Smart Innovation, Systems and Technologies 350

Xuesong Qiu · Yang Xiao · Zhiqiang Wu ·
Yudong Zhang · Yuan Tian ·
Bo Liu *Editors*

The 7th International Conference on Information Science, Communication and Computing

KES International

Springer

Smart Innovation, Systems and Technologies 350

Series Editors

Robert J. Howlett, *KES International, Shoreham-by-Sea, UK*
Lakhmi C. Jain, *KES International, Shoreham-by-Sea, UK*

The Smart Innovation, Systems and Technologies book series encompasses the topics of knowledge, intelligence, innovation and sustainability. The aim of the series is to make available a platform for the publication of books on all aspects of single and multi-disciplinary research on these themes in order to make the latest results available in a readily-accessible form. Volumes on interdisciplinary research combining two or more of these areas is particularly sought.

The series covers systems and paradigms that employ knowledge and intelligence in a broad sense. Its scope is systems having embedded knowledge and intelligence, which may be applied to the solution of world problems in industry, the environment and the community. It also focusses on the knowledge-transfer methodologies and innovation strategies employed to make this happen effectively. The combination of intelligent systems tools and a broad range of applications introduces a need for a synergy of disciplines from science, technology, business and the humanities. The series will include conference proceedings, edited collections, monographs, handbooks, reference books, and other relevant types of book in areas of science and technology where smart systems and technologies can offer innovative solutions.

High quality content is an essential feature for all book proposals accepted for the series. It is expected that editors of all accepted volumes will ensure that contributions are subjected to an appropriate level of reviewing process and adhere to KES quality principles.

Indexed by SCOPUS, EI Compendex, INSPEC, WTI Frankfurt eG, zbMATH, Japanese Science and Technology Agency (JST), SCImago, DBLP.

All books published in the series are submitted for consideration in Web of Science.

Xuesong Qiu · Yang Xiao · Zhiqiang Wu ·
Yudong Zhang · Yuan Tian · Bo Liu
Editors

The 7th International Conference on Information Science, Communication and Computing

Springer

Editors
Xuesong Qiu
School of Computer Science (National Pilot
Software Engineering School)
Beijing University of Posts and Telecomm
Beijing, Beijing, China

Zhiqiang Wu
Department of Electrical Engineering
Wright State University
Dayton, OH, USA

Yuan Tian
School of Computer Engineering
Nanjing Institute of Technology
Nanjing, Jiangsu, China

Yang Xiao
Department of Computer Science
The University of Alabama
Tuscaloosa, AL, USA

Yudong Zhang
Department of Informatics
University of Leicester
Leicester, UK

Bo Liu
School of Physics and Optoelectronic
Engineering
Nanjing University of Information Science
and Technology
Nanjing, Jiangsu, China

ISSN 2190-3018 ISSN 2190-3026 (electronic)
Smart Innovation, Systems and Technologies
ISBN 978-981-99-7160-2 ISBN 978-981-99-7161-9 (eBook)
https://doi.org/10.1007/978-981-99-7161-9

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.

Contents

Visualization Analysis of Research Hot Spots of Drug Patents in China

Fang Xia, Yiguo Cai, Siyu Sun, Ziying Xu, and Yufang He(✉)

School of Health Management, Changchun University of Chinese Medicine,
Changchun 130117, China
Xiafang425@126.com, hyf_1992@163.com

Abstract. The purpose of the article is to provide references for the future development of drug patent field in China by analyzing the hotpots and trends thereof. The related articles of CNKI were retrieved with "drug patent" as the subject word and keyword, and visualized by CiteSpace software. The number of articles published in the field of drug patents is generally on the rise, and drug patent protection has become a research hotpots. The institutions and authors with high output concentrate on the innovation of drug patent system and the protection of intellectual property rights, which form three relatively close cooperation institutions; The main hot keywords are DRUG PATENTS, PATENT PROTECTION, BALANCE OF INTERESTS; Research on "drugs", "drug patents" and "safeguarding the legitimate rights and interests of patentee" has been formed. To protect the legitimate rights and interests of the patentee and promote the further reduction of drug prices.

Keywords: Drug patents · Patent system · CiteSpace

1 Introduction

Drug patents refer to patents applied for drugs, including drug product patents, drug preparation technology patents, drug use patents and other different types [1]. With the unprecedented development of science and technology and the development of reverse engineering, the research and development results of pharmaceutical enterprises are easy to be imitated at low cost, and the value of the disclosure of patented technology schemes decreases, so the demand for the protection of technical schemes by right holders is more urgent [2]. In recent years, drug patent protection has attracted much attention as an important means to promote the development and innovation of the pharmaceutical industry. On July 4, 2021, the National Medical Products Administration and the State Intellectual Property Office promulgated the *Implementation Measures for the Mechanism for the Early Settlement of Drug Patent Disputes (Trial)* (hereinafter referred to as the Implementation Measures). On July 5, 2021, the State Intellectual Property Office issued the *Administrative Decision on the Early Settlement Mechanism for Drug Patent Disputes* (hereinafter referred to as Administrative Decision), Meanwhile, the Supreme People's Court issued the *Provisions on Several Issues concerning the Application of*

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 1–12, 2024.
https://doi.org/10.1007/978-981-99-7161-9_1

Law to the Trial of Civil Cases of Disputes over Patent Rights Related to Drugs Applied for Registration, which came into force today, marking the official implementation of the 1.0 version of China's drug patent link system [3]. Improvement of China's patent information registration system for Listed drugs. Academics see the field as one way to resolve various patent disputes and speed up the launch of generic drugs to the benefit of other companies and patients. In this study, CiteSpace software is used to analyze the relevant literature in this field, to discuss the trends and hot spots of this field, to provide reliable scientific basis for relevant researchers to explore the future development trend, and to provide reference for further research in this field.

2 Information and Algorithm

2.1 Literature Search

The literature related to the field of drug patents was searched in the CNKI database and the search time span from 2010 to 2021. After manual screening and software elimination of duplicates, 1031 articles are finally include, including 164 core journals, accounting for 15.9%.

2.2 Clustering Method

In this paper, CiteSpaceV software developed by Dr. Chen Chaomei is used to draw the knowledge map and keyword co-occurrence map based on the cooperation of authors, institutions, etc., and extract the author and keyword information of higher cited literature for analysis [4].

The algorithm formula is $LLR(b_i) = ln\frac{\mathrm{P}[b_i=0|\mathrm{y}]}{\mathrm{P}[b_i=1|\mathrm{y}]} = \frac{1}{\sigma^2}[min_{x:bi=1}\{|\mathrm{y} - \beta\mathrm{x}|^2\} - min_{x;bi=0}\{||\mathrm{y} - \beta\mathrm{x}||^2\}]$, and y is the input symbol to the de-mapper calculation; x is the QAM constellation points; β(BETA) is the constellation energy; $\frac{1}{\sigma^2} = 1/NV$ (Noise Variance Inverse-NVI).

Consider two random variables X and Y whose joint probability density function is p(x, y) and whose marginal probability density functions are p(x) and p(y), respectively. The mutual information I(X, Y) is the relative entropy between the joint distributions p(x, y) and p(x)p(y).

$$KLD = D(p|q) = \sum_x p(x)\log\frac{p(x)}{q(x)} = E_p \log\frac{p(x)}{q(x)}$$

p and q are two probability distributions.

$$MI = I(X;Y) = \sum_X\sum_Y p(x,y)log\frac{(x,y)}{p(x)p(y)} = D(p(x,y)\|p(x)p(y))$$

$$I = (X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) + H(X) + H(Y) - H(X,Y)$$

The LSI is based on the singular value decomposition (SDV) method to obtain the article topic. Te SDV decomposition can be approximated by writing: $A_{m*n} \approx U_{m*k}\Sigma_{k*k}V^T_{k*n}$.

Applying the above equation to the topic model, SDV can be interpreted as follows: input m texts with n words in each text. $\mathbf{A_{ij}}$ corresponds to the feature value of the **j**th word in the **i**th text, commonly based on the preprocessed is normalized TF-IDF value. **K** is the assumed number of topics, generally less than the number of texts. After SDV decomposition, $\mathbf{U_{il}}$ corresponds to the relevance of the **i**th text and the **l**th topic; $\mathbf{\Sigma_{lm}}$ corresponds to the the correlation between the **I**th topic and the **m**th word sense; $\mathbf{V_{jm}}$ corresponds to the correlation between the **l**th word and the **m**th word.

Generally, the clustering effect of the atlas is measured according to the clustering modularity index (Q value) and the clustering contour index (S-value), and the larger the value, the better the clustering effect of the network. When the Q value exceeds 0.3 and the S value is greater than 0.5, clustering is considered reasonable.

In terms of literature volume prediction, the former Soviet scientists Narimov and Freidutz believed that the literature could not grow indefinitely. Based on the research, a logical curve growth law of the literature was proposed, whose mathematical formula is$f(t) = \frac{k}{1+ae^{-bt}}$.

$f(t)$ is t-years of literature accumulation; k is Literature cumulative maximum; a is Parameters; b is continuous growth rate of the literature; t is time.

3 Results

3.1 Distribution of Posting Time

We can quickly understand the overall evolution status of the feld through the publication number of documents. Figure 1 shows the changes in the number of publications on drug patent during 2010–2021 (2022 is the predicted, the data from China Knowledge Network). Generally, the publication trend is gradually increasing. In detail, we can see that from 2010 to 2013,the number of relevant research papers has not increased or even decreased, the average number of papers issued is 72; From 2014 to 2017,the number of relevant research was stable, with an average annual number of 59. The rapid development stage is 2018–2021, with an average annual number of 114 documents. This trend indicates that more scholars have paid extensive attention in drug patent as time elapsed. Therefore, it is reasonable to believe that the research in drug patent will fourish in the future, and more scholars will participate in this domain.

3.2 Author Distribution and Co-Linear Network

Figure 2 shows the network map of authors' cooperation in drug patent research. The results show that there are 344 nodes, 98 connections, and the network density is 0.0017. Observing Fig. 2, it is apparent that many authors tend to collaborate with a relatively stable group of collaborators to generate several major author clusters, and each cluster usually contains two or more core authors. Figure 2 demonstrates that the most representative author in the field is Jingxi Ding, Rong Shao and Jiejing Yao,etc.

Table 2 lists the top 10 most frequently cited literature authors. Learning relevant experience from abroad to promoting the establishment of China's drug patent linkage system [5–7] and the protection of drug patent intellectual property rights [8, 9] are the main research contents.

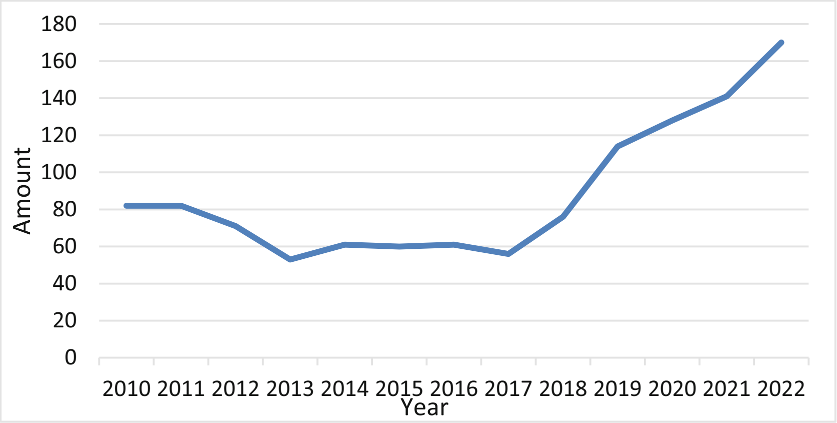


Fig. 1. Publication trends on drug patent (2000–2022)

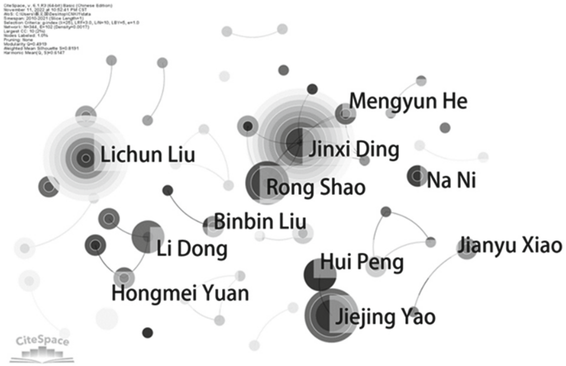

CiteSpace, v. 6.1.R3 (64-bit) Basic (Chinese Edition)
November 11, 2022 at 10:52:41 PM CST
WoS: C:\Users\[illegible]\Desktop\CNKI\1\data
Timespan: 2010-2021 (Slice Length=1)
Selection Criteria: g-index (k=25), LRF=3.0, L/N=10, LBY=5, e=1.0
Network: N=344, E=102 (Density=0.0017)
Largest CC: 10 (2%)
Nodes Labeled: 1.0%
Pruning: None
Modularity Q=0.4919
Weighted Mean Silhouette S=0.8191
Harmonic Mean(Q, S)=0.6147
Mengyun He
Lichun Liu
Jinxi Ding
Rong Shao
Na Ni
Binbin Liu
Li Dong
Jianyu Xiao
Hui Peng
Hongmei Yuan
Jiejing Yao
CiteSpace

Fig. 2. Author collaboration network

According to Price's law [10], the minimum value of core journal authorship is N = 0.749 × $\sqrt{Npmax}$ (Npmax is the highest yielding authorship)The top 10 core authors and their units and number of publications in this study are shown in Table 1. It can be seen from the table that Jinxi Ding, the most prolific author, has published 9 articles.This gives a minimum value of N = 0.749 × $\sqrt{9}$= 2.247 for the number of core author publications in this study.The minimum number of articles issued by core authors is two according to the upper limit is rounded. 136 core authors, 164 papers accounting for 15.9% (50%) of all papers in the field.

3.3 Institution Distribution and Co-Linear Network

Figure 3 shows the academic cooperation among diferent institutions in drug patent research. The fgure is composed of 277 nodes and 98 cooperation links and the network density is 0.0014. It can be seen that the network density of the atlas is low, and the cooperation between the author's organizations is not close. In terms of node size, China

Table 1. Top10 core authors in the field of pharmaceutical patent research in China

Core Authors	Institution	Number	Core Authors	Institution	Number
JinxiDing	China Pharmaceutical University	9	XiaoxiaoHu	Central South University of Forestry Technology	3
LichunLiu	China Pharmaceutical University	7	HongmeYuan	Shenyang Pharmaceutical University	3
RongShao	China Pharmaceutical University	4	HuaHe	China Pharmaceutical University	3
LiDong	Shenyang Pharmaceutical University	3	XuezhongZhu	Tongji University	3
KanTian	Nanjing University of Chinese Medicine	3	YuanjiaHu	University of Macao	3

Pharmaceutical University, Shenyang Pharmaceutical University, East China University of Political Science and low and China University of political and law has the most significant node size, most of them are cooperation between colleges and universities.

3.4 Keyword Co-occurrence Analysis

Figure 4 shows the knowledge network of co-occurred keywords, which consists of 364 nodes and 654 connections. We can fnd that the current popular keywords in this feld include "pharmaceutical patents", "public health", "compulsory licensing", "generic drugs", "patent links", "balance of interests", "patent protection", and "patent law".

In detail, Table 3 lists the most frequently co-occurred keywords in terms of frequency, centrality, and year of occurrence. The top co-occurred keywords are "Pharmaceutical patents" (254 times), "Public Health" (130 times), and "Compulsory licensing" (125 times), "Generic Drugs" (107times). The keywords "Pharmaceutical patents"and"Public Health"are most frequently manily because drug patents protect the interests of drug developers and give them more incentive to develop new drugs to help the public escape health crises.

3.5 Keyword Clustering Analysis

The purpose of cluster analysis is to understand the research hotspots in the field and is based on keyword co-occurrence networks. The results showed that the keywords studied in this field were clustered into 9 categories, which is displayed in Fig. 5, and the sub-categories were #0 generic drugs, #1 drug patents, #2 patents, #3 patent protection, #4 compulsory licenses, #5 intellectual property rights, #6 patentees, #7 patented drugs,

Table 2. Top 10 most cited references of drug patent research

Number	Title	Author	Periodicals	Year	Frequency
1	Transplantation and Creation of Pharmaceutical Patent Linkage System	Zhiwen Liang	Politics and Law	2017	80
2	TRIPS-PLUS protection for pharmaceuticals in U.S. free trade agreements	Zhiwen Liang	Comparative Law Studies	2014	65
3	The Expansion of TRIPS-PLUS Clause and China's Response Strategy	Xueyan Wu	Modern Jurisprudence	2010	62
4	Application of Compulsory Licensing System for Pharmaceutical Patents in Developing Countries	Ming Hao	Intellectual Property	2015	59
5	Protection of Intellectual Property Rights in International Trade in the Context of Economic Globalization	Chao Fan	Journal of Northeast University of Finance and Economics	2011	57
6	Challenges and Responses: The Future of China's Pharmaceutical Patent System	Meili Wang	Intellectual Property	2017	57

(*continued*)

and #8 patent infringement, and some of the tag words for this cluster are shown in Table 4.

Figure 5 shows the keyword co-occurrence clusters in drug patent research.This clustering profile has a significant structure and reasonable clustering with a Modularity value of 0.4919 (>0.300) and a Silhouette value of 0.819 (>0.500) [11]. Generally, we can fnd that the keywords cover various topics, such as the aspect of drug ("#0, #1, and

Table 2. (*continued*)

Number	Title	Author	Periodicals	Year	Frequency
7	The Selection of Elements of Drug Patent Linkage Systems in the United States and Canada and Their Implications for China	Lichun Liu	China Science and Technology Forum	2014	56
8	Research on the development rules and policies of biomedical industry	Jianchong Wang	Journal of Huazhong Normal University	2011	55
9	A Study of the U.S. Drug Patent Linkage System	Jin Chen	Chinese Journal of New Drugs	2012	52
10	Exploration of the establishment of a patent linkage system for pharmaceuticals in China	Yongshun Chen	Technology and Law	2018	51

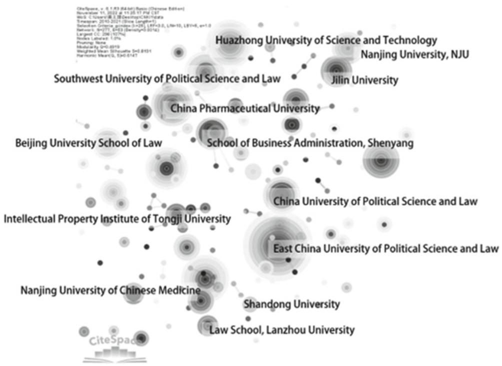

Huazhong University of Science and Technology
Nanjing University, NJU
Southwest University of Political Science and Law
Jilin University
China Pharmaceutical University
Beijing University School of Law
School of Business Administration, Shenyang
China University of Political Science and Law
Intellectual Property Institute of Tongji University
East China University of Political Science and Law
Nanjing University of Chinese Medicine
Shandong University
Law School, Lanzhou University
CiteSpace

Fig. 3. Institution collabration network

#7"), drug patent rights("#2, #3, and #4"), ("#5, #6 and #8")are mainly for the protection of the legitimate rights and interests of the patentee and the protection of intellectual property rights.

