain technologies in blockchain networks: an examination and state-of-the-art review. *J. Netw. Comput. Appl.* **149**, 102471 (2020)



# A Survey on the Integration of Blockchain Smart Contracts and Natural Language Processing

Zikai Song<sup>1</sup>, Pengxu Shen<sup>1</sup>, Chuan Liu<sup>1</sup>, Chao Liu<sup>2</sup>, Haoyu Gao<sup>1,3</sup>,  
and Hong Lei<sup>1,4</sup> (✉)

<sup>1</sup> School of Cyberspace Security, Hainan University, Haikou 570228, China  
1095055672@qq.com, leiluono1@163.com

<sup>2</sup> The Blockhouse Technology Limited, Oxford OX2 6XJ, UK  
liuchao@tbt1.com

<sup>3</sup> Oxford-Hainan Blockchain Research Institute, Chengmai 571924, China

<sup>4</sup> SSC Holding Company Ltd, Chengmai 571924, China

**Abstract.** Smart contract is an automated contract system based on blockchain technology, which is self-executing, tamper-evident and decentralized. The writing and analysis of smart contracts still face several challenges, including complex programming languages and potential security vulnerabilities. Natural Language Processing (NLP) as a discipline that studies the interaction between natural language and computers, can provide strong support for the development and analysis of smart contracts. This paper explores the cross-application of blockchain, smart contracts and NLP. First, this paper introduces the basic principles of blockchain technology and the concept of smart contracts. Then it points out the problems in the development process of smart contracts, and focuses on the analysis and summary of the relevant research results of NLP technology in the generation of smart contract code and annotation generation, and summarizes and analyzes the important role of NLP technology on the efficiency of smart contract development, the correctness, reliability, readability, and maintainability of the code. Secondly, for the security of smart contracts, the research related to smart contract vulnerability detection using NLP technology is summarized. Finally, the advantages, challenges and future development directions of combining natural language processing with blockchain smart contracts are pointed out to provide reference and inspiration for research and application in related fields.

**Keywords:** Blockchain · Smart contract · Natural language processing

## 1 Introduction

With the rapid development of blockchain technology, smart contracts, as an important part of blockchain, have attracted wide attention. Blockchain technology provides revolutionary solutions for many fields, including finance, supply chain management, and digital assets [1], through decentralized, tamper-resistant, and verifiable features [2]. As an automatically executed computer program, smart contract realizes trust mechanism and business logic by writing contract code, which provides programmability and scalability for blockchain applications [3].

With the rapid growth of blockchain applications, the development and deployment of smart contracts face some challenges and problems [4]. First, writing and debugging smart contracts requires familiarity with blockchain development frameworks and programming languages, and there is a certain threshold for non-technical professionals. There is a problem of low development efficiency in the development of smart contracts. Secondly, smart contracts are prone to vulnerabilities and security problems during development, such as reentrant attacks, overflow errors, etc. [5], which may lead to financial losses and user privacy disclosure [6].

In order to solve the problems faced by the above smart contracts in development and deployment, the method based on natural language processing provides us with some promising solutions. NLP can be used to write and verify smart contracts. By using natural language processing technology, contract requirements and specifications can be transformed into executable smart contract code, thereby reducing the threshold and difficulty of writing contracts. In addition, NLP can also be used to verify the correctness and security of contracts, and detect potential vulnerabilities and security risks by analyzing contract code and semantics.

This paper aims to explore the integration of blockchain and natural language processing, as well as its application and potential advantages in smart contract development. We will discuss the basic concepts and characteristics of blockchain technology, as well as the problems and challenges in the development of smart contracts. Subsequently, we will introduce the overview and characteristics of large language models and their potential applications in smart contract development.

## **2 Overview of Blockchain Smart Contracts and Natural Language Processing**

### **2.1 Blockchain and Smart Contracts**

Blockchain technology is a decentralized e-cash system, which was first known in Nakamoto's 'Bitcoin: a peer-to-peer e-cash system' [7]. In the traditional electronic cash system, in order to ensure the security and reliability of transactions, it is necessary to rely on trusted third-party financial institutions for verification. However, there are some problems in this way, such as the risk of double payment. In order to solve these problems, blockchain came into being.

Blockchains form a tamper-evident chain of transaction records by tying them to timestamps and linking them together using a random hashing algorithm. The longest branch of such a chain is considered as proof of the order of transactions, and since most honest nodes will have longer chains than malicious nodes, transactions become tamper-proof in the blockchain.

Smart contracts were first introduced in the 1990s by Nick Szabo, who defined them as a computer program that executes automatically between contract participants. 2014 saw the emergence of the Ethereum blockchain, which has led to the widespread adoption of smart contracts. A smart contract is a program that contains both data (such as account balances) and executable code that executes automatically when certain prerequisites are met [8]. The Ethereum blockchain has Turing's complete programming capabilities

and supports contract programming, enabling blockchain technology to provide more applications in commercial and non-commercial fields, such as online auctions. The life cycle of smart contract includes four main stages: creation, deployment, execution and completion [9]. The following is the step-by-step process of the smart contract life cycle: The developer writes the logic of the contract using the smart contract programming language supported by the blockchain platform. Then, the source code representing their smart contract is compiled using a specific compiler and bytecode is obtained [4]. After the smart contract source code is compiled into bytecode, it will be deployed to the blockchain platform and stored on the blockchain. Depending on the blockchain platform, smart contracts are read-only or modifiable after they are released. For example, Ethereum does not allow modifying smart contracts [5], while EOSIO allows overwriting by uploading new bytecode [6]. If it is read-only, to provide updates, developers will need to release a new version of the smart contract and redirect users to it. The contract terms are monitored and evaluated after the smart contract is deployed. When a smart contract condition is triggered, the corresponding statement will be executed automatically, the transaction will be executed and verified by miners in the blockchain, and the submitted transaction and updated status will be stored on the blockchain. The status of the parties associated with the smart contract will be updated after its execution. The transactions that occur during the execution of a smart contract and the updated status are permanently recorded in the blockchain, and subsequently, the smart contract completes its complete life cycle.

## 2.2 Natural Language Processing

Natural language processing (NLP) is a subject in the field of artificial intelligence that involves processing and understanding human language. The goal of NLP is to enable computers to understand, parse, generate, and process natural language text or speech data. The application of NLP is very extensive, including text classification, sentiment analysis, machine translation, question answering system, information retrieval, named entity recognition, language model and so on [7]. These tasks aim to process and analyze text data so that the computer can extract meaningful information from the text for further reasoning and application.

One of the key challenges of NLP is the complexity and ambiguity of natural language. The language has rich grammatical structure, semantic differences, context dependence and ambiguity, which increases the difficulty of accurate understanding and processing of computers. Therefore, the research focus of NLP includes semantic understanding, grammatical analysis, word sense disambiguation, language generation and so on.

In order to achieve these tasks, NLP uses a variety of techniques and methods. It includes statistical methods, machine learning methods and deep learning methods [8]. Statistical methods mainly use statistical rules and probability models in large-scale corpora to solve language problems. Machine learning methods learn patterns and rules from labeled training data and apply them to the classification, analysis and generation of unknown data. The deep learning method uses a neural network model for end-to-end language processing [9], such as using a Recurrent Neural Network (RNN) and Transformer for semantic understanding and language generation.



### 3 Application of NLP in Smart Contracts

#### 3.1 Automated Generation of Smart Contracts

The programmability of smart contracts makes it flexible and adaptable, which can be applied to different fields and scenarios, and promotes the development of innovation and new business models. However, there may be some challenges and problems in the development of smart contracts. According to the research [10], there are three problems in the development of smart contracts: (1) The preparation and debugging of smart contracts require professional knowledge of blockchain platforms and programming languages, and the technical threshold is high. At the same time, the preparation of smart contracts requires programmers with development experience, and there are communication problems between domain experts and developers. (2) The lack of sufficient development tools makes the development of smart contracts inefficient. (3) Smart contracts are prone to vulnerabilities and security problems in the development process, and the correctness, reliability and security of the contract code must be ensured.

Therefore, before deploying smart contracts, ensuring the correctness of smart contracts and non-functional requirements is crucial in smart contracts. In order to solve the above problems, researchers have proposed different methods for automatically generating smart contracts. In this section, we will discuss the application of NLP in smart contracts from the perspective of automatically generating smart contracts, and compare it with the Domain-Specific-Languages -Based smart contract code generation method.

**Smart Contract Code Generation Based on Domain-Specific Languages.** DSL can generate smart contracts through three perspectives: formal model, contract template and code transformation. DSL framework based on formal model is generally easy to use [29], but can give developers the most intuitive feeling, but the completeness of contract transactions is lower and flexibility is higher. The DSL framework based on contract templates is the most user-friendly for non-experts and has higher completeness of contract transactions, but less flexibility. The code-transformation based DSL framework can reduce the extra learning cost for code developers to focus on what they are good at, however, there is more learning cost for non-professionals [30]. As shown in Table 1, common DSL frameworks are Mavridou [31], iContractML [32], Rahman [33], CML [34], SLCML [35], etc.