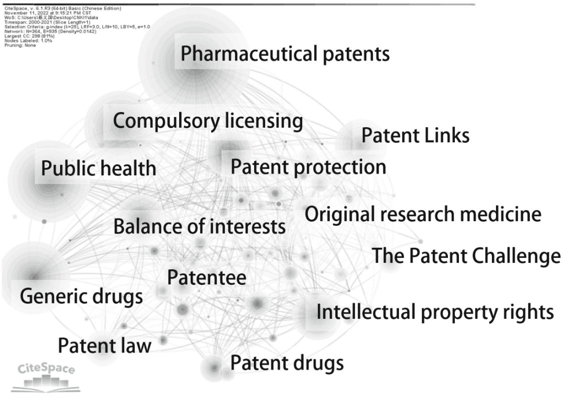

CiteSpace, v. 6.1.R3 (64-bit) Basic (Chinese Edition)
November 11, 2022 at 9:15:21 PM CST
WoS: C:\Users\蔡义国\Desktop\CNKI1\data
Timespan: 2000-2021 (Slice Length=1)
Selection Criteria: g-index (k=25), LRF=3.0, L/N=10, LBY=5, e=1.0
Network: N=364, E=935 (Density=0.0142)
Largest CC: 298 (81%)
Nodes Labeled: 1.0%
Pruning: None
Pharmaceutical patents
Compulsory licensing
Patent Links
Public health
Patent protection
Original research medicine
Balance of interests
The Patent Challenge
Patentee
Generic drugs
Intellectual property rights
Patent law
Patent drugs
CiteSpace

Fig. 4. Keyword co-occurrence network

Table 3. The top 10 keywords in terms of frequency

Nnmber	Keywords	Frequency	Centrality	Year
1	Pharmaceutical patents	254	0.34	2010
2	Public Health	130	0.14	2010
3	Compulsory licensing	125	0.12	2010
4	Generic Drugs	107	0.19	2010
5	Drugs	70	0.17	2010
6	Patent Links	69	0.11	2010
7	Balance of interests	63	0.12	2010
8	Intellectual Property	54	0.2	2010
9	Patent Protection	49	0.14	2010
10	Patent Law	33	0.1	2010

3.6 Analysis of Emergent Words

The citation burst of keywords reflects the changes in hotspots and the emerging trends of topics in a particular research feld. As shown in Fig. 6, this study selects 20 keywords with high burst intensity in the drug patent field.

Table 4. Keyword clustering information

Cluster Number	Frequency	Cluster name	Centrality	Clustered sub-clusters
#0	48	Generic Drugs	0.86	Patent Links, Pharmaceutical Patent Protection, Listed drugs
#1	48	Pharmaceutical patents	0.733	Drug Accessibility, Pharmaceutical patents, Rationalization of technical effects
#2	41	Patents	0.858	Compulsory licensing, Public Health, Drug Accessibility
#3	39	Patent Protection	0.84	Intellectual Property Protection, Patent Protection, Reverse Payment Agreement
#4	35	Compulsory licensing	0.695	Compulsory licensing, Patent evergreening, Public Interest
#5	32	Intellectual Property	0.824	Pharmaceutical patent rights, Patent measurement, New Drug Research and Development
#6	31	Patentee	0.874	Patent protection duration, Intellectual Property Enforcement, Intellectual Property Agreement
#7	17	Proprietary drugs	0.897	Centralized Purchasing, Price negotiation mechanism, Innovative Drugs
#8	7	Patent Infringement	0.951	Principle of Equivalence, Patent Infringement, Technical Basis

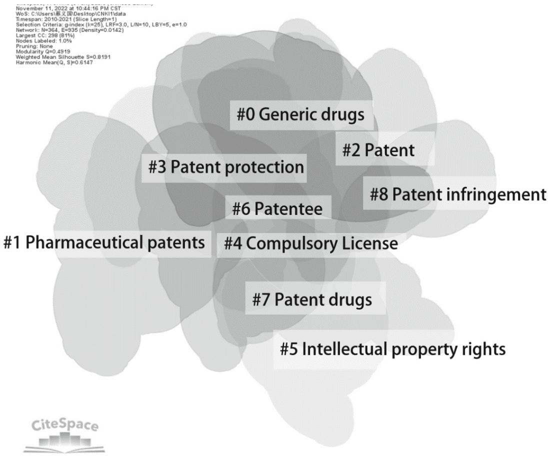
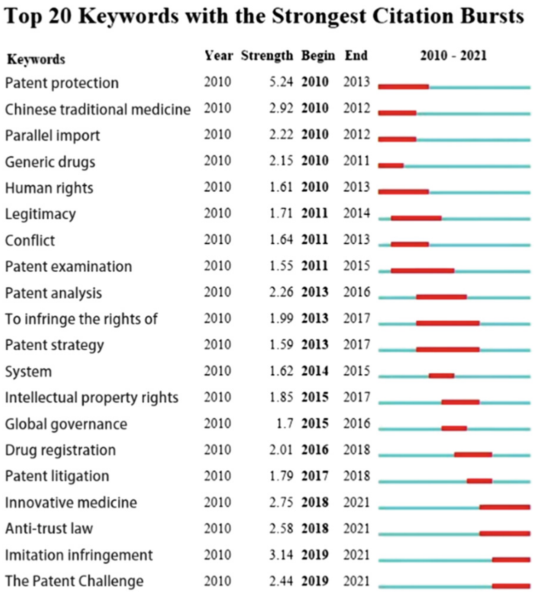

November 11, 2022 at 10:44:16 PM CST
WoS: C:\Users\蔡文国\Desktop\CNKI1\data
Timespan: 2010-2021 (Slice Length=1)
Selection Criteria: g-index (k=25), LRF=3.0, L/N=10, LBY=5, e=1.0
Network: N=364, E=935 (Density=0.0142)
Largest CC: 298 (81%)
Nodes Labeled: 1.0%
Pruning: None
Modularity Q=0.4919
Weighted Mean Silhouette S=0.8191
Harmonic Mean(Q, S)=0.6147
#0 Generic drugs
#2 Patent
#3 Patent protection
#8 Patent infringement
#6 Patentee
#1 Pharmaceutical patents
#4 Compulsory License
#7 Patent drugs
#5 Intellectual property rights
CiteSpace

Fig. 5. Keyword cluster network


Top 20 Keywords with the Strongest Citation Bursts

Keywords	Year	Strength	Begin	End
Patent protection	2010	5.24	**2010**	2013
Chinese traditional medicine	2010	2.92	**2010**	2012
Parallel import	2010	2.22	**2010**	2012
Generic drugs	2010	2.15	**2010**	2011
Human rights	2010	1.61	**2010**	2013
Legitimacy	2010	1.71	**2011**	2014
Conflict	2010	1.64	**2011**	2013
Patent examination	2010	1.55	**2011**	2015
Patent analysis	2010	2.26	**2013**	2016
To infringe the rights of	2010	1.99	**2013**	2017
Patent strategy	2010	1.59	**2013**	2017
System	2010	1.62	**2014**	2015
Intellectual property rights	2010	1.85	**2015**	2017
Global governance	2010	1.7	**2015**	2016
Drug registration	2010	2.01	**2016**	2018
Patent litigation	2010	1.79	**2017**	2018
Innovative medicine	2010	2.75	**2018**	2021
Anti-trust law	2010	2.58	**2018**	2021
Imitation infringement	2010	3.14	**2019**	2021
The Patent Challenge	2010	2.44	**2019**	2021

Fig. 6. Top 20 keywords with the strongest citation bursts

4 Conclusion

4.1 Literature Characterization

The authors agree that the network map presents an unstable core group of authors, and the number of individual publications of core authors is low, and there is a lack of in-depth research. In the distribution of author institutions, the scale of cooperation between institutions of higher learning and other institutions is relatively limited, and the cooperation between relevant authors and other institutions can expand the cooperation network.

The results of keyword co-occurrence network showed that "drug patent" and "public health" had large nodes and high centrality, followed by "generic drugs". This is because the development of medicines is linked to public health issues and in many developing countries has a direct impact on the public's access to necessary treatment and health services[12]. Imitation is a strategy for Chinese pharmaceutical enterprises to develop new products in the present and even in the future for a long time, and this way of R&D is the most likely to produce patent disputes[13]. However, the keywords such as "patent law" and "patent protection" appear less frequently, indicating that there are few legal and regulatory research levels in this field.

Combined with 9 key words clustering group and each cluster sub-cluster, the research content in this field is differentiated significantly, involving drug patent system, drug price, patent protection and other aspects.

Through the emergence graph of high-frequency keywords, it can be seen that the research hotpots have changed from the large scope of patent protection and patent analysis to the more detailed aspects of patent link, anti-monopoly law, patent challenge and data protection, so as to balance the interests of original pharmaceutical enterprises, generic pharmaceutical enterprises and public health.

4.2 Research Hotspots and Trends

Patent protection is a hot spot for research. At present, there are problems such as insufficient legislation on pharmaceutical intellectual property rights, difficulties in judicial handling of infringement cases, and inconsistency between authorization standards and infringement standards in China [14]. Solving the above problems is of great significance to strengthen patent protection and safeguard the interests of original drug enterprises, which is a study of patents from the perspective of original drug pharmaceutical enterprises.

The balance of interests is a hot topic that continues to rise. 2019 to 2024 is the second global drug patent cliff", and a large number of drug patents will expire [15]. Many generic drug companies will take advantage of the opportunity to seize the market to gain more benefits. The emergence of the drug patent linkage system will not only avoid patent infringement, but also reduce the waiting period for generic drugs to be marketed, which will benefit generic companies and patients.

Patent challenges and anti-monopoly are the future research trends in this field. On the one hand, it is to reduce the monopolistic behavior of pharmaceutical giants and allow a large number of generic drugs to enter the market in order to reduce drug prices. On the other hand, it is to stimulate the original drug companies to innovate continuously to produce drugs with better efficacy and fewer adverse reactions.

References

1. Yijia, W.: On the Protection of Pharmaceutical Patents [D]. Zhengzhou. Zhengzhou University, 2012: 13

2. Guan, R., Liu, S.: Mechanism and strategy of drug patent challenge[J]. Journal of Shenyang University of Technology (Social Science Edition) **15**(2), 97–103 (2022)
3. Xiaoxiao, H.: Improvement of the registration system of patent information of listed drugs in China[J]. Politics and Law **6**, 126–142 (2022)
4. Yue, C., Chaomei, C.: Methodological functions of CiteSpace knowledge graph[J]. Scientology Research, 33(2): 242–253 (2015)
5. Liang, Z.: The transplantation and creation of drug patent linkage system[J]. Politics and Law **8**, 104–114 (2017)
6. Liu, L., Zhu, X.: The choice of elements of drug patent linkage system in the United States and Canada and its inspiration to China[J]. China Science and Technology Fo-rum **1**, 147–154 (2014)
7. Cheng, Y., Lijuan, W.: Exploration of the establishment of drug patent linkage system in China[J]. Technology and Law **3**, 1–10 (2018)
8. Zhiwen Liang.Drug TRIPS-Plus protection in U.S. free trade agreements[J]. Comparative Law Research,2014(1):125–140
9. Hao, M.: The application of compulsory licensing system of drug patents in developing countries: from the case of Lu Yong, the first person to purchase anti-cancer drugs on behalf of others[J]. Intellectual Property Rights **8**, 95–101 (2015)
10. Yao, X.: Chuanping. Constructing a core author user database for a scientific journal **29**(1), 64–66 (2017)
11. Yue, X., GuiHua, X., Wang, Q., et al.: CiteSpace-based visualization of research hotspots in Chinese medicine for post-chemotherapy bone marrow suppression[J]. World Science and Technology - Modernization of Chinese Medicine **24**(2), 705–715 (2022)
12. Cao, H., Song, B., Wang, Z., et al.: Research on drug patent linkage system[J]. China Market Regulation Research **3**, 49–53 (2021)
13. Hao, M.: Drug registration and drug patents[J]. Journal of Chinese Medicine Man-agement **16**(10), 734–737 (2008)
14. Liu, T.: Economic analysis of domestic pharmaceutical intellectual property law at the present stage[J]. Legal Expo **34**, 23–25 (2020)
15. Seehttps://www.pharmaceuticalprocessingworld.com/impending-patent-cliff-threatens-billions-of-global-prescription-drug-sales/,Acces sed 16 November 2021

Ceramic Tile Production Intelligent Decision Research Based on Reinforcement Learning Algorithm

Rongjian Cheng[1], Yixiang Fang[1](✉), Yi Zhao[1], Tianzhu Zhang[1], Jun Li[1], Linna Ruan[2], and Junxiang Wang[1]

[1] Jingdezhen Ceramic University, Jiangxi 333403, China
fangyixiang@jci.edu.cn
[2] University of Melbourne, Victoria 3010, Australia

Abstract. Ceramic tile production includes a complex decision system, which involves several intelligent decision acts and might affect the product quality. In general, traditional ceramic tile production utilized many repeated empirical experiments based on their engineers to determine an appropriate production parameter and pursue the desired product quality. However, it is observed that traditional ceramic tile production mainly depends on empirical experiments and couldn't ensure a stable product quality. Moreover, the various surrounding environments for ceramic tile production might further result in a worse product quality when the empirical production parameters determined by empirical experiments couldn't be adjusted by the actual situation. To solve the issue that empirical production parameters determination in the traditional ceramic tile production, a ceramic tile production intelligent decision framework is firstly designed based on reinforcement learning algorithm (i.e., Deep Q-networks (DQN)) in the paper. In the framework, both environment and agent modules are built, where environment module is designed to simulate various surrounding environments for ceramic tile production and then predict the corresponding product quality in time by a self-prediction random forest (RF) model. In addition, agent module aims to rapidly adjust the production parameters adaptively based on the predicted product quality to achieve a desired final product quality. The experiment results indicate that proposed ceramic tile production intelligent decision framework could effectively solve adaptive production parameters determination issues in the practice.

Keywords: Prediction model · Reinforcement learning · Ceramic tile production · Production parameters

1 Introduction

The ceramic tile production industry is an important construction-related industry. China, as the world's largest producer, consumer, and exporter of ceramic tiles, has driven global expansion by sheer volume. However, the production of ceramic tiles is a fairly complex process involving numerous operating sessions and several production parameters (a

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 13–27, 2024.
https://doi.org/10.1007/978-981-99-7161-9_2

brief example is provided in Fig. 1, where equipment and production parameter include several variables). In general, the production parameters mostly rely on expertise and experience and have been determined through trial-and-error which results in uncontrollable product waste. Therefore, establishing an intelligent decision-making framework for ceramic tile production that overcomes the limitation of empirical is necessary.

As the production of ceramic tiles involves several phases, the correlation between production parameters and product performance is typically complex and ambiguous. In previous studies, fuzzy systems [1] and expert systems [2] were used to optimize the production parameters for ceramic tiles based on production data and human expertise. Currently, machine learning is commonly used to optimize the parameters automatically by computer algorithms. Deng et al. [3] used an orthogonal experiment design and back-propagation artificial neural networks (BP ANNs) to investigate an alumina slurry with excellent extrusion and shape retention properties. Ahmmad et al. [4] applied Random Forest (RF) to predict the density of novel oxy-fluoro glasses based on their chemical composition and ionic radii which acquired the highest R^2 compared with other Artificial Intelligence techniques. Similarly, Mu et al. [5] reported that artificial intelligence-aided is effective in the identification of ancient Chinese ceramics. There are some intelligent algorithms used in other related industries, but due to the more phases and great uncertainty in the ceramic production process, they are less used in ceramic production.

In industry 4.0 era, the processes of ceramic tiles manufacturing involve many production parameters. It is significant for us to search optimal production parameters among the huge searching space and thus achieve a desired product quality. The traditional methods either simplify certain insignificant details or require prior expert knowledge and manual intervention that results in not dealing with those problems flexibly among the huge searching space. The process of searching the optimal production parameters setting can be modeled as a Markov decision process, and reinforcement learning (RL) [6, 7] can effectively learn the optimal decision of the Markov decision process in high-dimension searching space that has been broadly used to tackle the practical optimization and decision-making problem in the industry. For example, in [8], the renewal price adjustment problem in the insurance industry was modeled as a sequential decision problem in terms of a Markov decision process (MDP), and the revenue is optimized subject to customer retention by the RL algorithm. Han et al. [9] used a proximal policy optimization algorithm in RL to construct an intelligent decision-making model for pavement maintenance plans, which could be applied to the increasing demand for pavement maintenance. The authors of [10] have applied dueling based deep reinforcement learning to optimally dispatch the household energy management system (HEMS). Guo et al. [11] employed a RL framework and a self-prediction artificial neural network model to approach the narrow process windows problem and could produce ultra-high precision products. He et al. [12] constructed a framework that transformed the textile process optimization problem into a stochastic game, and used a deep Q-networks algorithm to achieve the optimal solutions for the textile ozonation process in a multi-agent system. Related applications of RL for decision-making have been reported. However, at present, there is no complete study to solve a complex production parameters adjustment issue, especially in the ceramic tile manufacturing industry.

Inspired by the above methods, process parameter optimization is considered as a highly dynamic and complex decision-making process in ceramic tile production. This study aims at developing a decision-making framework for optimizing the ceramic tile manufacturing process based on RL. The key contributions of this paper are summarized as follows:

(1) Design a reinforcement learning-based production parameters optimization framework for the ceramic tile manufacturing process.
(2) Train self-prediction quality model. Establish a RF prediction model that can map the complex relationship between the production parameters and product quality by using the background data. Then employ the trained RF prediction model as a part of the environment module.
(3) Train RL decision model. Build and train a decision model for learning production parameter adjustment strategies through a reinforcement learning algorithm. The reinforcement learning agent would be trained by interacting with the environment.

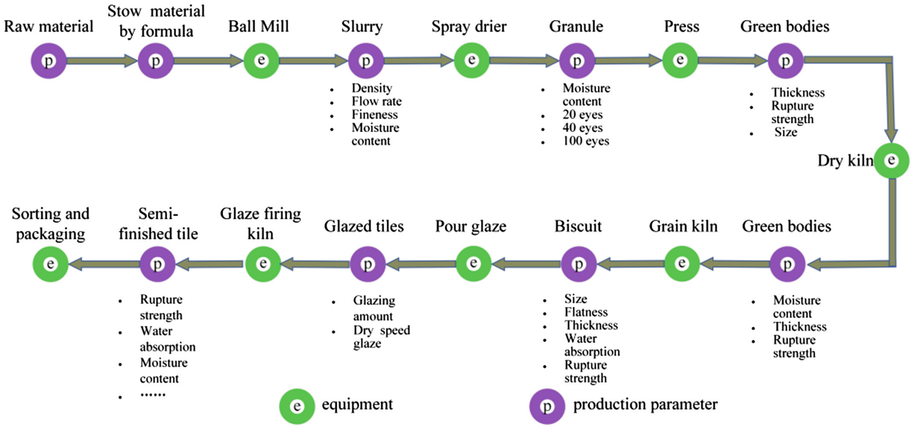


Fig. 1. The complete flow diagram for the ceramic tile production

2 Literature Review

2.1 Artificial Intelligent Techniques

In recent years, researches regarding predictive models based on various regression approaches or machine learning algorithms, such as support vector machine, artificial neural network and random forest have be used in many industries. Support vector machine is a popular machine learning tool for classification and regression, the excellent use of support vector machine in textile industry has been issued for predicting yarn properties [13]. In this study, high volume instrument and advanced fiber information system fiber test results consisting of different fiber properties are used to predict the rotor spun yarn strength. Cassar et al. [14] designed and trained an artificial neural network in predicting glass transition temperatures for more complex oxide glasses. A previous study [15] comparing the random forest with other machine learning to predict the T_g of glasses based on their chemical composition. The results show that the best machine learning algorithm for predicting T_g is the random forest. In this paper, the attempt of modeling the ceramic tile production process by the application of the three artificial intelligent techniques is conducted. The predicted models were constructed with corresponding optimization process to comparatively find the potential applicability of them in predicting the product performance of the ceramic tile production process. The model with fine prediction performance will be used to build the environment module of reinforcement learning. The model was realized by using the Scikit-learn library in Python 3.7.

2.2 Deep Q-networks Reinforcement Learning Algorithm

As an effective artificial intelligence method, reinforcement learning has been widely applied to deal with decision-making issues in various fields [16, 17]. Thus, this article uses DQN as a decision algorithm. The primary components of reinforcement learning are the autonomously learning agent module and the external environment module.

We used a typical reinforcement learning algorithm policy-based learning (DQN) [21] to solve the decision optimization problems. Different from some basic reinforcement learning algorithms is the special agent module. In order to address the dimensionality challenges of Q-learning [18], the DQN method employs a DNN in agent module, parameterized by θ, which takes as input a continuous state s_t and outputs an estimate of the Q-value function (i.e. $Q(s_t, \mathrm{a}_t) \approx Q_\theta(s_t, \mathrm{a}_t)$) for each discrete action. When agent learns the optimal strategy, the agent's decision in terms of which action A_t is chosen at a certain state S_t is driven by a policy $p(S_t) = A_t$. The agent changes its strategy for selecting actions based on the action's maximal value. At this time, the environment gives the agent a feedback reward $\mathrm{R_t}$ based the action's effect, and the environment reaches a new state S_{t+1}, then the agent repeats the above operations. The environment's state $s \in S$, where S is a finite set, similarly, $\mathrm{a} \in A$ and $r \in R$.

Considering the dynamic optimization procedure in ceramic tile production is a sequential decision problem that can be modeled as a Markov Decision Process (MDP). The MDP can be solved by reinforcement learning (RL) [22].

3 Proposed RL Framework in This Study

Figure 2 depicts the main structure of proposed RL framework, where the decision-maker acts as the agent to traverse and explore the state space in environment module, i.e., the different production parameters situations in ceramic tile production process. The environment module mainly consists of a pre-trained prediction model, and the adjustment of production parameters denotes the action. When RL framework optimizing production parameters, the agent module takes action on a state (production parameters) in the environment module and the environment transform the state to a new state, then prediction model take new state as input and output the variables (product quality). The variables are used to calculate the reward by designed reward function.

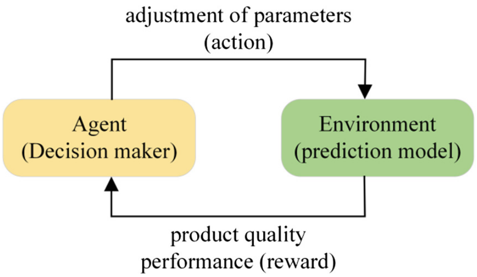


Fig. 2. The main structure of proposed RL framework

3.1 Problem Formulation

In this Subsection, we defined some parameter variables. The $\{pv_1, pv_2 \cdots pv_n\}$ is defined to denotes the production parameters in ceramic tile manufacturing process, while the multi-criteria of $\{c_1, c_2 \cdots c_n\}$ denotes the product quality corresponding to product parameters. Decision-making system in this paper needs to figure out how those parameter variables affect the product quality in terms of each criterion, and whether a solution set $\{pv_1, pv_2 \cdots pv_n\}$ is good or not relating to $\{c_1, c_2 \cdots c_n\}$, the product quality performance of the specific solution could be presented by:

$$f_i(pv_1, pv_2 \ldots pv_n)|c_i, for\ i = 1, \ldots m \tag{1}$$

When the domain of $pv_i \in PV_j$ is known, and the multi-criteria $\{c_1, c_2 \cdots c_m\}$ problem could be somehow represented by C, and the Eq. (1) could be simplified to (2), and so that the objective of decision-makers is to find (3):

$$f(pv_1, pv_2 \ldots pv_n)|C, pv_j \in PV_j \tag{2}$$

$$\text{argmax}_{pv_j \in PV_j}[f(pv_1, pv_2 \ldots pv_n)|C] \tag{3}$$

The objective of Eq. (3) is to find the optimal solution of variable settings, whereas prior operations in traditional ceramic tile production depended mainly on trial and error. Subsection 3.2 and 3.3 describes in detail how to utilize the RL model in the ceramic tile production decision-making.

3.2 Prediction Model

The application of prediction model in proposed decision-making framework is divided into two steps:

(1) Pre-trained the prediction model: a prediction mapping model could be built to predict the output corresponding to the input after the experience data are obtained. The model in this paper would be used to predict the quality characteristics under different process parameter conditions. The machine learning library of Scikit-learn is employed to develop the prediction models [22].

Prior to the experience data being fed to the prediction model, it should be preprocessed. The production parameters $\{pv_1, pv_2 \cdots pv_n\}$ and corresponding process response/outputs $\{c_1, c_2 \cdots c_n\}$ be processed by using the train_test_split function of scikit-learn, the data is split into training and test sets. A test size of 0.2 for all the experience data was fixed, it shows we could use 20% of the data for testing ensuring maximum reproducibility. The construction procedure is described below, and a forecast flow chart is shown in Fig. 3.

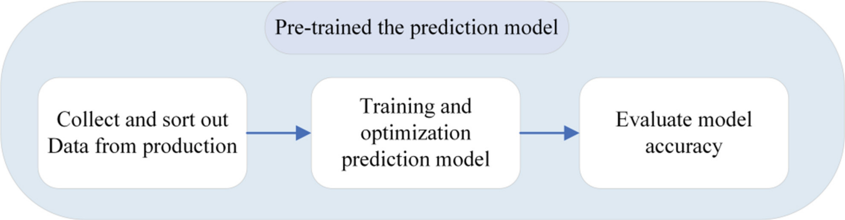

Pre-trained the prediction model
Collect and sort out Data from production
Training and optimization prediction model
Evaluate model accuracy

Fig. 3. The construction process of the prediction model

We demonstrate the process optimization method to improve the performance of ceramic tiles by considering a small subset of the process variables. This model later can be extended to encompass all relevant parameters. The two prediction models we established adopted two parts of data respectively. The one production parameters data come from multi-process (Spray drying, Press, Kiln), and the other from Single-process (Spray drying).

(2) Employ the trained prediction model as a part of the environment module: After comparing the prediction performance of support vector machine, artificial neural network and random forest prediction models. The random forest (RF) predictive model, constructed using Multivariate Random Forest (MRF) [23] in which a sample input has more than one target output, is applied to simulate the ceramic tile production process in the proposed framework.

3.3 DQN for Ceramic Tile Production Decision

The ceramic tile production decision RL model based on DQN is presented as follows. Figure 4 illustrates the framework for the proposed decision model to address our problems, which would be attempted to solve the performance quality optimization problem of the spray drying process.

In our scheme, the agent continuously interacts the values/parameters with the environment module, which feedbacks the rewards to the agent. Through cumulative rewards, the agent is expected to learn to control the process parameter of the spray drier in order to meet the production granule performance that minimizes the difference between such specific process treated granule product and the targeted sample performance.

In this paper, the decision-making problem is modeled as an MDP, which consists of a tuple of five elements (S, A, T, r, γ). Where T is a state transition probability function $T(s_{t+1}|s_t, a_t)$. The details of those elements are described as follows:

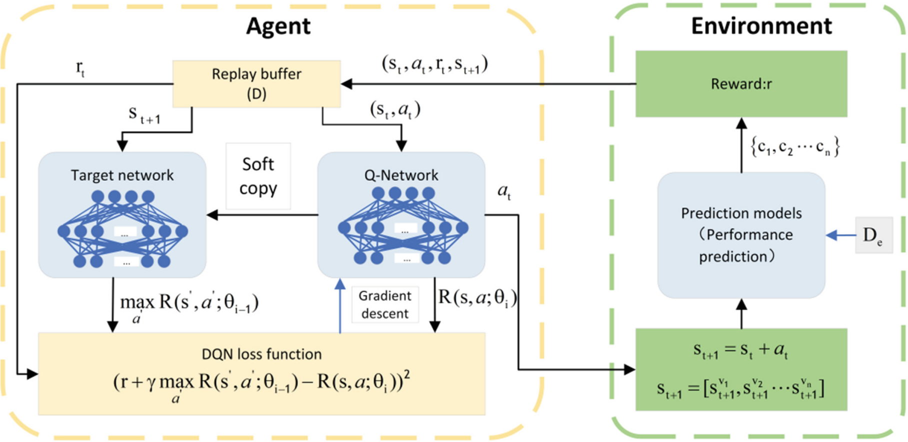

Agent
Environment
r_t
Replay buffer (D)
(s_t, a_t, r_t, s_{t+1})
s_{t+1}
(s_t, a_t)
Reward:r
$\{c_1, c_2 \cdots c_n\}$
Target network
Soft copy
Q-Network
a_t
Prediction models (Performance prediction)
D_e
$\max_{a'} R(s', a'; \theta_{i-1})$
Gradient descent
$R(s, a; \theta_i)$
DQN loss function
$(r + \gamma \max_{a'} R(s', a'; \theta_{i-1}) - R(s, a; \theta_i))^2$
$s_{t+1} = s_t + a_t$
$s_{t+1} = [s_{t+1}^{v_1}, s_{t+1}^{v_2} \cdots s_{t+1}^{v_n}]$

Fig. 4. Workflow of the algorithm implementing the proposed DQN method for ceramic tile manufacturing process optimization.

State space S: A state space $s_t \in S$ in this case is composed by the solutions with four production parameters (burning temperature, inlet air temperature, exhaust temperature, temperature of the tower), which is the input parameters $\{pv_1, pv_2 \cdots pv_n\}$ of the prediction model in environment module. It is described as $S_t = \{s_t^{pv1}, s_t^{pv2}, s_t^{pv3}, s_t^{pv4}\}$, where $s_t^{pv_k}$ is the current value of the kth process parameter.

Action space A: An action that recommends an adjustment amount of the production parameters based on the current s_t, is denoted as $A_t = \{a_t^{pv1}, a_t^{pv2}, a_t^{pv3}, a_t^{pv4}\}$. The four corresponding production parameters are controlled by the agent within the constraints. As the action of a single variable pv_k could be kept as 0 or adjusted in the given range with specific unit u, where $a_t^{pv_k} \in \{-u_k, 0, +u_k\}$.

Transition function P: The transition function maps a given input state s_t and an action a_t to the next state s_{t+1}. The transition probability is 1 for the states in the given range of the state space above, but 0 for the states out of it.

Reward R: The immediate reward that the agent receives at any time step t is a function of the current states and the control action taken by the agent, given by $r_t(s_t, a_t)$. We set up the reward function as illustrated below to induce the agents to realize the corresponding optimization objectives:

$$r_t = \sum_{i=1}^{k} (f_i(s_{t+1}) - pc_i) - \sum_{i=1}^{k} (f_i(s_t) - pc_i) \tag{4}$$

where pc_i denotes the expected granule performances of spray drier product output, and the $f_i(s_t)$ represents the prediction output (moisture content, 20 eyes, 40 eyes, 100 eyes) of the prediction model.

Discount rate γ: The discount rate γ for updating the loss function, when $\gamma = 0$, the agent only considers the immediate reward to take action. Conversely, when $\gamma = 1$, the agent will take action by considering all future rewards. We set it as 0.9 here.

The setting parameters of DQN after the experiment adjustment illustrate as follows. Here the number of time steps N set as 5000 for each episode, the replay memory size D is 2000, the learning rate is 0.01, and etc. In particular, the step F for updating DQN here denotes that the Q-networks would be updated at every 5 steps after 100 steps.

Using the preceding notations and definitions, the problem of production parameter optimization can be characterized formally as follows: through interactions between the agent and the environment, the agent is anticipated to discover the control strategies that maximize the cumulative rewards. Actual production can be guided by optimal production parameter conditions that meet quality criteria.

4 Experiment and Discussion

In this section, the experiment settings are explained and the simulations are performed by training the prediction model and the decision-making model. Experiments are conducted to examine the effectiveness of the proposed framework.

4.1 Ceramic Process Parameter Definition

Table 1. The value range in continuous process parameter

Process parameter	Type	Lower bound	Upper bound
Granule moisture (%)	Input	6.0	6.7
Granule unit weight	Input	0.892	0.935
Thickness of green bodies(mm)	Input	9.05	9.37
Moisture of dried green	Input	0.59	0.79
Temperature of kiln (°C)	In-process	Several temperatures of firing curve	
Rupture modulus (label 1)	Output	17.65	24.43
Water absorption (label 2)	Output	16.32	20.93
Biscuit size (mm) (label 3)	Output	607.53	609.14
Biscuit thickness (mm) (label 4)	Output	8.97	9.37

The background data in ceramic tile production utilized in this study to completed two sets of experiments. The data of the first set are: continuous process production parameters (Spray drier, Press, Kiln) include several parameters which before kiln as input variables, and process response parameters (e.g., quality characteristics of ceramic tile) as the output variables. The data set consists of 348 input-output pairs. Full details of the parameters are described in Table 1.

The data of the second set are: single session production parameters. The single session parameters collected from spray drier, including operating conditions and output granule performance record within a detection cycle. A few features of the proposed "Input", "In-process", and "Output" variables of spray drying are summarized in Table 2, where the ‘In-process’ variable is generated through internal treatments of spray drying. The data set consists of 203 input-output pairs. However, the process of ceramic tile production is mainly impacted by the complexity of the interdependent and correlated process variables, it is felt that a full theoretical understanding of spray drying treatments like all other complex processes would be helpful for ‘production line’ to achieve intelligent decision.

Table 2. Constraints and adjustment step sizes of spray drier production parameters.

Process parameter	Type	Lower bound	Upper bound	Step size(u)
Burning temperature (°C)	In-process	1001	1044	2
Inlet air temperature (°C)	In-process	640	659	1
Exhausted air temperature (°C)	In-process	97	125	2
Tower temperature (°C)	In-process	428	460	2
Slip feeding pressure (Mpa)	Input	30	33.2	–
Slip specific gravity	Input	1.68	1.707	–
Moisture content (%) (label 1)	Output	5.2	6.4	–
20 eyes(g) (label 2)	Output	0.15	0.54	–
40 eyes(g) (label 3)	Output	48.2	56.37	–
100 eyes(g) (label 4)	Output	0.41	2.16	–

4.2 Prediction Model Building Based on Various Parameters

According to the above two set of parameters, we are going to establish prediction model and give the prediction results to verify. In order to verify the prediction effect and combination with practical applications, we classified the output parameters. Generally, a standard range would be imposed on every output production quality feature. The median values of the upper and lower ranges of some feature parameters are better, and other feature parameters should not be lower than or exceed a certain limit value are better. It is unacceptable if the feature parameters are beyond the standard range, so the “In-process” variables must be controlled when the parameters are close to the boundary of the standard range. We divided the output parameters into two categories based on the experts’ experience and production conditions, one representing the range (0) within which the “In-process” variables should be controlled, and the other representing the safety range (1) within which the operating conditions could be maintained. The classified details are described in Fig. 5 as follows:

$$\begin{cases} 1, \quad Q_{\min} + \lambda(Q_{\max} - Q_{\min}) \le Q \le Q_{\max} - \lambda(Q_{\max} - Q_{\min}) \\ 0, \; Q \le Q_{\min} + \lambda(Q_{\max} - Q_{\min}) or Q_{\max} - \lambda(Q_{\max} - Q_{\min}) \le Q \end{cases} \tag{5}$$

$$\begin{cases} 1, \; Q_{\max} - \delta(Q_{\max} - Q_{\min}) \le Q \le Q_{\max} \\ 0, \; Q_{\min} \le Q \le Q_{\max} - \delta(Q_{\max} - Q_{\min}) \end{cases} \tag{6}$$

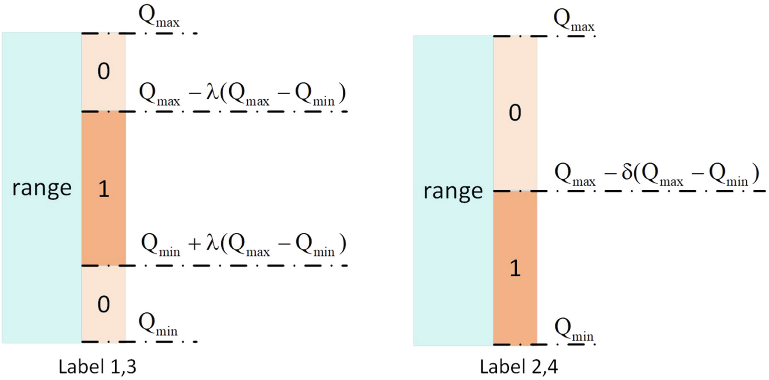

range
0
1
0
Q_{max}
$Q_{max} - \lambda(Q_{max} - Q_{min})$
$Q_{min} + \lambda(Q_{max} - Q_{min})$
Q_{min}
Label 1,3
range
0
1
Q_{max}
$Q_{max} - \delta(Q_{max} - Q_{min})$
Q_{min}
Label 2,4

Fig. 5. Classification criteria for the parameters involved.