**Smart Contract Code Generation Based on Natural Language Processing.** The result of smart contract generation based on DSL is usually a smart contract skeleton that still relies on the manual implementation of the core logic. Therefore, scholars have proposed some smart contract code generation methods based on NLP.

Olivia Choudhury et al. proposed a framework that aims to automatically generate domain-specific smart contracts [10]. The business rules are first extracted from regulatory documents using machine learning and NLP techniques, and then domain knowledge is applied to transform the extracted rules into smart contract functions, where the formal representation is ontology and semantic rules. A case study was conducted with a clinical trial to demonstrate the feasibility and effectiveness of a framework for automatic smart contract generation based on regulatory documents.

Gao [11] et al. proposed a method for automatic generation of ethereum-oriented smart contracts, which generates codes of basic functions of transaction class smart

contracts by clustering analysis, and uses BLEU and SmartCheck for code detection, and achieves good detection results.

Yu et al. proposed an Artificial Intelligence-Assisted Smart Contract Generation (AIASCG) framework to provide generalization of smart contracts through Machine Natural Language (MNL) [12]. It is indicated that an AI-based automatic word splitting technique is proposed to achieve automatic splitting of sentences. The word splitting technique, as a core component of AIASCG, accurately recommends the intermediate MNL output of natural language sentences, significantly reducing the manual work in the contract generation process. In the manual evaluation, participants believed that 88.67% of sentences could be saved 80–100% of the time by automatic word splitting.

Hao et al. proposed a new approach to generate smart contract code templates using LSTM-RNN to improve usability [13], using an Abstract Syntax Tree (AST) and word2vec to extract lexical unit sequence features to obtain word vectors to analyze the semantics of the code. The generated sequence vector features were then fed into LSTM-RNN for template generation, and the efficiency of the four vectorization methods models was tested.

The significance of large language models has been increasingly recognized, and ChatGPT based on GPT-3.5 and GPT-4 has been widely used in various natural language processing domains, including dialogue systems, question and answer systems, machine translation, and natural language generation. In these domains, automatic generation of smart contracts using ChatGPT is an effective approach. According to the experiment of Liu et al. [14] authors compare ChatGPT-generated SQL statements with several current language models for improving large-scale text-to-SQL languages, such as T5-3B, RASAT, and RESDSQL-3B. Combining ChatGPT with several public benchmark datasets for experimental tests, it is concluded that ChatGPT performs similarly to comparable methods/models {(T5-3B + PICARD), (RASAT + PICARD), (RESDSQL-3B + NatSQL)} in terms of fulfilling large-scale text-to-SQL conversion tasks across multiple diverse datasets (SPIDER, SPIDER SYN, SPIDER-REALISTIC, SPIDER-DK, ADVETA (RPL), ADVETA (ADD), SPIDER-CG (SUB), SPIDER CG (APP)), and the fraction that satisfies the generation of SQL statements that satisfy the conditions is about 65%. This study provides useful exploration and empirical evidence for using ChatGPT to generate smart contracts.

As shown in Table 2, this paper analyzes and summarizes the related research on NLP-based code generation from two perspectives, methodology and application areas.

**Smart Contract Code Annotation Generation.** Accurate and high-quality code annotations play an important role in the readability and understandability of smart contract code and are crucial in the development and maintenance of smart contracts. However, in actual smart contract development, code comments are often missing or inconsistent with the actual code semantics due to project budget constraints, lack of programming experience, or failure to update comments in a timely manner when the code is modified. In addition, researchers have found that about 10% of security vulnerabilities in smart contracts are due to code cloning [31], where misuse of under-annotated code is one of the main causes. Therefore, there is an urgent need to design an effective automatic code annotation generation method for developers for smart contracts.

**Table 1.** Common DSL frameworks.

Generation method	Type	Platform	Smart contract language	Functional integrity
Mavridou [31]	Formal model	Ethereum	Solidity	Low
iContractML [32]	Formal model	Multi	Multi	Low
Rahman [33]	Contract template	Ethereum	Solidity	Medium
CML [34]	Code conversion	Ethereum	Solidity	High
SLCML [35]	Code conversion	Ethereum	Solidity	High

**Table 2.** NLP-based code generation summary.

Literature	Methodology/techniques	Application areas
Choudhury et al. [10]	NLP, AST	Domain-specific smart contracts
Gao et al. [11]	Char-RNN	Ether-directed smart contract generation
Yu et al. [12]	AIASCG	Smart contract generation
Hao et al. [13]	LSTM-RNN	Smart contract code template generation
Liu et al. [14]	ChatGPT	SQL statement generation

Yang et al. proposed a multimodal Transformer (MMTrans) based method for smart contract code summarization [16]. The method represents the source code by learning two heterogeneous modalities (structural traversal sequences and graphs) of the abstract syntax tree. In particular, the structure traversal sequence provides the overall semantic information of the abstract syntax tree, while the graph convolution focuses on local details. MMTrans uses two encoders to extract global and local semantic information from these two modalities, respectively, and a joint decoder to generate code annotations. Both encoders and decoders employ Transformer’s multi-headed attention structure to enhance the ability to capture long-range dependencies between code tokens. The researchers constructed a dataset containing over 300K smart contract < method, annotation > pairs and evaluated the performance of MMTrans on this dataset. The experimental results show that MMTrans achieves significant advantages over state-of-the-art baseline methods in all four evaluation metrics and is able to generate higher quality annotations.

Shi et al. proposed a fine-grained annotation generation based on machine translation for so-lidity smart contracts [15]. The AST parsing path and core attributes used for translation were identified, and corresponding translation templates were proposed for special utterances. Then a grammar synthesizer based on probabilistic context-independent grammar was trained using reinforcement learning for generating easy-to-understand English sentences as annotations.

These innovative methods contribute to the advancement of automatic code annotation generation in smart contract development. Their research provides valuable insights into improving the quality and consistency of code annotations, thereby enhancing the understandability and maintainability of smart contracts.

### 3.2 Natural Language Processing and Smart Contract Security

Smart contract security refers to the potential risks and vulnerabilities that may exist during the design, development, deployment, and execution of smart contracts [17]. Since smart contracts are publicly executed and immutable on the blockchain [18], the presence of security vulnerabilities may lead to serious consequences, including loss of funds, data leakage, and inconsistency in contract execution, etc. In 2016, the DAO project on the Ethereum blockchain was hacked, and the attackers exploited a re-entry vulnerability in the project to steal 3.6 million Ethereum worth \$50 million [14]. In June 2017, attackers exploited a vulnerability in the library contract used by the Parity signature wallet and stole \$30 million worth of Ether [19]. In November of the same year, a vulnerability in a new version of the Parity wallet caused \$150 million worth of Ether to be permanently frozen [20]. And in August 2021, hackers stole \$60 million worth of cryptocurrency through a vulnerability [21]. Therefore, the security of smart contracts cannot be ignored. NLP technology can identify possible vulnerability patterns and common problems in smart contracts. It is also widely used in the field of smart contract vulnerability detection.

Yang et al. proposed a smart contract vulnerability auditing method with multiple semantics [22] which uses three different tokenization criteria to generate sequences of smart contracts and capture the semantic contexts using n-gram language model respectively, and finally integrates the audit results from multiple semantic contexts using an effective intersection or concatenation combination strategy. The problem that previous data-driven approaches usually label smart contracts as a series of sequences according to the purpose of vulnerability detection and process them according to only one tokenization criterion is solved, resulting in some semantic contexts not being reflected within the restricted sequence length.

Wu et al. proposed a Peculiar [23] for smart contract vulnerability detection based on key data flow graphs and pre-training techniques, which uses key data flow graphs based on pre-training techniques to detect smart contract vulnerabilities. Compared with the traditional data flow graphs already used in existing methods, the key data flow graph is simpler and does not have an overly deep hierarchy, making it easier for the model to focus on key features. In addition, a pre-training technique is introduced into the model as it achieves significant improvements in various natural language processing tasks. Empirical results show that Peculiar achieves 91.80% precision and 92.40% recall for one of the most serious and common smart contract vulnerabilities detected on 40,932 smart contract files, the re-entry vulnerability, outperforming existing approaches (e.g., Smartcheck achieves 79.37% precision and 70.50% recall).

Qian et al. proposed a BiLSTM attention model for detecting smart contract defects [24]. The model treats the operation code of a smart contract as a sequential sentence and uses an attention-based bi-directional long and short-term memory (BiLSTM-Attention) model to discover defects in smart contracts. The performance of the model and other

models are evaluated for 45,622 real-world smart contracts. The experimental results show that our model can achieve higher accuracy (95.40%) and F1 score (95.38%).

Huang et al. proposed a multi-task learning-based vulnerability detection model for smart contracts [25]. By setting auxiliary tasks to learn more directional vulnerability features, the detection capability of the model is improved, and vulnerability detection and identification is achieved. The model is based on a hard-shared design and consists of two parts. The underlying shared layer is mainly used to learn the semantic information of the input contract. The text representation is first converted into new vectors by word and location embedding, and then a neural network based on the attention mechanism is used to learn and extract the feature vectors of the contract. Task-specific layers are mainly used to implement the functionality of each task. A classical convolutional neural network is used to construct a classification model for each task, and features are learned and extracted from the shared layers to achieve the respective task goals.