Where Q is the actual quality characteristic. The Q_{min} is the lower bound value and Q_{max} is the upper bound value. The threshold λ(0.25) and $\delta(0.5)$ is set up by the experts.

Prediction models are built according to the background data introduced in the subsection above. Next, we will complete the experiment of prediction models:

Experiment I: The first is a multi-session parameters model for optimizing the experimentation and process controlling.

Experiment II: The second is a spray drying process model for revealing the relationships between the input and output variables.

Multi-Session Parameters and Spray Drying Process Modeling and Prediction. For Experiment I, we trained the prediction models to predict the quality characteristics of ceramic tile. And the prediction result is obtained according to formula (7). The prediction performance of models displayed in Table 3. It is observed that the experimental results meet the expected requirements, and the prediction model is meaningful for practical engineering use. and the random forest prediction model has better prediction performance.

The overall classification accuracy, can be expressed as

$$accuracy\_score = \frac{TP + TN}{TP + FN + FP + TN} \tag{7}$$

where TP, FP, TN, and FN denote the classification results determined as true positive, false positive, true negative, and false negative, respectively.

Spray Drying Process Modeling and Prediction. for experiment II, We trained the prediction models to predict four objective granule performances of the spray drier output product. And the prediction result is obtained according to formula (7). The prediction performance was displayed in Table 4. It is observed that the experimental results meet the expected requirements, and could be used in the environment module for train the proposed decision framework. Random forest also has better prediction performance in this group of experiments. thus, we use the random forest to construct the environment part.

Table 3. The accuracy_score of multi-station parameters

	Rupture modulus	Water absorption	Biscuit size	Biscuit thick-ness
Support vector machine	0.81	0.84	0.78	0.80
Artificial neural network	0.82	0.83	0.79	0.77
Random forest	0.84	0.86	0.81	0.81

Table 4. The accuracy_score of granule production parameters

	Moisture content	20eyes	40eyes	100eyes
Support vector machine	0.83	0.85	0.90	0.88
Artificial neural network	0.81	0.87	0.91	0.89
Random forest	0.83	0.88	0.92	0.9

4.3 Deep Q-networks for Optimal Decision-Making Analysis

Production parameter optimization is a very important procedure in the ceramic tile process and has not been resolved to date. Changes in production parameters could notably affect product quality, especially at spray drying process. In spray drying process, the production parameter types consist of "In-process" and "Input" are illustrated in Table 2. Compared with the "In-process" in production, the "Input" in production be adjusted frequently. Therefore, the proposed decision-making model mainly controls product quality by adjusting "In-process" parameters. The production parameters composed the state $S_t = \{s_t^{\omega 1}, s_t^{\omega 2}, s_t^{\omega 3}, s_t^{\omega 4}\}$ that could be adjusted by $A_t = \{\mathrm{a}_t^{\omega 1}, \mathrm{a}_t^{\omega 2}, \mathrm{a}_t^{\omega 3},\mathrm{a}_t^{\omega 4}\}$ when the decision model is training. Due to the single action vector $a_t^{\omega k} \in \{-u_k, 0, u_k\}$,$k \in \{1, 2, 3, 4\}$. In the time step t, the unit u_k, $k \in \{1, 2, 3, 4\}$ of these parameter variables are 2, 1, 2, and 2 respectively. The action A_t could be any combination of the elements from the following action vector sets: $\{+2, 0, -2\}$, $\{+1, 0, -1\}$, $\{+2, 0, -2\}$ and $\{+ 2, 0, –2\}$. The total number of action spaces should be $3^4 = 81$. In order to validate the applicability of this decision-making framework, the experiments are designed to find the solution in the spray drier process to achieve the target granule performance. For contrast, the original granule performance results are listed in Table 5. It is found that there is only a small amount of '1' in the actual classification value of output.

In particular, the neural networks implemented by TensorFlow [24] are employed to realize Q-networks. The networks consist of two layers with 50 and 3^4 hidden nodes respectively, where the latter layer corresponds to the actions. As demonstrated in Table 5, there are 10 targeted experimental samples that were used in the present instance. The loss function of target Q-networks for each scenario are converged quickly to be steady after training. Five of the ten experimental samples, which serial number is from 1 to 10 odd integer, are selected to display the loss value during the iteration. The variations in the loss value during the iteration are shown in Fig. 6.

Table 5. Experimental data to be optimized

Burning temperature	Inlet air temperature	Exhausted air temperature	Tower temperature	Slip feeding pressure	Slip specific gravity	Output classification			
1030	655	105	436	30.3	1.7	0	1	0	0
1030	655	104	442	30.5	1.697	1	0	0	1
1031	650	100	437	30.9	1.69	0	1	0	0
1032	655	101	449	31.1	1.68	0	0	0	1
1037	655	102	451	31.1	1.68	1	0	0	1
1022	655	104	438	31.4	1.68	1	1	0	0
1035	645	108	460	32.5	1.696	0	0	1	0
1035	650	110	457	31.9	1.696	1	0	1	0
1036	650	111	450	31.5	1.68	0	1	0	0
1024	640	111	438	30.8	1.7	0	0	1	1

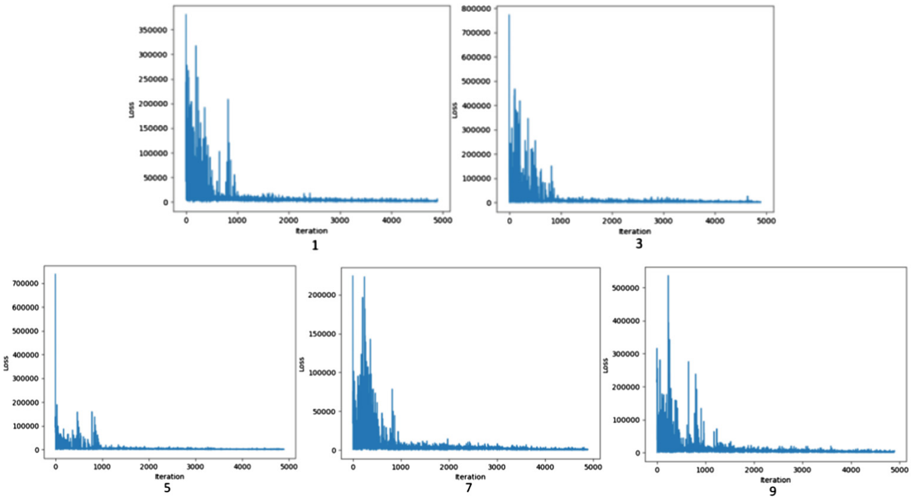


Fig. 6. The loss function of target networks for each scenario with several targets.

The loss function fluctuated greatly in the early stage due to the instability of the training in Fig. 6, and it began to converge and gradually became stable after about 800 iterations. As demonstrated in Table 6, there are still some optimized results which did not achieve the desired effect. This indicates that more iteration steps are needed to make the model more efficient.

The objective of the experiment is to utilize the deep reinforcement learning algorithm and to alter the input equipment operation parameter values, such that the relevant performance parameters are more classified to be ‘1’ and the optimization decision

Table 6. Optimized results by decision-making model (800 iterations)

Burning temperature	Inlet air temperature	Exhausted air temperature	Tower temperature	Slip feeding pressure	Slip specific gravity	Output classification			
1044	657	125	460	30.3	1.7	1	0	1	1
1004	659	120	428	30.5	1.697	1	0	1	1
1003	641	122	427	30.9	1.69	0	1	1	1
1030	642	97	427	31.1	1.68	1	1	1	1
1035	642	126	459	31.1	1.68	0	0	1	1
1018	647	118	430	31.4	1.68	1	1	1	1
1038	648	116	452	32.5	1.696	1	0	1	1
1003	650	115	443	31.9	1.696	1	0	1	1
1006	642	125	454	31.5	1.68	0	1	1	1
1036	646	100	454	30.8	1.7	1	0	1	1

process is realized. It is discovered that the reward function can effectively guide the agent to find the optimum solutions in the environment by the proposed RL scheme. Finally, the agent's rewards converge to a maximum value, which indicates that our agent could learn how to adjust the production parameters according to the interactions with the environment. The optimized process parameter settings by RL model are shown in Table 7.

Table 7. Optimized results by decision-making model (5000 iteration)

Burning temperature	Inlet air temperature	Exhausted air temperature	Tower temperature	Slip feeding pressure	Slip specific gravity	Output classification			
1018	655	99	430	30.3	1.7	1	1	1	1
1030	659	126	430	30.5	1.697	1	1	1	1
1045	645	110	461	30.9	1.69	1	0	1	1
1000	647	105	443	31.1	1.68	1	1	1	1
1039	658	110	461	31.1	1.68	1	0	1	1
1026	640	96	432	31.4	1.68	1	1	1	1
1023	640	122	428	32.5	1.696	1	1	1	1
1035	647	98	439	31.9	1.696	1	1	1	1
1008	642	107	428	31.5	1.68	1	1	1	1
1030	644	105	428	30.8	1.7	1	1	1	1

5 Conclusions and Future Work

In this paper, we firstly designed a ceramic tile production intelligent decision framework based on reinforcement learning algorithm. In order to simulate various surrounding environments for ceramic tile production, we constructed a self-prediction random forest (RF) model to predict the product quality. Then employ the trained RF prediction model is used as a part of the environment module in reinforcement learning. And the optimized results are displayed in Table 7, comparing with the original process parameter depicted in Table 5, where the optimized results received more categorization value of '1' by the decision-making framework that demonstrates the model's validity. Future study on the decision-making process of the ceramic tile production based on reinforcement learning will primarily concentrate on investigation of the prediction performance of the ceramic tile production parameters, and determine the practical effects of this system for industrial implementation.

Acknowledgements. This work was supported by the National Natural Science Foundation of China under Grant No.62062044 and 62063010.

References

1. Qin, Y., Jia, L.M.: Fuzzy hybrid control and its applications in complex combustion processes. IEEE Int. Conf. Artif. Intell. Syst., 78–81(2002)
2. Zhu, Y.H., Zhao, Y.F.: Hybrid intelligent control of ceramic shuttle kiln firing temperature, (2016)
3. Deng, L.N., Feng, B., Zhang, Y.: An optimization method for multi-objective and multi-factor designing of a ceramic slurry: Combining orthogonal experimental design with artificial neural networks. Ceram. Int. **44**, 15918–15923 (2018)
4. Ahmmad, S.K., Jabeen, N., Ahmed, S.T.U., et al: Density of fluoride glasses through artificial intelligence techniques. Ceram. Int. **47**, 30172–30177 (2021).
5. Mu, T.H., Wang, F., Wang, X.F., et al.: Research on ancient ceramic identification by artificial intelligence. Ceram. Int. **45**, 18140–18146 (2019)
6. Silver, D., Schrittwieser, J., Simonyan, K., et al.: Mastering the game of Go without human knowledge. Nature **550**, 354–359 (2017)
7. Chen, Y.F., Wang, Z., Wang, Z.J., et al.: Automated design of neural network architectures with reinforcement learning for detection of global manipulations. IEEE J. Sel. Top. Signal Process. **14**, 997–1011 (2020)
8. Krasheninnikova, E., García, J., Maestre, R., et al.: Reinforcement learning for pricing strategy optimization in the insurance industry. Eng. Appl. Artif. Intell. **80**, 8–19 (2019)
9. Han, C.J., Ma, T.: Chen, S.Y, Asphalt pavement maintenance plans intelligent decision model based on reinforcement learning algorithm. Constr. Build. Mater. **299**, 124278 (2021)
10. Ren, M.F., Liu, X.F., Yang, Z.L., et al.: A novel forecasting based scheduling method for household energy management system based on deep reinforcement learning. Sustain. Cities Soc. **76**, 103207 (2021)
11. Guo, F., Zhou, X.B., Liu, J.H., et al.: A reinforcement learning decision model for online process parameters optimization from offline data in injection molding. Appl. Soft Comput. **85**, 105828 (2019)

12. He, Z.L., Tran, K.P., Thomassey, S., et al.: Multi-Objective optimization of the textile manufacturing process using Deep-Q-Network based Multi-Agent reinforcement learning. J. Manuf. Syst. **62**, 939–949 (2022)
13. Nurwaha, D., Wang, X.H.: Prediction of rotor spun yarn strength using support vector machines method. Fibers Polym. **12**, 546–549 (2011)
14. Daniel, R.C., André, C.P.L.F.C., Edgar, D.Z.: Predicting glass transition temperatures using neural networks. Acta Materialia **18**, (2018)
15. Alcobaca, E., Mastelini, S.M., Botari, T., et al.: Explainable machine learning algorithms for predicting glass transition temperatures. Acta Mater. **188**, 92–100 (2020)
16. Qin, S.J., Cheng, L.: A real-time tracking controller for piezoelectric actuators based on re-inforcement learning and inverse compensation. Sustain. Cities Soc. **69**, 102822 (2021)
17. Vinyals, O., Babuschkin, I., Czarnecki, WM., et al.: Grandmaster level in StarCraft II using multi-agent reinforcement learning. Nature., 1–5 (2019)
18. Sutton, R.S., McAllester, D., Singh, S., et al.: Policy gradient methods for reinforcement learning with function approximation. Adv. Neural. Inf. Process. Syst. **12**, 1057–1063 (1999)
19. Watkins, C.J.C.H., Dayan, P.: Technical note: Q-learning. Mach. Learn. **8**, 279–292 (1992)
20. Sutton, R.S., Barto, A.G.: Reinforcement Learning: An Introduction. Massachusetts, Cambridge (2018)
21. Mnih, V., Kavukcuoglu, K., Silver, S., et al.: Human-level control through deep reinforcement learning. Nature **518**, 529–533 (2015)
22. Pedregosa, F., Varoquaux, G., Gramfort, A., et al.: Scikit-learn: Machine learning in python. J. Mach. Learn. Res. **12**, 2825–2830 (2011)
23. Rahman, R., Otridge, J., Pal, R.: IntegratedMRF: random forest-based framework for integrating prediction from different data types. Bioinformatics **33**, 1407–1410 (2017)
24. Abadi, M., Agarwal, A., Barham, P., et al.: TensorFlow: Large-Scale machine learning on heterogeneous distributed systems. ArXiv, 265–283 (2016)

Distributed Physical Device Connection Relationship Discovery Technology Based on Traffic Information

Jiaxing Wang[1](✉), Junyan Rui[2], Huibo Niu[3], Yuan Chang[3], and Jiawen Hu[4]

[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, No. 10 Xitucheng Road, Haidian District, Beijing 100876, China
wangjiaxing@bupt.edu.cn

[2] School of Computer Science and Technology of Anhui University, Anhui, China

[3] China Aerospace Science and Industry Network Information Development Co., Ltd., Beijing, China

[4] University of Waterloo, Ontario, ON, Canada

Abstract. Cloud data center networks have a complex structure, in which multiple network protocols are utilised to participate in the composition of the data center. How to achieve topology discovery and mapping in the face of complex, multi-structured cloud data centre network devices has become a hot research problem. Network tomography (NT), as an end-to-end measurement technique of network boundaries, enables protocol-independent network measurements without the collaboration of internal nodes. The emergence of this technique provides a new research idea for cloud data center network topology mapping. In this paper, we propose a topology discovery technique based on the delay covariance matrix and a topology optimisation method based on the delay peak map, and conduct simulations for these two algorithms to verify the feasibility of the protocol-independent topology discovery technique applied to data center topology discovery.

Keywords: Cloud data center network · Topology discovery · Data flow · Delay covariance matrix

1 Introduction

With the rapid development of cloud data center networks in industry [1], how to quickly implement the mapping of network structures has become one of the hot research problems at present. A large number of research results [2,3] have been developed for mapping the network structure of the Internet and IoT, and a series of structure mapping methods such as SNMP-based protocols [4], DNS-based protocols [5], and ARP-based protocols [6] have been developed, but all these methods rely on a specific network protocol and are difficult to be applied

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 28–41, 2024.
https://doi.org/10.1007/978-981-99-7161-9_3

in cloud data center networks with dynamically changing structures and cross-network protocols. Therefore, how to achieve fast topology discovery for complex and changing cloud data centers without relying on a specific protocol is a key problem that needs to be addressed.

Most of the current topology discovery techniques, apart from relying on a single protocol, utilize the idea of active probing [7] to send probe packets into the network to be tested, which can have a large impact on the normal operation of the network due to the need to send additional probe packets and can be easily detected by the network being probed in the actual network probe discovery. Therefore, there is an urgent need for a method that draws on the idea of passive probing to achieve the discovery of devices in the network as well as network connectivity relationships using the traffic data information generated in the normal operation of the network without disrupting the normal operation of the network and without increasing the network load.
The main contributions of this paper are as follows.

- A topology discovery idea for diversifying cloud data center networks using traffic analysis under the passive detection idea is proposed. The advantage of this idea is to achieve fast discovery of network topology based on latency with a large amount of traffic data obtained without relying on specific protocols and without increasing the network load and disrupting the normal operation of the network.
- A topology discovery technique based on the delay covariance matrix is designed. In this paper, the feasibility of using delay analysis is analyzed and simulations based on traffic data are carried out.
- A topology optimization method based on the delay peak graph is proposed, which analyses the topology for common topologies in the network, eliminates the influence of possible anonymous routers, enables the subsumption of virtual links and further optimizes the topology discovery results.

The main structure of this paper is as follows: Chap. 1 introduces the research background and the main contributions of this paper. Chapter 2 presents the research work related to the study of this paper. Chapter 3 proposes a topology discovery technique for the time-delay covariance matrix, Chap. 4 proposes a topology optimization method based on the time-delay peak map, and simulates the proposed algorithm in Chap. 5 and concludes in Chap. 6.

2 Related Works

There are a number of studies addressing network topology discovery. Alhanani et al. [8] present a review of network topology discovery algorithms, discussing and comparing a variety of appropriate techniques for extracting network management information through traditional methods, protocols and through graph theory, genetic algorithms and bee colony algorithms belonging to artificial intelligence.

Breitbart et al. [9] implemented the designed algorithm for physical topology discovery in heterogeneous IP networks relying on SNMP MIB information, in the context of the NetInventory topology discovery tool, which can consistently and accurately discover the physical network topology and maintain good operational efficiency even in fairly large network configurations. In addition to this, HaoWang [10] designed an improvement to the traditional SNMP algorithm with the aim of achieving efficient and accurate management of computer networks and ensuring stable operation of computer networks in a variety of applications, optimising the SNMP algorithm for the heterogeneity of network devices, thus achieving the universality of network topologies. However, due to the specificity of cloud data centre networks, a single topology discovery algorithm that relies on SNMP technology is not applicable to the complex and variable cloud data centre networks.

Wei et al [11] proposed a multi-featured subnet discovery algorithm to solve the low accuracy problem caused by insufficient boundary conditions and integrity of factor networks, which focuses on the traceroute path characteristics of IPs in the same subnet, thus iteratively solving the subnet discovery problem. The traceroute-based topology discovery technique is an active detection technique, and this reliance on ideas can cause disruption to the normal operation of the network, and relying on additional traffic information for topology discovery is a huge drain on large data centres.

3 Topology Discovery Techniques Based on Time Delay Covariance Matrix

In order to achieve fast and efficient discovery of network topology without disturbing the normal operation of the network, the collected traffic data can be analysed with the help of delay covariance matrix [12], and fast topology discovery can be achieved with the help of traffic covariance matrix.

Definition 1. The same source node sends packets to two different destination nodes through paths that may or may not overlap, and the part of the path that overlaps is said to be a shared path. Two possible path scenarios are shown in the Figs. 1 and 2.

The main idea of the algorithm is to analyse the value of covariance calculation between two or more nodes with the same source node and different destination nodes. When the source nodes are the same, two different destination nodes may or may not have a shared path, and the covariance enables the discovery of shared paths.

Proposition 1. *Packets are sent from the same source node to two different destination nodes, and the traffic covariance between the two destination nodes is calculated, with the value of this covariance relating only to the shared paths within it. The equation is expressed as:*

$$\operatorname{Cov}\left(T_i(k), T_j(k)\right) = E\left[\widetilde{T}_{i,hared}\left(k\right) \cdot \widetilde{T}_{j,\ shared}\left(k\right)\right] \tag{1}$$

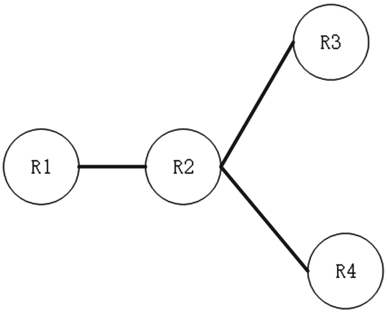


Fig. 1. Cases with shared paths

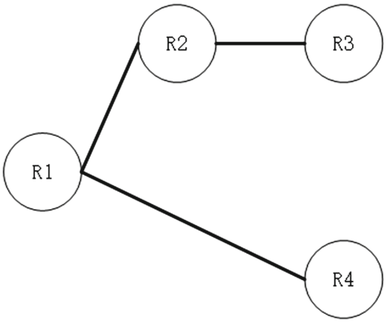


Fig. 2. Cases without shared paths

where i and j denote the two destination nodes,$\widetilde{T}_{m,\ shared}\,(k), m = i, j$ *denotes the delay of the shared path of the path corresponding to the two destination nodes i, j.*

Proof. The corresponding covariance of the two destination nodes is written as:

$$\operatorname{Cov}\left(T_i(k), T_j(k)\right) = E\left[\widetilde{T}_i(k) \cdot \widetilde{T}_j(k)\right] \tag{2}$$

where $\tilde{T}_m(k) = T_m(k) - \mu_m, m = i, j, \quad \mu_m, m = i, j$ denotes the average RTT in each case. In addition to this format, $\tilde{T}_m(k), m = i, j$ can also be written in the following form:

$$\tilde{T}_m(k) = \widetilde{T}_{m,\text{ shared}}\,(k) + \widetilde{T}_{m,\text{ unshared}}\,(k), m = i, j \tag{3}$$

where $\widetilde{T}_{m,\text{ shared}}\,(k), m = i, j$ denotes the delay of the shared path of the path corresponding to the two destination nodes i, j, $\widetilde{T}_{m,\text{ unshared}}\,(k), m = i, j$ denotes the remaining path segment delay. So the formula for the time delay can be further simplified.

$$\begin{aligned}
&\operatorname{Cov}\left(T_i(k), T_j(k)\right)=E\left[\widetilde{T}_i(k)\cdot\widetilde{T}_j(k)\right]\\
&=E\left[\left(\widetilde{T}_{i,\text{ shared }}(k)+\widetilde{T}_{i,\text{ unshared }}(k)\right)\cdot\left(\widetilde{T}_{j,\text{ shared }}(k)+\widetilde{T}_{j,\text{unshared }}(k)\right)\right]\\
&=E\left[\widetilde{T}_{i,\text{ shared }}(k)\cdot\widetilde{T}_{j,\text{ shared }}(k)+\widetilde{T}_{i,\text{ shared }}(k)\cdot\widetilde{T}_{j,\text{ unshared }}(k)\right.\\
&\left.+\widetilde{T}_{i,\text{ unshared }}(k)\cdot\widetilde{T}_{j,\text{ shared }}(k)+\widetilde{T}_{i,\text{ unshared }}(k)\cdot\widetilde{T}_{j,\text{ unshared }}(k)\right]\\
&=E\left[[\widetilde{T}_{i,\text{ shared }}(k)\cdot\widetilde{T}_{j,\text{ shared }}(k)\right]+E\left[[\widetilde{T}_{i,\text{ shared }}(k)\cdot\widetilde{T}_{j,\text{ unshared }}(k)\right]\\
&+E\left[[\widetilde{T}_{i,\text{ unshared }}(k)\cdot\widetilde{T}_{j,\text{ shared }}(k)\right]E\left[[\widetilde{T}_{i,\text{ unshared }}(k)\cdot\widetilde{T}_{j,\text{ unshared }}(k)\right]
\end{aligned} \tag{4}$$

Since the two segments that are not shared paths are uncorrelated, the above equation can be further simplified based on the uncorrelated nature of the covariance. The final result is obtained as follows:

$$\operatorname{Cov}\left(T_i(k), T_j(k)\right)=E\left[\widetilde{T}_{i,,\text{hared }}(k)\cdot\widetilde{T}_{j,\text{ shared }}(k)\right] \tag{5}$$

The above equation shows that the covariance of the time delay of two paths with different destination nodes at the same source node is only related to the shared path in them. With the help of this conclusion, it is possible to determine whether there is a shared path between two paths by the time delay.

When we extend the discovery of topological relationships to large networks, suppose n nodes are discovered and an N*N covariance matrix is constructed.

$$\begin{bmatrix} \sigma_{1,1}^2, \sigma_{1,2}^2, \cdots \sigma_{1,N}^2 \\ \ddots \\ \\ \ddots \\ \sigma_{N,1}^2, \sigma_{N,2}^2 \cdots \sigma_{N,N}^2 \end{bmatrix} \tag{6}$$

where $\sigma_{i,j}^2=\operatorname{Cov}\left(T_i(k), T_j(k)\right)=E\left[\widetilde{T}_{i,\text{hared }}(k)\cdot\widetilde{T}_{j,\text{ shared }}(k)\right]$, The covariance matrix gives an indication of the shared paths between the entire N nodes. You can tell how many nodes share a path. And the larger the covariance value the more shared paths there are and the more similar the paths are.

4 Topology Optimization Method Based on Delay Peak Maps

There are undetectable anonymous routers in the network [13], thus affecting the proper construction of the topology for analysis.

Definition 2. Due to the fact that the probe source does not have access to the target node, there are a large number of unidentifiable nodes in the data, which are called "anonymous routers".

Therefore, a topology optimisation method based on the delay peak graph is proposed, which focuses on the analysis of delay data under the same source and destination nodes. In this paper, three common network structures are analysed: parallel, star and interleaved structures, and the possibility of interleaved structures is derived to analyse another more complex type of structure that may arise.

The main steps are:

(A) Select the source and destination nodes.
(B) Obtain the packets sent from the selected source node to the destination node from the large amount of traffic data obtained. Since the network latency is often related to the devices passed through and also the transmission of the path, the latency of the packets arriving at the destination is counted.
(C) Based on the results of the latency statistics, the latency peak graph is analysed and can also be combined with the latency covariance matrix to make a joint path determination.

4.1 Parallel Structure

The parallel structure is one of the simplest and most common local network topologies. This structure has the same starting and destination nodes, which may pass through one or more anonymous routers in between.

Due to the existence of anonymous routers and other reasons, we cannot determine how many paths exist between A and B. In order to merge anonymous routers, identify the number of anonymous routers and obtain the real link distribution, we can use the delay distribution map to obtain the delay distribution. That is, multiple packets are sent from A to B, and the number of links is judged according to the delay distribution of the transmitted packets (assuming that the delay is different under different paths)

Optimal case: When there is only one peak in the delay distribution graph, it means that there is the simplest parallel structure between A and B, and the rest are virtual links.

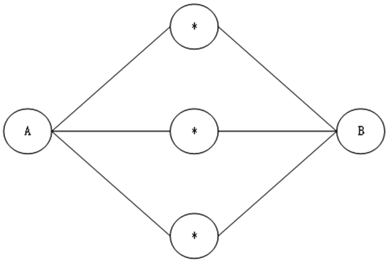


Fig. 3. Parallel structure (Complex)

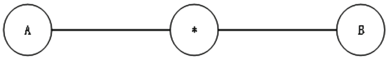


Fig. 4. Parallel structure (Simple)

4.2 Star-Shaped Structure

In a star structure, all known nodes can communicate with each other two by two and that communication passes through one or more anonymous routers, each of which is connected at both ends to a known router.

A packet is sent from A to BCD.

- A ⇒ BCD all have three peaks. Considering that the actual message will prefer the path with the shorter path length in transmission, it basically means that the link is real.
- A ⇒ B has two peaks. The specific judgment is based on the actual transmission of other nodes. It means that one of the three paths of A-¿B is a virtual path.
- Best case: A ⇒ BCD all have only one peak. Indicates that the anonymous routers marked are all the same anonymous router.

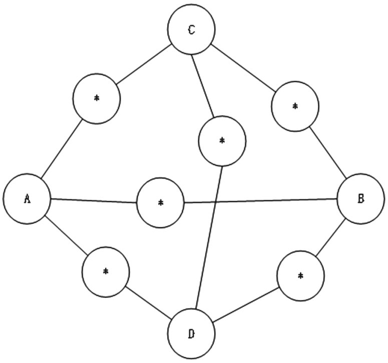


Fig. 5. Star-shaped structure (Complex)

4.3 Interlocking Structure

In an interleaved structure, the number of source and destination nodes on either side of the anonymous router is at least 2. These known nodes need to pass through at least one anonymous router to communicate with each other. Packets are sent from A and B to CDE respectively to determine the covariance matrix.

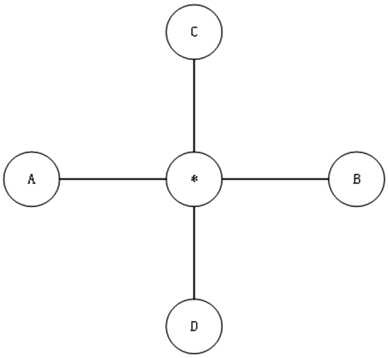


Fig. 6. Star-shaped structure (Simple)

- If $\sigma_{i,j}^2 \geq \delta, i, j = CD, CE, DE$, and send the packet with C as the source node, if $\sigma_{i,j}^2 \geq \delta, i, j = AB$,Then there is a shared path between A, B⇒ CDE. This is the simplest interleaved structure.
- If $\sigma_{i,j}^2 \leq \delta, i, j = CD, CE, DE$,Then there is not shared path between A, B ⇒ CDE. This is the complex interleaved structure.
- The cases in between are analysed on a case-by-case basis and according to the results of the time delay covariance matrix.

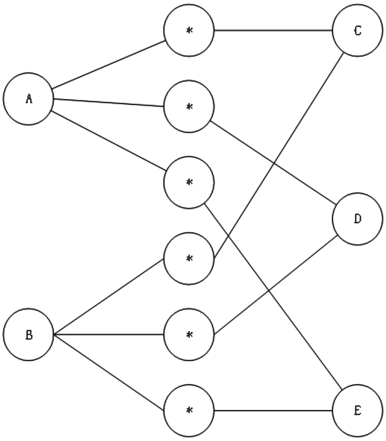


Fig. 7. Interlocking structure (Complex)

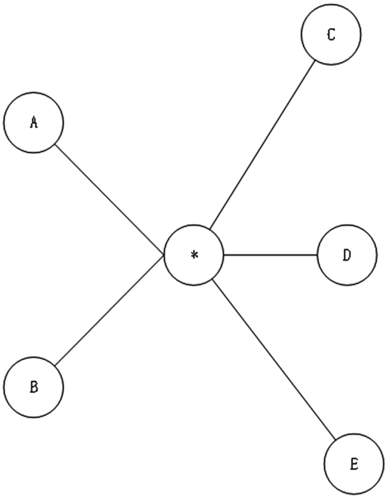


Fig. 8. Interlocking structure (Simple)

4.4 Autonomous Systems

4.5 Interlocking Structure Derivation

More complex interleaved structures may also exist in the network, again using delay covariance matrices and delay peaks to determine collaboratively.

Send a packet from A to CDE.

(A) First use the delay peak graph to initially simplify and determine how many paths each of A ⇒ CDE have (to see how many peaks there are in the delay distribution).

(B) Then use the covariance matrix to calculate the covariance of the A ⇒ C, A ⇒ D, and A ⇒ E delays respectively to determine the shared paths.

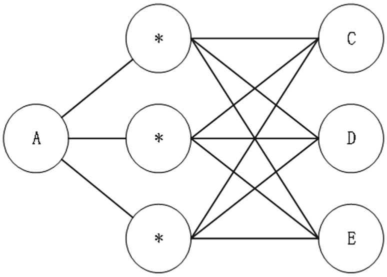


Fig. 9. Interlocking structure derivation (Complex)

The analysis of this structure is more complex and requires a combination of actual covariance matrix results and peak plot results.

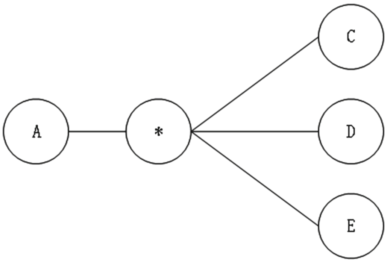


Fig. 10. Interlocking structure derivation (Simple)

5 Simulation

NS3 was used to construct the network topology, gnuplot was used to show the peak case and python was used to construct the delay covariance matrix.

5.1 Time Delay Covariance Matrix

As there may be anonymous router problems in the network, resulting in many virtual links, then it is necessary to use the delay covariance matrix + delay peak diagram to subsume the virtual links caused by the anonymous router when analysing multiple structures.

To analyse whether the delay covariance matrix reflects the similarity of links at different destination nodes of the same node, the network topology diagram is designed as shown below.

A simulated network topology is constructed using NS3 based on the designed network topology diagram. Packets are sent with R0 as the source and the rest as the destination node. Set up to execute a global routing protocol, i.e. use the Open Shortest Path First (OSPF) routing algorithm to generate a routing table for packet transmission. Set the runtime to 0s–10s and the bandwidth to the critical case of the bandwidth of each path. Set NS3 to build the simulated network with the outgoing packet simulation diagram as follows. Processing of the collected data using python:

According to the results of the calculation, the correlation between several leaf nodes (6, 8, 9, 10, 11, 12, 13, 14, 15) can be seen. It can be seen that the covariance values of 9, 10 and 11 are the closest, indicating that the shared paths for sending packets from the source node to nodes 9, 10 and 11 are the same, i.e. they can be analysed as being under the same node. Similarly, the relationships of the other nodes can be analysed and, ignoring the effect of errors, the results match the designed network topology diagram, indicating that the covariance matrix can reflect the shared paths, i.e. virtual paths caused by anonymous routers can be discovered and subsumed with the help of the covariance matrix + delay peak graph.