Zhu et al. proposed a triple network-based optimization option and compiler version smart contract bytecode similarity detection [26]. Analysis for contract bytecode addresses the situation that contracts cannot be analyzed for security due to the fact that most smart contracts only release bytecode without disclosing the source code. Hengyan Zhang et al. proposed detecting smart contract vulnerabilities by deep semantic extraction [27], and Wanqing Jie et al. proposed a novel extended multimodal AI for smart contract vulnerability detection framework [28].

Compared with traditional smart contract vulnerability detection methods, the introduction of NLP techniques can provide a more comprehensive analysis of smart contract vulnerabilities through semantic understanding and feature extraction of smart contract code. Although these methods have achieved significant results in smart contract vulnerability detection, there are still some shortcomings. One of these shortcomings is the ability to detect new types of vulnerabilities, which are constantly emerging due to the complexity of smart contracts and evolving threat patterns. As a result, researchers need to continuously update their models and algorithms to address new vulnerability types. In addition, the process of vulnerability detection is a black-box model, and the working state and processing of its internal detection vulnerabilities are not transparent, resulting in a lack of reasonable interpretation of the detection results. In response to the shortcomings of the current NLP-based smart contract vulnerability detection, this paper summarizes the following future research directions: (1) Continue to improve the accuracy and robustness of the model to reduce the false alarm rate and leakage rate of vulnerabilities (2) Combine the vulnerability-related rules and semantic information from traditional smart contract vulnerability detection methods with NLP models to improve the interpretability of vulnerability detection results.

## 4 Summary and Outlook

This paper discusses the integration of blockchain technology and NLP in smart contract development. Smart contracts, as automatically executed computer programs, provide programmability and scalability for blockchain applications. To address the problems of inefficient development, personnel communication barriers, reliability of code, and difficulty in guaranteeing security during the writing, debugging, and maintenance of

smart contracts, NLP technology provides promising solutions for this purpose by using natural language to automate the generation and verification of smart contracts. The article explores some of the applications of NLP in automated smart contract generation, comparing it with DSL. Various approaches, such as cluster analysis, Char-RNN and LSTM-RNN, are discussed for automatic smart contract code generation. The article explores the significance of large language models like ChatGPT in code generation and presents empirical evidence of domain-specific code generation using ChatGPT as a way to support the feasibility of generating highly usable smart contracts using ChatGPT. In addition, the article highlights the importance of accurate code annotation in smart contract development and summarizes research related to the use of NLP techniques to improve the readability and comprehensibility of code.

In terms of security issues in smart contracts, the use of NLP techniques can identify possible security vulnerabilities in smart contracts and achieve a more desirable identification accuracy rate. In practical applications, it can be used as a supplement to traditional security verification techniques such as SmartCheck [36], Zeus [37], and ContractFuzzer [38] to discover potential security vulnerabilities and errors in time to improve the security of smart contracts.

Despite the great potential of NLP in the application of smart contracts, it still faces some challenges and limitations. One of them is the ambiguity and inaccuracy of natural language, which may lead to misunderstandings or errors in the generated smart contracts. Therefore, in future research efforts to integrate NLP with the smart contract domain, there are the following research directions: (1) Enhancing the accuracy of smart contract code generation. Improving the natural language understanding capability of NLP models enables contract requirements and specifications to be more accurately and efficiently translated into executable smart contract code. Large language models like ChatGPT can be further refined and trained specifically for generating smart contract code. By leveraging large-scale text-to-code conversion datasets and incorporating domain-specific knowledge, these models can generate high-quality, reliable and secure smart contract templates. (2) Optimization of smart contract code, such as Ethereum's contracts, where smart contract code generated via NLP may be redundant and can be optimized to reduce Gas consumption as well as improve performance. (3) Improving the portability of automatically generated smart contract code, using NLP techniques to form common contract logic expressions to generate smart contracts written in different languages. (4) The combination of NLP-generated smart contract code and regulatory compliance techniques. NLP can help ensure compliance with regulatory requirements and standards in smart contract development. By analyzing regulatory documents and extracting relevant rules and conditions, NLP models can assist in automatically generating smart contracts that comply with legal and regulatory frameworks. This integration can ensure the legality and validity of smart contracts.

The integration of blockchain technology and NLP has the potential to revolutionize smart contract development and deployment. By addressing challenges such as development efficiency, security vulnerabilities, the further development in this field can open up new possibilities for blockchain applications in areas such as digital identity, supply chain management, and the Internet of Things (IoT).