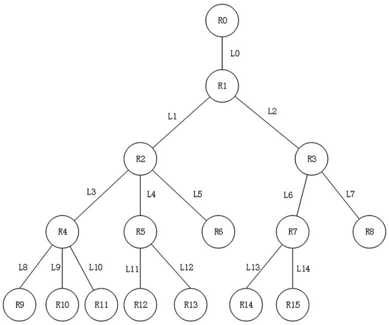


Fig. 11. The connection telationship

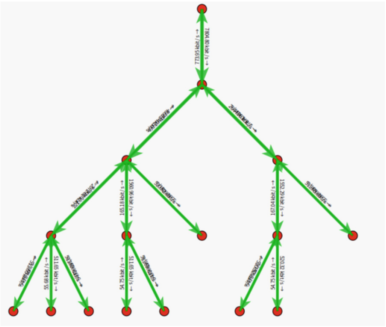
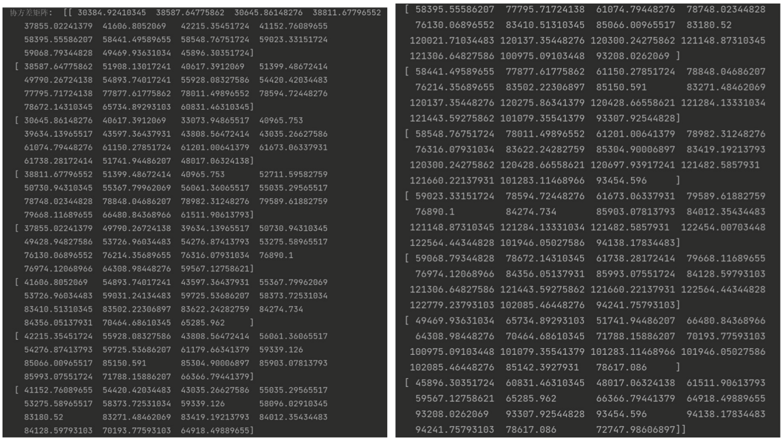


Fig. 12. Network topology simulation



```
协方差矩阵:  [[ 30384.92410345  38587.64775862  30645.86148276  38811.67796552
   37855.02241379  41606.8052069   42215.35451724  41152.76089655
   58395.55586207  58441.49589655  58548.76751724  59023.33151724
   59068.79344828  49469.93631034  45896.30351724]
 [ 38587.64775862  51908.13017241  40617.3912069   51399.48672414
   49790.26724138  54893.74017241  55928.08327586  54420.42034483
   77795.71724138  77877.61775862  78011.49896552  78594.72448276
   78672.14310345  65734.89293103  60831.46310345]
 [ 30645.86148276  40617.3912069   33073.94865517  40965.753
   39634.13965517  43597.36437931  43808.56472414  43035.26627586
   61074.79448276  61150.27851724  61201.00641379  61673.06337931
   61738.28172414  51741.94486207  48017.06324138]
 [ 38811.67796552  51399.48672414  40965.753       52711.59582759
   50730.94310345  55367.79962069  56061.36065517  55035.29565517
   78748.02344828  78848.04686207  78982.31248276  79589.61882759
   79668.11689655  66480.84368966  61511.90613793]
 [ 37855.02241379  49790.26724138  39634.13965517  50730.94310345
   49428.94827586  53726.96034483  54276.87413793  53275.58965517
   76130.06896552  76214.35689655  76316.07931034  76890.1
   76974.12068966  64308.98448276  59567.12758621]
 [ 41606.8052069   54893.74017241  43597.36437931  55367.79962069
   53726.96034483  59031.24134483  59725.53686207  58373.72531034
   83410.51310345  83502.22306897  83622.24282759  84274.734
   84356.05137931  70464.68610345  65285.962     ]
 [ 42215.35451724  55928.08327586  43808.56472414  56061.36065517
   54276.87413793  59725.53686207  61179.66341379  59339.126
   85066.00965517  85150.591       85304.90006897  85903.07813793
   85993.07551724  71788.15886207  66366.79441379]
 [ 41152.76089655  54420.42034483  43035.26627586  55035.29565517
   53275.58965517  58373.72531034  59339.126       58096.02910345
   83180.52        83271.48462069  83419.19213793  84012.35434483
   84128.59793103  70193.77593103  64918.49889655]
```

```
 [ 58395.55586207  77795.71724138  61074.79448276  78748.02344828
   76130.06896552  83410.51310345  85066.00965517  83180.52
  120021.71034483 120137.35448276 120300.24275862 121148.87310345
  121306.64827586 100975.09103448  93208.0262069 ]
 [ 58441.49589655  77877.61775862  61150.27851724  78848.04686207
   76214.35689655  83502.22306897  85150.591       83271.48462069
  120137.35448276 120275.86341379 120428.66558621 121284.13331034
  121443.59275862 101079.35541379  93307.92544828]
 [ 58548.76751724  78011.49896552  61201.00641379  78982.31248276
   76316.07931034  83622.24282759  85304.90006897  83419.19213793
  120300.24275862 120428.66558621 120697.93917241 121482.5857931
  121660.22137931 101283.11468966  93454.596     ]
 [ 59023.33151724  78594.72448276  61673.06337931  79589.61882759
   76890.1         84274.734       85903.07813793  84012.35434483
  121148.87310345 121284.13331034 121482.5857931  122454.00703448
  122564.44344828 101946.05027586  94138.17834483]
 [ 59068.79344828  78672.14310345  61738.28172414  79668.11689655
   76974.12068966  84356.05137931  85993.07551724  84128.59793103
  121306.64827586 121443.59275862 121660.22137931 122564.44344828
  122779.23793103 102085.46448276  94241.75793103]
 [ 49469.93631034  65734.89293103  51741.94486207  66480.84368966
   64308.98448276  70464.68610345  71788.15886207  70193.77593103
  100975.09103448 101079.35541379 101283.11468966 101946.05027586
  102085.46448276  85142.3927931   78617.086     ]
 [ 45896.30351724  60831.46310345  48017.06324138  61511.90613793
   59567.12758621  65285.962       66366.79441379  64918.49889655
   93208.0262069   93307.92544828  93454.596       94138.17834483
   94241.75793103  78617.086       72747.98606897]]
```

Fig. 13. Covariance matrix calculation results

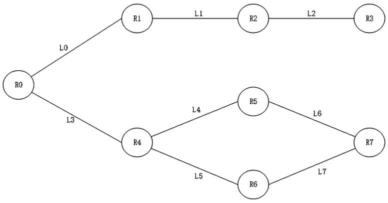


Fig. 14. The connection relationship

5.2 Delay Peaks and Paths

Build a network topology diagram with R0 as the source and R3 and R7 as the destination nodes to send packets. Set up a static route and configure the routing table so that the outgoing packet path is R0 ⇒ R1 ⇒ R2 ⇒ R3, R0 ⇒ R4 ⇒ R5 ⇒ R7, R0 ⇒ R4 ⇒ R6 ⇒ R7.

Set 0s–20s to send packets from R0 to R3 and 20s–40s to send packets from R0 to R7. To show the difference in paths, set the bandwidth to 200Kbps for L4 and L6 and 300Kbps for L5 and L7. Set NS3 to construct the simulated network with the outgoing packet simulation diagram as follows.

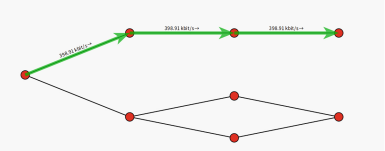


Fig. 15. 0s–20s network topology simulation

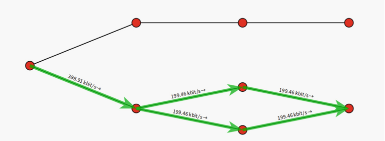


Fig. 16. 20s–40s network topology simulation

The horizontal coordinate of the first of the two sets of graphs is time (s) and the vertical coordinate is the statistical delay (ms) of packets sent from the source node to the destination node. Due to bandwidth limitations, the delay gradually increases when saturation is not reached until it reaches equilibrium, when the delay stabilises. The second horizontal coordinate is the delay (ms)

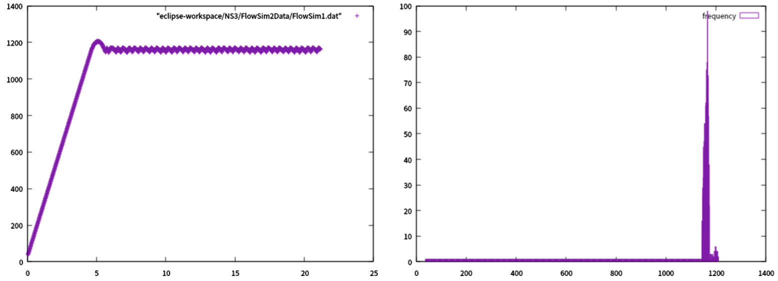


Fig. 17. 0s–20s time delay results graph

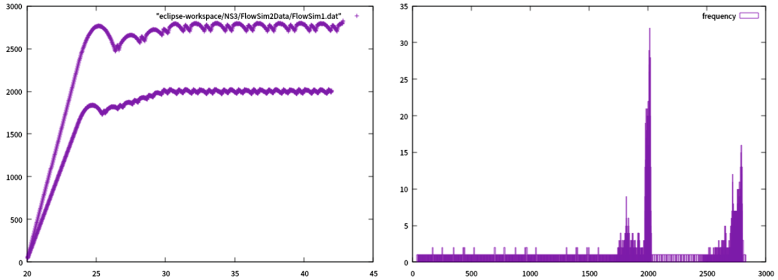


Fig. 18. 20s–40s time delay results graph

of packets sent from the source node to the destination node, and the vertical coordinate is the frequency (%). From the graph, we can see that the delay is mainly concentrated around 1200 ms when the 0s–20s tends to be stable, and the right graph shows only one peak in the delay peak graph. 20s–40s tends to be stable when the delay is mainly concentrated around 1700 and 2700 ms, and the right graph shows two peaks in the delay peak graph. This shows that using the peak delay graph can help determine the number of paths between the source and destination nodes, and the peak delay graph can assist in the merging of links.

6 Conclusion

This paper investigates the problems in network mapping for topology discovery in cloud data centres, and achieves fast topology discovery for complex and variable cloud data centres without relying on specific protocols. The topology discovery technique based on the delay covariance matrix and the topology optimization method based on the delay peak map are proposed to achieve fast topology analysis without relying on specific network protocols and without additional network load, which can propose new research ideas for the research of network topology analysis and mapping in cloud data centres.

Acknowledgments. This work was supported by National Key R&D Program of China (2020YFB1807800).

References

1. Singh, A.K., Kumar, J.: Secure and energy aware load balancing framework for cloud data centre networks. Electron. Lett. **55**(9), 540–541 (2019). https://doi.org/10.1109/LCN.2016.83
2. Donnet B, Friedman T (2007) Internet topology discovery: a survey. IEEE Commun. Surv. Tutor. 9(4):56–69; Fourth Quarter (2007). https://doi.org/10.1109/COMST.2007.4444750
3. Deng, G.C., Wang, K.C.: An Application-aware QoS Routing Algorithm for SDN-based IoT Networking. In: 2018 IEEE Symposium on Computers and Communications (ISCC), pp. 00186–00191 (2018). https://doi.org/10.1109/ISCC.2018.8538551
4. Lowekamp, B., O'Hallaron, D., Gross, T.: Topology discovery for large ethernet networks. SIGCOMM Comput. Commun. Rev. **31**(4):237–248. https://doi.org/10.1145/964723.383078
5. Lee, H., Dai, P., Wan, M., Lipatnikov, A.N.: A DNS study of extreme and leading points in lean hydrogen-air turbulent flames—part II: Local velocity field and flame topology. In: Combustion and Flame, vol. 235, pp. 111712 (2022). https://doi.org/10.1016/j.combustflame.2021.111712
6. Alharbi, T., Durando, D., Pakzad, F., Portmann, M.: Securing ARP in Software defined networks. In: 2016 IEEE 41st Conference on Local Computer Networks (LCN), pp. 523–526 (2016). https://doi.org/10.1109/LCN.2016.83
7. Donnet,B., Friedman,T., Crovella, M.: Improved algorithms for network topology discovery. In: Dovrolis, C. (eds) Passive and Active Network Measurement. PAM 2005. Lecture Notes in Computer Science, vol 3431. Springer, Berlin (2005). https://doi.org/10.1007/978-3-540-31966-5_12
8. Alhanani, R.A. Abouchabaka, J.: An overview of different techniques and algorithms for network topology discovery: the NetInventory system. In: 2014 Second World Conference on Complex Systems (WCCS), pp. 530–535 (2014). https://doi.org/10.1109/ICoCS.2014.7061004
9. Breitbart, Y., Garofalakis, M., Jai, B., Martin, C., Rastogi, R., Silberschatz, A.: Topology discovery in heterogeneous IP networks: the NetInventory system. IEEE/ACM Trans. Netw. 12(3):401–414 (2004). https://doi.org/10.1109/TNET.2004.828963
10. Wang H.: Improvement and implementation of wireless network topology system based on snmp protocol for router equipment. In: Computer Communications, vol. 151, pp. 10–18 (2020). https://doi.org/10.1016/j.comcom.2019.12.038
11. Yao, W., Chen, X.Y., Zhao, H., Zhu, J.: Multi-characteristic subnets discovery and analysis based on traceroute. J. Northeast Univ. (Natural Science) **41**(8):1075–1082 (2020). http://xuebao.neu.edu.cn/natural/EN/10.12068/j.issn.1005-3026.2020.08.003
12. Xu, X., Li, X.Y., Mao, X.F., Tang, S.J., Wang, S.G.: A delay-efficient algorithm for data aggregation in multihop wireless sensor networks. IEEE Trans Parallel Distrib Syst 22(1):163–175 (2011). https://doi.org/10.1109/TPDS.2010.80
13. Reed, M.G., Syverson, P.F., Goldschlag, D.M.: Proxies for anonymous routing. In: Proceedings 12th Annual Computer Security Applications Conference, pp. 95–104 (1996). https://doi.org/10.1109/CSAC.1996.569678

A Survey of RoCEv2 Congestion Control

Dingyu Yan[2], Yaping Liu[1,2](✉), Shuo Zhang[1,2](✉), Zhikai Yang[2], and Yingzhen Wang[3]

[1] Peng Cheng Laboratory Shenzhen, Shenzhen, China
ypliu@gzhu.edu.cn, zhangsh@pcl.ac.cn

[2] Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou, China
yandingyu134@foxmail.com, yangzhikai96@foxmail.com

[3] Faculty of Engineering, The University of Sydney, Sydney, Australia

Abstract. The traditional TCP/IP protocol stack cannot meet the high-bandwidth and low-latency requirements of data center applications for the network. Due to the kernel bypass and zero-copy features of RoCEv2 (RDMA on Converged Ethernet v2), the RoCEv2 protocol stack has been widely deployed in high-speed networks of data centers. The large-scale deployments of RoCEv2 network depends on the lossless network based on PFC (Priority Flow Control) protocol. However, PFC will lead to congestion diffusion, deadlock and other performance problems. Therefore, RoCEv2 network needs an effective congestion control mechanism to avoid network congestion to ensure high-performance transmission. This paper briefly introduces the principle of RoCEv2, the target of RoCEv2 congestion control and the problems and challenges it faces. It also classifies the congestion control protocols, analyzes the main research in the field of RoCEv2 congestion control in recent years, and finally looks forward to the development of RoCEv2 congestion control in the future, pointing out the direction for future research work.

Keywords: Data center · PFC · RoCEv2 · Congestion control

1 Introduction

With the rapid development of cloud computing and machine learning, the bandwidth of the data center network has gradually increased from 40Gbps to 100Gbps [1]. Applications (such as Storage Backup, MapReduce, etc.) require the network to have ultra-low latency while ensuring high-bandwidth [2]. The network stack has gradually become the bottleneck of application communication. TCP/IP network has gradually reached its limit in terms of both CPU utilization and network delay. Therefore, a development trend of the existing data center high-speed network is to offload the network stack to the network card hardware for processing [3]. While realizing high bandwidth and low delay of network transmission, it can also maintain low CPU utilization.

At present, most cloud providers use RDMA (Remote Direct Memory Access) to offload network stack [4]. RoCEv2 network is the main deployment form of RDMA

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 42–56, 2024.
https://doi.org/10.1007/978-981-99-7161-9_4

network, and its large-scale deployments still faces huge challenges. The reliable transmission of RDMA depends on the GBN (go-back-N) retransmission strategy. Packet loss caused by network congestion will lead to a large number of packet retransmissions, and the performance of RDMA will decline sharply. Therefore, RoCEv2 needs the lossless network based on PFC protocol [5] to ensure that there will be no packet loss caused by switch buffer overflow. However, frequent triggering of PFC will bring many serious performance problems. Therefore, many schemes deploy reliable congestion control protocols to ensure the performance of RoCEv2 network.

This paper will focus on the key issue of RoCEv2 congestion control in data center. The RoCEv2 congestion control protocol reasonably adjusts the sending rate to reduce the occurrence of network congestion while making full use of the network bandwidth. The second part introduces the main principles and challenges of RoCEv2 network and its congestion control. The third part introduces the latest research of existing RoCEv2 congestion control in detail. The fourth part will summarize the existing research mechanisms and discuss the future development trend of RoCEv2 network congestion control in data center.

2 Background

In this part, we will first introduce the definitions and related terms of RDMA and RoCEv2, then briefly describe the necessity and shortcomings of RoCEv2 network flow control, and finally analyze the mechanism and principle of RoCEv2 congestion control in detail.

2.1 RDMA and RoCEv2

RDMA supports users' direct access to remote memory [6]. Because its data access operation does not require operating system intervention, it avoids additional data copy operations, and has the characteristics of kernel bypass and zero-copy, meeting the requirements of data center applications for high throughput, low latency, and low CPU utilization.

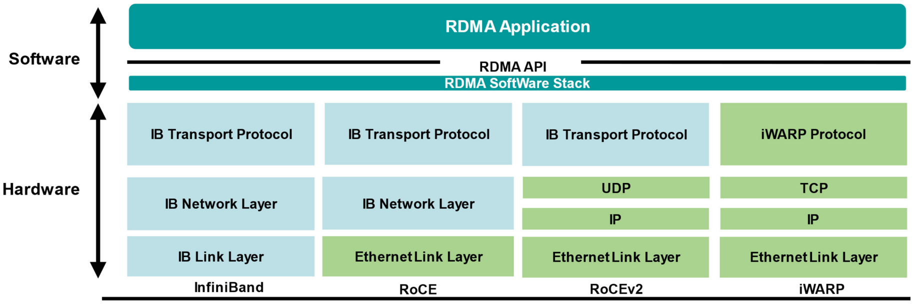


Fig. 1. RDMA network stack

As shown in Fig. 1, RDMA is originally implemented based on IB (InfiniBand) networks [6], mainly used in the field of high-performance computing (HPC) [7, 8], which requires the support of dedicated network cards and switches, and is incompatible with the traditional Ethernet-based data center network architecture. Therefore, RoCE [9], RoCEv2 [10], iWARP (Internet Wide Area RDMA Protocol) [11] have emerged, all of which are Ethernet-based RDMA technology implementations.

Among them, RoCE still needs switches and network card hardware to support IB network layer protocol, which is expensive to deploy; while iWARP provides an RDMA application interface on top of the TCP/IP protocol stack. Compared with RoCEv2 protocol, iWARP only supports reliable connection-oriented transmission, and its memory requirements are large when there are high concurrent connections [12]. RoCEv2 is the RDMA technology based on UDP/IP protocol stack. Due to its strong scalability and low implementation difficulty, RoCEv2 is widely used in the RDMA high-speed network deployment of data centers.

2.2 RoCEv2 Flow Control

Since the RoCEv2 transport layer protocol is implemented by hardware and does not support the out-of-order reception or selective retransmission of packets [6, 10], the hardware often adopts GBN retransmission strategy to solve the problem of packet disorder or packet loss [3]. However, this will lead to retransmission of a large number of packets when the network is congested, seriously reducing the goodput of RoCEv2. Therefore, the high-performance transmission of RoCEv2 requires high reliability of the network. IB network uses a credit-based hop-by-hop flow control mechanism to prevent packet loss caused by switch buffer overflow; however, traditional Ethernet cannot provide the reliability guarantee required by RDMA. Therefore, RoCEv2 uses PFC protocol to provide approximate lossless Ethernet.