**Acknowledgments.** This work was supported in part by the National Key R&D Program of China (No. 2021YFB2700600); in part by the Finance Science and Technology Project of Hainan Province (No. ZDKJ2020009); in part by the National Natural Science Foundation of China (No. 62163011); in part by the Research Startup Fund of Hainan University under Grant KYQD(ZR)-21071.

## References

1. Feng, Z., Boxuan, S., Wenbao, J.: A review of blockchain key technologies and application research. *J. Netw. Inf. Secur.* **4**(4), 22–29 (2018)
2. Yuan, Y., Wang, F.Y.: Blockchain: the state of the art and future trends. *Acta Autom. Sin.* **42**(4), 481–494 (2016)
3. Ouyang, L.W., Wang, S.H., Yuan, Y., et al.: Smart contracts: architecture and progress. *J. Autom.* **45**(3), 445–457 (2019)
4. Zou, W., Lo, D., Kochhar, P.S., et al.: Smart contract development: challenges and opportunities. *IEEE Trans. Software Eng.* **47**(10), 2084–2106 (2019)
5. Sayeed, S., Marco-Gisbert, H., Cairra, T.: Smart contract: attacks and protections. *IEEE Access* **8**, 24416–24427 (2020)
6. Wang, Z., Jin, H., Dai, W., et al.: Ethereum smart contract security research: survey and future research opportunities. *Front. Comput. Sci.* **15**, 1–18 (2021)
7. Fu Liyu, L., Yiming, G.W., et al.: A review of blockchain technology research and its development. *Comput. Sci.* **49**(6A), 447–461 (2022)
8. Zou, W., Lo, D., Kochhar, P.S., et al.: Smart contract development: challenges and opportunities. *IEEE Trans. Software Eng.* **47**(10), 2084–2106 (2019)
9. Zheng, Z., Xie, S., Dai, H.N., et al.: An overview on smart contracts: challenges, advances and platforms. *Futur. Gener. Comput. Syst.* **105**, 475–491 (2020)
10. Choudhury, O., Dhuliawala, M., Fay, N., et al.: Auto-translation of regulatory documents into smart contracts. *IEEE Blockchain Initiative*, (September), 1–5 (2018)
11. Yichen, G., Bin, Z., Zao, Z.: Research and implementation of automatic generation method of smart contracts for Ethernet. *J. East China Normal Univ. (Nat. Sci.)* (2020)
12. Tong, Y., Tan, W., Guo, J., et al.: Smart contract generation assisted by AI-based word segmentation. *Appl. Sci.* **12**(9), 4773 (2022)
13. Hao, Z., Zhang, B., Mao, D., et al.: A novel method using LSTM-RNN to generate smart contracts code templates for improved usability. In: *Multimedia Tools and Applications*, pp. 1–31 (2023)
14. Liu, A., Hu, X., Wen, L., et al.: A comprehensive evaluation of ChatGPT’s zero-shot Text-to-SQL capability. *arXiv preprint arXiv:2303.13547* (2023)
15. Shi, C., Xiang, Y., Yu, J., et al.: Machine translation-based fine-grained comments generation for solidity smart contracts. *Inf. Softw. Technol.* **153**, 107065 (2023)
16. Yang, Z., Keung, J., Yu, X., et al.: A multi-modal transformer-based code summarization approach for smart contracts. In: *2021 IEEE/ACM 29th International Conference on Program Comprehension (ICPC)*, pp. 1–12. IEEE (2021)
17. Atzei, N., Bartoletti, M., Cimoli, T.: A survey of attacks on ethereum smart contracts (sok). In: *Principles of Security and Trust: 6th International Conference, POST 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22–29, 2017, Proceedings*, vol. 6, pp. 164–186. Springer, Berlin (2017)
18. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper* **2014**(151), 1–32 (2014)

19. BlockCAT. On the Parity multi-sig wallet attack (2017). <https://medium.com/blockcat/on-the-parity-multi-sig-wallet-attack-83fb5e7f4b8c>
20. Pretrov, S.: Another Parity wallet hack explained (2017). <https://medium.com/@Pr0Ger/another-parity-wallet-hack-explained-847ca46a2e1c>
21. Wikipedia. Poly network exploit (2023). [https://en.wikipedia.org/wiki/Poly\\_Network\\_exploit](https://en.wikipedia.org/wiki/Poly_Network_exploit)
22. Yang, Z., Keung, J., Zhang, M., et al.: Smart contracts vulnerability auditing with multi-semantics. In: 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 892–901. IEEE (2020)
23. Wu, H., Zhang, Z., Wang, S., et al.: Peculiar: smart contract vulnerability detection based on crucial data flow graph and pre-training techniques. In: 2021 IEEE 32nd International Symposium on Software Reliability Engineering (ISSRE), pp. 378–389. IEEE (2021)
24. Qian, C., Hu, T., Li, B.: A BiLSTM-attention model for detecting smart contract defects more accurately. In: 2022 IEEE 22nd International Conference on Software Quality, Reliability and Security (QRS), pp. 53–62. IEEE (2022)
25. Huang, J., Zhou, K., Xiong, A., Li, D.: Smart contract vulnerability detection model based on multi-task learning. *Sensors* **2022**, 22 (1829). <https://doi.org/10.3390/s22051829>
26. Zhu, D., Yue, F., Pang, J., Zhou, X., Han, W., Liu, F.: Bytecode similarity detection of smart contract across optimization options and compiler versions based on triplet network. *Electronics* **11**, 597 (2022). <https://doi.org/10.3390/electronics11040597>
27. Zhang, H., Zhang, W., Feng, Y., et al.: SVScanner: detecting smart contract vulnerabilities via deep semantic extraction. *J. Inf. Secur. Appl.* **75**, 103484 (2023)
28. Jie, W., Chen, Q., Wang, J., et al.: A novel extended multimodal AI framework towards vulnerability detection in smart contracts. *Inf. Sci.* **636**, 118907 (2023)
29. Kurtev, I., Bézivin, J., Jouault, F., et al.: Model-based DSL frameworks. In: Companion to the 21st ACM SIGPLAN Symposium on Object-Oriented Programming Systems, Languages, and Applications, pp. 602–616 (2006)
30. *Fundamentals of DSL Technology*. CRC Press (2005)
31. Mavridou, A., Laszka, A.: Designing secure ethereum smart contracts: A finite state machine based approach. In: International Conference on Financial Cryptography and Data Security, pp. 523–540. Springer (2018)
32. Hamdaqa, M., Metz, L.A.P., Qasse, I.: IContractML: a domain-specific language for modeling and deploying smart contracts onto multiple blockchain platforms. In: Proceedings of the 12th System Analysis and Modelling Conference, pp. 34–43 (2020)
33. Rahman, R., Liu, K., Kagal, L.: From legal agreements to blockchain smart contracts. In: 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1–5. IEEE (2020)
34. Wöhrer, M., Zdun, U.: Domain specific language for smart contract development. In: 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1–9. IEEE (2020)
35. Dwivedi, V., Norta, A., Wulf, A., et al.: A formal specification smart-contract language for legally binding decentralized autonomous organizations. *IEEE Access* **9**, 76069–76082 (2021)
36. Tikhomirov, S., Voskresenskaya, E., Ivanitskiy, I., et al.: Smartcheck: static analysis of ethereum smart contracts. In: Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, pp. 9–16 (2018)
37. Kalra, S., Goel, S., Dhawan, M., et al.: Zeus: analyzing safety of smart contracts. In: Ndss, pp. 1–12 (2018)
38. Jiang, B., Liu, Y., Chan, W.K.: Contractfuzzer: Fuzzing smart contracts for vulnerability detection. In: 2018 33rd IEEE/ACM International Conference on Automated Software Engineering (ASE), pp. 259–269. IEEE (2018)



# Author Index

## B

Bao, Fengbo 32  
Bao, Yuben 249

## C

Cai, Daomeng 343  
Cai, Yuqian 39  
Cao, Siyi 423  
Cao, Yalin 190  
Cao, Yang 173, 182  
Chao, Cong 393  
Chen, Dunhua 22  
Chen, Gong 68  
Chen, Jiwei 249, 281  
Chen, Longjie 383  
Chen, Min 120  
Chen, Pu 140  
Chen, Shuo 456  
Chen, Tianxin 402  
Chen, Xingyu 293  
Chen, Yalin 374

## D

Dai, Cheng 402  
Dai, Meiling 200, 210  
Dong, Wenkuo 238  
Dong, Yunzhou 335  
Dreibholz, Thomas 436, 447  
Du, Jia 82  
Duan, Ruolan 1

## F

Fan, Chengwen 316  
Fan, Huicong 326  
Feng, Lei 153, 190, 230, 238  
Feng, Yuqing 374  
Fu, Fa 436, 447

## G

Gan, Xinli 1  
Gao, Feng 153

Gao, Haoyu 456, 467  
Gao, Jing 238  
Gao, Qiang 269  
Gao, Yuan 130, 140  
Guo, Chengwei 230  
Guo, Jinsong 32  
Guo, Shaoyong 258

## H

Han, Xun 413  
Hao, Jiakai 281  
He, Meiling 413  
Hou, Huanpeng 220, 366  
Hu, Feifei 173, 182  
Hu, Xinyue 68  
Hu, Yu 383  
Huang, Chenrong 100  
Huang, Donghai 249  
Huang, Dongyan 356  
Huang, Jianqiang 436, 447  
Huang, Jie 316  
Huang, Wei 316  
Huang, Yan 90  
Huo, Zhilin 343