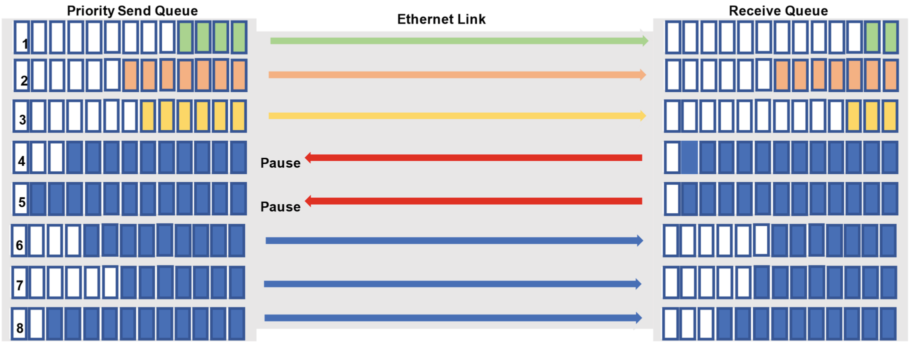


Fig. 2. Priority based flow control.

As shown in Fig. 2, PFC divides the physical link into eight virtual channels, and each channel represents a priority. The device can send Pause or Resume frames to upstream devices (switches or NICs) according to the congestion conditions of the priority channels to suspend or resume data transmission of the designated priority channels, while ensuring data transmission of other priority channels. Since the PFC protocol is a coarse-grained flow control at the port level, while ensuring the lossless Ethernet, frequent PFC triggering will cause various performance problems such as HOL (head-of-line) blocking, deadlock and congestion-spreading [1]. At present, RoCEv2 network mainly solves the performance problems caused by PFC through flow level congestion control schemes [3].

2.3 RoCEv2 Congestion Control

The targets of RoCEv2 network congestion control [13] is: (1) Reduce the flow completion time (FCT); (2) Reduce the triggering of PFC; (3) Prevent deadlock. This requires that the congestion control mechanism can meet the four requirements of high bandwidth utilization, fairness, stability and fast convergence. Fairness requires that multiple flows can share congestion link bandwidth fairly; high bandwidth utilization requires traffic to make full use of bandwidth; fast convergence requires that the congestion flow rate can quickly adjust the set fair rate; stability requires that the congestion control mechanism can still guarantee good performance under network fluctuation. Finally, the route deadlock caused by PFC can be effectively reduced by reducing the triggering of FCT and PFC.

The RoCEv2 specification [10] and Data Center Bridging (DCB) Task Group [14] specify the RoCEv2 congestion control Management, that is, the switch detects congestion, the receiver generates congestion notification packets (CNP), and the sender adjusts the rate. The subsequent research work abstracts the RoCEv2 network congestion control framework into RP (reaction point), CP (congestion point), NP (notification point) [1], which correspond to the sender, switch, and receiver respectively. Each RoCEv2 congestion control mechanism operates on the three parties, mainly including two parts: (1) congestion signal, and (2) rate adjustment strategies.

Congestion Signal. Congestion signal refers to the standard by which the congestion mechanism measures the occurrence of network congestion. The selection of congestion signal affects the convergence and stability of the sending rate. The types of congestion signals are mainly divided into two categories: direct congestion signals and indirect congestion signals [15]. The direct congestion signal usually reflects the absolute state change of the network, including the switch queue-length, RTT (Round Trip Time), and ECN (Explicit Congestion Notification) [16] signal. With the continuous development of network in-band detection technology, the INT (in Band Network Telemetry) [17] information also develops into a direct congestion signal. The indirect congestion signal reflects the change trend of network congestion, such as RTT gradient and queue length gradient. Some congestion control mechanisms will combine a variety of congestion signals to detect network conditions, Such as composite congestion signals combining ECN and RTT. There are also some congestion control protocols that use custom congestion signals, such as special FRP (Flow Rate Packet) [18], etc.

Rate Adjustment Strategies. Rate adjustment refers to that the congestion control mechanism adjusts the sending rate according to different strategies and the congestion degree of the current network to make it converge quickly and stably. The choice of strategy also affects the convergence and stability of congestion control protocol. Common rate adjustment strategies mainly include heuristic AIMD (Additive Increase Multiple Decrease) [19], that is, when the network is congested, the sending rate is reduced by product, usually to half of the original rate; when the network is not congested, the addative increase the sending rate to gradually approach the fair rate.

With the development of congestion signals, rate adjustment strategies become more accurate. We classify these strategies as accurate rate adjustment strategies. Different precise congestion control mechanisms adopt different accurate rate adjustment strategies. Some mechanisms calculate the fair rate of bottleneck links in the network and adjust the sending rate based on precise INT information or queue information [4, [13]; others adjust the sending rate based on the receiving rate of the NP [20]. The accurate rate adjustment strategy is often faster than AIMD in convergence, but it often requires more complex congestion signals to detect network congestion.

3 RoCEv2 Congestion Control Schemes

In this part, we will classify RoCEv2 congestion control schemes and briefly analyze their principles. As shown in Fig. 3, according to the entities that play the key role in congestion control [13], we roughly divide the RoCEv2 congestion control schemes into sender-driven, switch-driven, and receiver-driven; we will also mention some RoCEv2 improvement schemes that do not apply to this classification method.

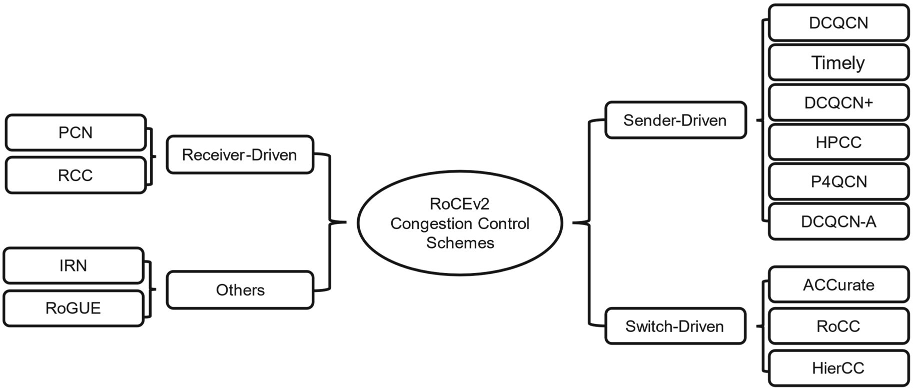


Fig. 3. Classification of RoCEv2 congestion control schemes

3.1 Sender-Driven Congestion Control Schemes

DCQCN. DCQCN [1] is the first end-to-end congestion control protocol with high practicability in RoCEv2 network. It uses ECN as the congestion signal, combines the rate adjustment ideas of DCTCP [21] and QCN [22], and adopts the heuristic AIMD rate adjustment strategy.

Its mechanism consists of three parts. The CP algorithm deployed in the switch performs the congestion marking based on RED-ECN [16, 23]. When the queue length of the switch exceeds the specified threshold, the RoCEv2 packet is marked with ECN to explacidly notify the sender and receiver of congestion in the network. The NP algorithm deployed in the receiver will generate a special CNP for the flow whenever it receives a packet with ECN-marked and send it to the sender RP at a higher priority to inform it that there is congestion in the network.

The RP algorithm deployed on the sender adjusts the sending rate of each flow. Whenever a CNP is received, it is considered that there is congestion on the corresponding flow path, and the sending rate is reduced according to Eq. (1), where Rc indicates the current sending rate of the flow, Rt stores the rate before the last speed reduction for rate recovery, congestion parameter α indicates the current network congestion level, g is the constant value.

$$\begin{aligned} Rt &= Rc, \\ Rc &= Rc \cdot 1 - \frac{\alpha}{2}, \\ \alpha &= (1-g)\cdot\alpha + g \end{aligned} \tag{1}$$

If CNP is not received for a period of time, it is considered that the congestion on the flow path is relieved, and the α is updated according to Eq. (2).

$$c\alpha = (1-g)\cdot\alpha \tag{2}$$

DCQCN introduces a byte counter and a timer to judge the growth stage in the rate increase. The byte counter increases the rate every time B bytes of data are sent, and the timer increases the rate every T unit time. The rate increase phase is judged by these two parameters. The rate increase is mainly divided into fast recovery phases and additive increase phases; the former increases the rate according to Eq. (3),

$$Rc = \frac{(Rt + Rc)}{2} \tag{3}$$

and the latter increases the rate according to Eq. (4), where Rai is a fixed additive increase factor.

$$Rt = Rt + Rai$$

$$Rc = \frac{(Rt + Rc)}{2} \tag{4}$$

There is also a hyper increase phase, and the growth rate is even faster. See [1] for more details.

DCQCN can effectively solve the performance problems such as congestion diffusion and unfairness caused by PFC. It has high practical value and has been deployed on commercial network cards [24]. However, because it contains multiple thresholds and parameters, the optimal parameter configuration of each network is different, and the actual configuration is more complex.

Timely. Timely [25] uses *RTT* and its gradient as congestion signal, and adopts AIMD strategy for rate adjustment. It is mainly deployed on the network card and does not depend on the additional hardware support of the switch in the network (Such as ECN Marking). Each time an ACK is received, Timely needs to calculate the corresponding *RTT* and the Gradient RTT_{grad} with the last RTT, then make a rate adjustment.

It uses two thresholds T_{low} and T_{high} detects that the bandwidth utilization is insufficient or the delay is too high. At this time, the sending rate is updated according to Eq. (5) to keep the measured *RTT* between T_{low} and T_{high}, where σ is the additive increasing parameter, and β is the multiplicative decreasing parameter.

$$Rc = Rc + \sigma \; if \; RTT \; < T_{low}$$

$$Rc = Rc \cdot \left[1 - \beta \cdot \left(1 - \frac{T_{high}}{RTT}\right)\right] if \; RTT \; > T_{high} \tag{5}$$

When the *RTT* is within the normal range, it adjusts the sending rate based on the *RTT* gradient. When the gradient is greater than zero, the network congestion increases and the sending rate increases; when the gradient is less than zero, the network congestion is relieved and the sending rate is reduced, as shown in Eq. (6), where N represents the rate increase phase.

$$\begin{array}{ll} Rc = Rc \cdot \left[1 - \beta \cdot \left(1 - RTT_{grad}\right)\right] & if \;\; RTT_{grad} \; > 0 \\ Rc = Rc + N \cdot \sigma \quad if \;\; RTT_{grad} \leq 0 & \end{array} \tag{6}$$

The advantage of Timely is that it responds quickly to network congestion, does not require switch hardware support, and is easy to deploy. However, previous work [26] has proved that it has no fixed rate convergence point, so it is rarely used in actual deployment.

DCQCN +. DCQCN + [27] is an improved protocol based on DCQCN, which is also based on ECN congestion signal and adopts AIMD rate adjustment strategy. It mainly aims at the shortcomings of DCQCN's fixed period and increment when increasing sending rating, and uses adaptive parameters to improve it. For large-scale incast, it adopts the growth strategy of long period and small increment; for small incast, the growth strategy is obtained by adopting short cycle and large increment.

It believes that the ability of the receiver to generate CNP is limited by the hardware when there are high concurrent connections, and the actual CNP generation cycle will increase. Therefore, it uses the method of dynamic CNP cycle to dynamically calculate the actual generation cycle of CNP at the receiver, piggybacks it in the CNP packet. When the sender receives the CNP, it dynamically adjusts each timer period and rate increment. The performance of DCQCN + is similar to that of DCQCN when it is used for small-scale incast, and it has the ability to handle large-scale incast.

HPCC. HPCC [4] is a congestion control strategy that uses INT information as congestion signal and adopts the accurate rate regulation strategy. It believes that the two-bit coarse-grained ECN information cannot reflect accurate link load information, so it uses INT information as the congestion signal. As shown in Fig. 4, when forwarding packets, the switch will add INT metadata information of the egress port to the packets, including bandwidth B, timestamp Ts, egress accumulated bytes txbytes, queue length qlen and other information. When the receiver generates the ACK, the INT information in the packet is piggybacked in the ACK.

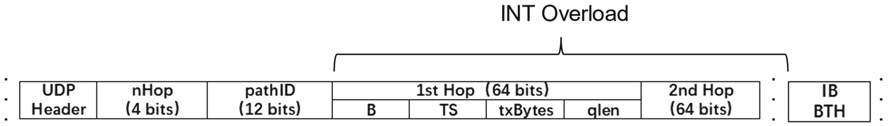


Fig. 4. The format of HPCC packet

Whenever the sender receives a new ACK, it will calculate the bandwidth utilization U of the most congested port in the link based on the INT information, and use this bandwidth utilization to accurately adjust the sending rate. Compared with other protocols, HPCC uses a rate adjustment strategy based on the window to limit the inflight bytes of the sender to prevent congestion.

HPCC's accurate rate adjustment strategy includes multiplicative increase/decrease (MI/MD) and additive increase (AI). Specifically, when the bandwidth utilization ratio U of the most congested port in the network is lower than the threshold η, it uses Eq. (7) to additive increase the rate, where W_c is the size of the sending window and W_{AI} is the additive increment parameter.

$$W_c = W_c + W_{AI} \tag{7}$$

When the bandwidth utilization ratio U of the most congested port in the network is higher than the threshold η or after several cycles of additive increase, it adjusts the sending window based on the U according to Eq. (8).

$$W_c = \frac{W_c}{U/\eta} + W_{AI} \tag{8}$$

HPCC responds quickly to network congestion and can make the bandwidth allocation converge to Pareto optimality within 1 RTT. However, it requires the switch to support the INT protocol, and because the part of the bandwidth is reserved for burst traffic, it cannot make full use of the link bandwidth.

P4QCN. P4QCN [28] is the L3 extension protocol of QCN (Quantified Congestion Notification). It uses queue length as congestion signal and AIMD strategy for rate adjustment. It periodically detects the queue length at the switch. When the queue length exceeds the specified threshold range, It generates a FBP (Feedback Packet) for the specified flow with a certain probability. When the sender receives the FBP, it adopts the same rate adjustment strategy as QCN. See [22] for more details. P4QCN directly detects queue congestion at the switch and responds more quickly to network congestion, but it relies on P4 programmable switches to implement special hardware logic.

DCQCN-A. DCQCN-A [29] is also an improved protocol based on DCQCN. It uses the composite congestion signal composed of ECN and RTT, Introduces the reference rate based on RTT in the rate adjustment phase, and Adopts the AIMD Rate Adjustment Strategy with Dynamic Increments.

It refers to the idea of NUM [30] and Copa algorithm [31], and believes that the fair rate R_{ref} in the network is related to the RTT gradient, and the fair rate is calculated according to Eq. (9), where d_q is the gradient of queuing delay, δ is the weight factor. When the sending rate is much higher than the fair rate, a smaller increment is adopted; on the contrary, a larger increment is used.

$$R_{ref} = \frac{1}{\delta \times d_q} \tag{9}$$

DCQCN-A performs better than DCQCN when dealing with large incast, and it can also maintain nearly zero queues, with better fairness and convergence.

As shown in Table 1, this section briefly describes several different schemes of RoCEv2 congestion control based on sender-driven, and briefly analyzes their advantages and disadvantages.

Table 1. Comparison of sender-driven RoCEv2 congestion control protocols

Schemes	Congestion signal	Rate adjustment strategy	Switch HW support
DCQCN [1]	ECN	AIMD	PFC, RED-ECN
Timely [25]	RTT	AIMD	None
DCQCN + [27]	ECN	AIMD	PFC, RED-ECN
HPCC [4]	INT	MI/AI, MD	PFC, INT
P4QCN [28]	Queue length	AIMD	P4
DCQCN-A [29]	ECN and RTT	AIMD	PFC, RED-ECN

3.2 Switch-Driven Congestion Control Schemes

RoCC. RoCC [13] uses the queue length as the congestion signal, and adopts the rate adjustment strategy of multiplicative increase and direct rate decrease. Specifically, as shown in Fig. 5, RoCC periodically samples the egress queue length Q_{cur} on the switch, and calculate the fair rate F according to Eq. (10), where α and β are adjustment parameters, Q_{ref} is the expected stable queue length, Q_{old} is the queue length at the time of last sampling. The fair rate calculation follows the Proportional Integral (PI) Control method [32], and the switch will generate the CNP containing the fair rate to directly control the rate reduction of the sender.

$$F = F - \alpha \cdot Q_{cur} \;-\; Q_{ref} - \beta \cdot Q_{cur} \;- Q_{old} \tag{10}$$

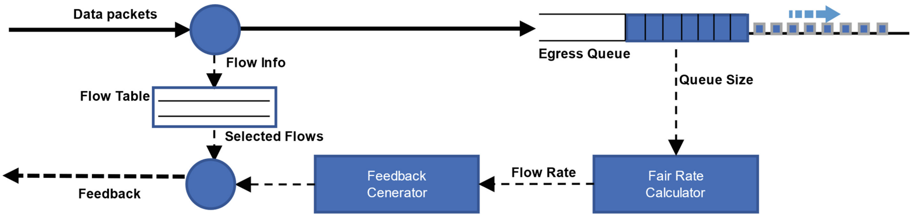


Fig. 5. RoCC CP algorithm

After receiving the CNP, the sender directly reduces the sending rate to the fair rate of the most congested port, that is, the minimum fair rate. When the CNP is not received for a period of time, the transmission rate is multiplied by Eq. (11), where R_{cur} is the current sending rate, R_{max} is the maximum rate of flow.

$$R_{cur} = R_{cur} \times 2ifR_{cur} < R_{max} \tag{11}$$

The advantage of RoCC is that it responds quickly the network congestion, and the method of multiplicative rate increasing and fair rate direct decreasing makes the sending rate converge rapidly. Since RoCC is directly deployed in the switch, it does not rely on PFC to ensure reliable transmission of RoCEv2.

HierCC. HierCC [33] is a hierarchical RoCEv2 congestion control mechanism, which uses virtual queue length as the congestion signal and adopts the rate adjustment strategy of direct rate control. It divides congestion into two types: the congestion between ToR and NICs, and the congestion between ToR. For the former, there are multiple virtual queues in each ToR, and each virtual queue caches all packets sent to the same server. The ToR periodically calculates the fair rate of each virtual queue, and directly controls the sending rate through the fair rate packets. For the latter, it adopts a credit-based flow control mechanism, and the virtual queue at the receiver sends credits periodically to the virtual queue at the sender, so as to prevent congestion in the network. HierCC uses a short control loop to quickly control network congestion, and uses directly rate allocation to adjust the sending rate, which can effectively limit the queue length and achieve rapid rate convergence.

ACCurate. ACCurate [18] uses FRP (Flow Rate Packet) as congestion information and adopts the rate adjustment strategy of direct rate allocation. It requires each sender to periodically inject FRP (Flow Rate Packet) for all active RDMA channels; when the switch detects FRP, it allocates the minimum rate of the flow according to the number of flows on the egress port. The receiver sends the FRP back to the sender, and the sender directly adjusts the sending rate according to the minimum rate. ACCurate can quickly respond to network congestion, throttles the offensive flows, and reduce the flow completion time by an order of magnitude.