## J

Ji, Yutong 374  
Jia, Huixue 343  
Jin, Ming 281

## K

Kang, Zhongmiao 249  
Kou, Wanli 82

## L

Lei, Hong 456, 467  
Li, Bo 393  
Li, Caiyun 326  
Li, Da 258  
Li, Gongming 220  
Li, Hongwei 163

Li, Jingwen 210  
 Li, Kelin 383  
 Li, Meng 423  
 Li, Mengyuan 258  
 Li, Mian 53  
 Li, Pengyu 230  
 Li, Wengjing 258  
 Li, Wenjing 238  
 Li, Wenxiao 326  
 Li, Xiangning 39  
 Li, Xiaoyu 343  
 Li, Yang 68  
 Li, Yongjie 220, 366  
 Li, Yue 68  
 Li, Yuting 281  
 Liang, Guangjun 423  
 Liang, Wandu 326  
 Lin, Peng 269, 335  
 Lin, Xubin 173, 182  
 Lin, Zhengdong 335  
 Liu, Boyu 153  
 Liu, Chao 456, 467  
 Liu, Chuan 467  
 Liu, Donglan 11  
 Liu, Hui 190  
 Liu, Tian 393  
 Liu, Wei 413  
 Liu, Xin 11  
 Liu, Yue 190  
 Liu, Zhaojun 436  
 Liu, Zhiwei 456  
 Lu, Gaoshang 447  
 Lu, Jizhao 190, 220, 366  
 Lu, Yanjing 53  
 Lu, Yi 210  
 Luo, Huihong 173, 182  
 Lv, Wei 269  
 Lyu, Andrew 100

**M**

Ma, Lei 11  
 Miao, Peidong 130

**N**

Nie, Jianyu 436

**P**

Pan, Detai 335  
 Peng, Jiansheng 22, 32

**Q**

Qi, Feng 258, 293  
 Qin, Tai 120  
 Qing, Yong 61  
 Qiu, Xuesong 293  
 Qiu, Yujie 153

**R**

Ren, Yinlin 293

**S**

Shen, Pengxu 467  
 Shen, Yan 120  
 Shi, Xiaohou 200  
 Shi, Yingji 230  
 Song, Yun 1  
 Song, Zikai 467  
 Sun, Bin 393  
 Sun, Lili 11  
 Sun, Mingyang 163  
 Sun, Pengzhan 293

**T**

Tang, Fan 326  
 Tian, Jingyue 39  
 Tian, Yu 374

**W**

Wang, Cong 343  
 Wang, Dong 258  
 Wang, Manxuan 423  
 Wang, Rui 11  
 Wang, Ruilin 304  
 Wang, Wenge 220, 366  
 Wang, Xudong 153  
 Wang, Yanru 153, 190  
 Wang, Yutong 200  
 Wang, Yuying 402  
 Wang, Zhanyang 90  
 Wang, Zhili 304  
 Wang, Zhiqiang 130, 140  
 Wen, Jin 130, 140  
 Weng, Junhong 269  
 Wu, Qian 269  
 Wu, Ruotong 39

**X**

Xiao, Yitao 281  
 Xing, Yanxia 230

Xiong, Ao 258  
Xu, Dawei 402  
Xu, Dongjiao 366  
Xu, Xiang 456

**Y**

Yang, Guilong 402  
Yang, Kelin 393  
Yang, Qing 22  
Yang, Shan 343  
Yang, Shaojie 200, 210  
Yang, Shuang 393  
Yang, Yang 316  
Yang, Yu 393  
Yang, Yunfan 402  
Yu, Haidong 61  
Yu, Hongguang 326

**Z**

Zhang, Chengmeng 68  
Zhang, Chengyao 356  
Zhang, Fangzhe 11

Zhang, Guoyi 173, 182  
Zhang, Hanrui 100  
Zhang, Hao 11  
Zhang, Jingqi 436  
Zhang, Peiming 249  
Zhang, Shibin 343  
Zhang, Shujun 343  
Zhang, Xin 436  
Zhang, Yuhang 53  
Zhang, Zheng 200  
Zhao, Fuhui 11  
Zhao, Guanghuai 281  
Zhao, Jianhua 326  
Zheng, Fei 383  
Zheng, Zelin 269  
Zheng, Zhen 335  
Zhou, Fanqin 230  
Zhou, Huaizhe 82  
Zhou, Zou 383  
Zhu, Cong 374  
Zhu, Hailong 173, 182  
Zhu, Shijia 326