As shown in Table 2, this section briefly describes several switch-driven RoCEv2 congestion control protocols. Because they directly detect network congestion at the switch, they can quickly respond to network congestion, but they often need customized hardware support from the switch (Table 3).

Table 2. Comparison of switch-driven RoCEv2 congestion control protocols

Schemes	Congestion signal	Rate adjustment strategy	Switch HW support
RoCC [13]	Queue length	MI/ Direct rate decrease	Customized hardware
HierCC [33]	Virtual queue length	Direct rate Allocation	Customized hardware
ACCurate [18]	FRP	Direct rate Allocation	Customized hardware

Table 3. Comparison of receiver-driven RoCEv2 congestion control protocols

Schemes	Congestion signal	Rate adjustment strategy	Switch HW support
PCN [20]	ECN	AI/ Receiving Rate Decrease	PFC, NP-ECN
RCC [34]	One-way delay	Direct Rate Allocation/ PID	PFC

3.3 Receiver-Driven Congestion Control Schemes

PCN. PCN [20] uses ECN as the congestion signal, and adopts the rate adjustment strategy of additive increase and direct deceleration based on the receiving rate. PCN believes that the existing RED-ECN marking method cannot correctly identify congested flows due to the impact of PFC protocol. Therefore, they propose the NP-ECN marking method, which can guarantee the throughput of non-congested flows while maintaining zero queues. PCN also requires the receiver to periodically unify the receiving rate of each flow, and generate a deceleration CNP or an acceleration CNP According to the proportion of packets with ECN-marked received. The receiver actively controls the rate adjustment of the sender. When the sender receives the deceleration cnp, the sender will extract the receiving rate *RecRate* contained in the CNP, reduce the sending rate according to Eq. (12) and reduce the value of W, Where *Rc* represents the current sending rate; *w* represents the rate increase weight, $w \in [w_{\min}, w_{\max}]$.

$$\begin{aligned} Rc &= \min\{Rc, \mathrm{Re}c\, Rate\ 1 - w_{\min}\} \\ w &= w_{min} \end{aligned} \tag{12}$$

When the sender receives the acceleration CNP, it will adopt a dynamic increment strategy based on the network card bandwidth *B*, increase the sending rate according to Eq. (13), and gradually increase the value of w.

$$\begin{aligned} Rc &= Rc \cdot 1 - w + B \cdot w_{max} \\ w &= w \cdot 1 - w + w_{max} \cdot w \end{aligned} \tag{13}$$

PCN can identify which flows are actually congested through the NP-ECN marking method, and its receiver-driven rate adjustment strategy can alleviate network congestion in a RTT as soon as possible.

RCC. RCC [34] uses one-way delay as congestion signal, and adopts the rate adjustment strategy combining direct rate adjustment and PID (Proportional Integral Derivative) adjustment. It divides the network congestion into two categories according to the spatial distribution: In-network congestion and last-hop congestion. For the former, the receiver directly calculates the fair rate window according to the number of flows sharing the receiving port, and piggybacks it in the ACK to directly control the size of the sending window; for the latter, RCC continuously adjusts the size of the sending window based on the PID adjustment strategy [32], so that the measured one-way delay matches the target one-way delay. RCC can effectively use the network bandwidth, while ensuring that the queue length is close to 0.

3.4 Other Schemes

IRN. IRN [35] can use ECN or RTT as congestion signal and adopt the rate adjustment strategy of AIMD. Its improvement on RoCEv2 transmission mechanism mainly includes two aspects: (1) implementing the SACK-based SR (Selective Retransmission) mechanism; (2) The End-To-End flow control mechanism—BDP flow control is implemented; by modifying RoCEv2 transmission mechanism, IRN can deploy RoCEv2 network on lossy ethernet and is compatible with other existing congestion control protocols.

RoGUE. RoGUE [36] Uses RTT as the congestion signal and adopts the rate adjustment strategy of AIMD. It adds a RoGUE software layer between the RDMA API and RDMA Application. Through this software layer, data operations are segmented and converted into multiple small-segment data operations. RoGUE performs congestion control and packet loss recovery based on these small-segment data. RoGUE does not require PFC, and its congestion control is implemented in software without the support of network card hardware.

As shown in Table 4, we classify the existing main RoCEv2 congestion control protocols according to the entity objects that play a key role, and briefly analyze the protocols from three aspects: congestion signal, rate adjustment strategy and switch hardware support.

4 Conclusion

In this paper, we classify and summarize the existing RoCEv2 congestion control protocols, and briefly describe each protocol from two aspects: congestion signal and rate adjustment strategy. When designing the RoCEv2 congestion control schemes, we should not only consider the fairness, stability and convergence of the schemes to reduce the flow completion time and PFC triggering; but also consider the reliability and complexity of the congestion signal, and the trade-off between performance and hardware cost should be made. With the continuous development of high-speed network in the data center, receiver-driven congestion control has a good performance in terms of hardware cost and the accuracy of congestion signals, which is one of the main development directions of RoCEv2 congestion control in the future.

Table 4. Comparison of RoCEv2 congestion control protocols

Category	Schemes	Congestion signal	Rate adjustment strategy	Switch HW support
Sender-Driven	DCQCN [1]	ECN	AIMD	PFC, RED-ECN
	Timely [25]	RTT	AIMD	None
	DCQCN + [27]	ECN	AIMD	PFC, RED-ECN
	HPCC [4]	INT	MI/AI, MD	PFC, INT
	P4QCN [28]	Queue Length	AIMD	P4
	DCQCN-A [29]	ECN and RTT	AIMD	PFC, RED-ECN
Switch-Driven	RoCC [13]	Queue Length	MI/ Direct Rate Decrease	Customized hardware
	HierCC [33]	Virtual Queue Length	Direct Rate Allocation	Customized hardware
	ACCurate [18]	FRP	Direct Rate Allocation	Customized hardware
Receiver-Driven	PCN [20]	ECN	AI/ Receiving Rate Decrease	PFC, NP-ECN
	RCC [34]	One-way delay	Direct Rate Allocation/ PID	PFC
Others	IRN [35]	ECN or RTT	AIMD	None
	RoGUE [36]	RTT	AIMD	None

Funding Statement. This work was supported by The Major Key Project of PCL (Grant No.PCL2022A03, PCL2021A02, PCL2021A09).

References

1. Zhu, Y. et al.: Congestion control for large-scale RDMA deployments. ACM SIGCOMM Comput Commun Review **45**(4), 523–536 (2015)
2. Benson, T., Akella, A., Maltz, D.A.: Network traffic characteristics of data centers in the wild. In:Proceedings of the 10th ACM SIGCOMM conference on Internet measurement, (2010)
3. Guo, C et al.: RDMA over commodity ethernet at scale. In: Proceedings of the 2016 ACM SIGCOMM conference, (2016)
4. Li, Y et al.: HPCC: High precision congestion control. In: Proceedings of the ACM special interest group on data communication, pp. 44–58 (2019)
5. IEEE DCB. 802.1Qbb—Priority-based flow control. http://www:ieee802:org/1/pages/802:1bb:html
6. Infiniband Trade Association.: InfiniBand architecture specification vol. 1 Release 1.3,2015
7. Woodall, T.S. et al.: High performance RDMA protocols in HPC. In: European parallel virtual machine/message passing interface users' group meeting. Springer, Berlin, Heidelberg, (2006)

8. Wasi-ur-Rahman, M et al.: High-performance design of YARN MapReduce on modern HPC clusters with Lustre and RDMA. In: 2015 IEEE International parallel and distributed processing symposium. IEEE, (2015)
9. Infiniband Trade Association.: Supplement to InfiniBand architecture specification vol. 1 Release 1.2.1, Annex A16: RDMA over Converged Ethernet (RoCE), (2010)
10. Infiniband Trade Association.: Supplement to InfiniBand architecture specification vol. 1 Release 1.2.1, Annex A17: RoCEv2,2014
11. RDMA Consortium. [online] Available http://www.rdmaconsortium.org
12. Rashti, M.J. et al.: iWARP redefined: Scalable connectionless communication over high-speed Ethernet. In: 2010 International conference on high performance computing. IEEE, (2010)
13. Taheri, P et al.: RoCC: robust congestion control for RDMA. In: Proceedings of the 16th International conference on emerging networking experiments and technologies, (2020)
14. IEEE 802.1 Qau - Congestion Notification. http://www.ieee802.org/1/pages/802.1au.html,2010
15. Addanki, V., Michel, O., Schmid, S.: {PowerTCP}: Pushing the performance limits of datacenter networks. In: 19th USENIX symposium on networked systems design and implementation (NSDI 22), (2022)
16. Ramakrishnan, K., Floyd, S., Black, D.: Rfc3168: The addition of explicit congestion notification (ecn) to ip[J]. (2001)
17. In-band Network Telemetry. https://p4.org/p4-spec/docs/INT_v2_1.pdf
18. Giannopoulos, D et al.: Accurate congestion control for RDMA transfers. In: 2018 Twelfth IEEE/ACM international symposium on networks-on-chip (NOCS). IEEE, (2018)
19. Yang, Y.R., Lam, S.S.: General AIMD congestion control. In: Proceedings 2000 International conference on network protocols. IEEE, (2000)
20. Cheng, W et al.: Re-architecting congestion management in lossless ethernet. NSDI., (2020)
21. Alizadeh, M et al.: Data center tcp (dctcp). In: Proceedings of the ACM SIGCOMM 2010 conference, (2010)
22. IEEE. 802.11Qau. Congestion Notification. 2010. Available online https://1.ieee802.org/dcb/802-1qau/
23. Floyd, S., Jacobson, V.: Random early detection gateways for congestion avoidance. IEEE/ACM Trans. Networking **1**(4), 397–413 (1993)
24. ConnectX-6 Dx Product Brief. https://www.nvidia.com/en-us/networking/ethernet/connectx-6-dx/
25. Mittal, R et al.: TIMELY: RTT-based congestion control for the datacenter. ACM SIGCOMM Comput. Commun. Rev. **45**(4), 537–550 (2015)
26. Zhu, Y et al.: ECN or Delay: Lessons learnt from analysis of DCQCN and TIMELY. In: Proceedings of the 12th international on conference on emerging networking experiments and technologies, (2016)
27. Gao, Y et al.: Dcqcn+: Taming large-scale incast congestion in rdma over ethernet networks. In: 2018 IEEE 26th International conference on network protocols (ICNP). IEEE, (2018)
28. Geng, J., Yan, J., Zhang, Y.: P4QCN: Congestion control using P4-capable device in data center networks. Electronics **8**(3), 280 (2019)
29. Hu, Y, et al.: DCQCN Advanced (DCQCN-A): Combining ECN and RTT for RDMA congestion control. In: 2021 IEEE 5th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), vol. 5. IEEE, (2021)
30. Kelly, F.P., Maulloo, A.K., Tan, D.K.H.: Rate control for communication networks: shadow prices, proportional fairness and stability. J. Oper. Res. Soc. **49**(3), 237–252 (1998)
31. Arun, V., Balakrishnan, H.: Copa: Practical {Delay-Based} congestion control for the internet. In:15th USENIX symposium on networked systems design and implementation (NSDI 18), (2018)

32. Pan, R. et al.: PIE: A lightweight control scheme to address the bufferbloat problem. In: 2013 IEEE 14th international conference on high performance switching and routing (HPSR). IEEE, (2013)
33. Zhang, J. et al.: HierCC: Hierarchical RDMA congestion control. In: 5th Asia-Pacific Workshop on Networking (APNet 2021), (2021)
34. Zhang, J. et al.:Receiver-Driven RDMA congestion control by differentiating congestion types in datacenter networks. In: 2021 IEEE 29th International conference on network protocols (ICNP). IEEE, (2021)
35. Mittal, R., et al.: Revisiting network support for RDMA. In: Proceedings of the 2018 Conference of the ACM special interest group on data communication, (2018)
36. Le, Y., et al.: (2018) Rogue: Rdma over generic unconverged ethernet. In: Proceedings of the ACM symposium on cloud computing, (2018)

Network Device Identification Scheme Based on Network Traffic Analysis

Miaomiao Wang[1](✉), Junyan Rui[2], Huibo Niu[3], Yuan Chang[3], and Siwen Xu[4]

[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
wangmiaomiao@bupt.edu.cn

[2] College of Computer Science and Technology, Anhui University, Anhui, China
347663416@qq.com

[3] China Aerospace Science andIndustry Network Information Development Co., Ltd., Beijing, China
632965725@qq.com, zzuchangyuan@163.com

[4] Université Paul Sabatier-Toulouse, Toulouse, France

Abstract. Network device identification is the basis of building network topology, which is the premise of preventing malicious attacks. It is of great significance to propose an efficient network device identification scheme. Existing physical device identification technologies are mainly oriented to Internet of Things devices and wireless devices. They collect network element information through active detection, which consumes extra network traffic and increases the risk of detection behavior identification. Identifying devices by protocol analysis or fingerprint matching has become the mainstream, but most of these solutions are based on a certain protocol, which is difficult to apply to the complex network of multi-protocol cloud data center. At present, there is no network device identification scheme for cloud data center network traffic analysis. Therefore, we propose a network device identification scheme based on network traffic analysis, which collects network traffic passively, selects network traffic characteristics automatically, and uses decision tree algorithm to realize network device identification. Finally, the accuracy of the proposed scheme is verified by the simulation, and the results show that the accuracy of the scheme is to 96%.

Keywords: Cloud data center · Network traffic analysis · Network device identification · Decision tree

1 Introduction

With the continuous development of network technology, the network structure of cloud data center has become more and more huge, and the network forms are also diverse. In recent years, mainstream cloud data center networks have obvious topological characteristics, such as Google Fat Tree, Dcell, Bcube, Facebook Fat Tree. They are a complex network composed of large-scale, multi-vendor

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 57–67, 2024.
https://doi.org/10.1007/978-981-99-7161-9_5

computing, storage, and network device through a variety of network protocols, such as OSPF, BGP, ISIS, Vxlan tunnel. Cloud data center network topology identification is conducive to building a network center panorama and defending against network attacks. Network topology identification is based on the identification of network devices. Therefore, it is urgent to propose an efficient network device identification technology for cloud data center network.

Device identification methods are divided into active and passive methods. Among them, the active method is to actively send detection packets to all management networks through the network management workstation, collect the information returned by each network element, and finally analyze to identify the network devices. In the passive method, a probe is deployed on the observed network. The probe collects network element information and sends it to a workstation to analyze and identify network devices on the workstation. In this way, the network and devices are not greatly affected.

In the research of network device identification, scholars [1–3] have proposed a variety of IoT device identification schemes, but most of these schemes are based on a single protocol, such as SNMP protocol, HTTP protocol or TCP protocol, which is difficult to apply to the complex network of multi-protocol cloud data center. Some schemes obtain data packets through active detection for analysis and identification, which requires additional network traffic and increases the risk of detection behavior being found. Some scholars [4,5] have proposed a convolutional neural network (CNN) recognition scheme for wireless devices. The network device involved in this paper refers to the device in the cloud data center network, including Modem, Firewall, Switches, Routers, Web Server, etc. They differ greatly from IoT devices and wireless devices in attributes, usage methods and scenarios, and network traffic generated during the use of devices. In terms of attributes, network devices such as switches and routers have specific ports, which are different from IoT devices such as smart speakers and intelligent sweeping robots. In terms of usage methods, network devices connect various devices through the transmission and analysis of data packets, IoT devices use sensors to collect data, usually transmit data through wireless networks, and wireless devices send and receive data through radio frequency signals. In terms of scenarios, network devices are mostly used in data center networks, while IoT devices are usually used in smart home and industrial Internet of Things, which are assisted by wireless devices. Therefore, existing identification schemes for IoT devices and wireless devices are difficult to apply to network device identification.

This paper proposes a protocol independent device identification scheme for the cloud data center network devices. This scheme passively collects network traffic by deploying probes, selects and analyzes the characteristics of network traffic data, and then the classification learning is carried out by the decision tree algorithm. Finally, the learned model is applied to the new cloud data center network data to identify network devices.

The main contributions of this paper are as follows:

1. This paper proposes a network device identification framework based on network traffic, which passively collects device network traffic through probes, analyzes network traffic and identifies network devices, not limited to one or two network protocols or data packets.
2. A network device identification scheme for network traffic analysis is proposed. This scheme filters irrelevant features, uses RFECV for feature selection, and obtains a identification model suitable for network devices through identification learning.
3. The simulations are carried out, and the results show that our device identification scheme has a high accuracy.

The rest of this paper is organized as follows: Sect. 2 reviews the related works. In Sect. 3, we propose the network device identification framework. Section 4 describes the network device identification scheme. In Sect. 5, experiments are conducted to demonstrate the effectiveness of our scheme. Section 6 concludes this article.

2 Related Works

Focusing on the requirements of device identification in cyberspace security or network management, many scholars have conducted in-depth research on physical device identification methods.

Imamura et al. [6] proposed a comprehensive scheme, which learned from the idea of random forest, analyzed the results of various identification methods, and improved the accuracy by combining the results of various identification methods through clustering, weight setting and other methods. Although the scheme improved the accuracy of device identification, the analysis data was not preprocessed. The low accuracy of single classifier resulted in the low accuracy of the scheme, which was only 78.4%. Kawai et al. [7] proposed a method to identify communication devices based on network traffic pattern analysis, which uses statistical traffic features such as the interval of arrival (IAT) and packet size, and uses support vector machine (SVM) algorithm to identify devices. Aneja et al. [8] proposed a novel DFP analysis scheme for device fingerprint. Based on the arrival interval time, this scheme can improve the efficiency of device identification by drawing IAT diagram for groups and using deep learning algorithm to process the generated graph. However, these two schemes ignore many important features, resulting in unsatisfactory accuracy of device identification.

Ali et al. [9] proposed multiple classifier algorithms to identify IoT devices. The program trained six machine learning models, Decision Trees (DT), Support Vector Machine (SVM), Naive Bayes (NB), K-Nearest Neighbours (KNN), Random Forest (RF), and Adaboost (AB), and tested them on four publicly available datasets. The test results show that the NB classifier is superior to all other classifiers in traffic based device recognition, with an average accuracy of 92%. However, this scheme does not combine six learning models to give full play to its greatest advantage. Yu et al. [10] proposed a fine-grained device identification scheme based on cross layer protocol fingerprint. The scheme collects HTTP and TCP cross layer data packets and determines the specific fields of the protocol. Then, the convolutional neural network (CNN) and long short-term memory (LSTM) are used to extract the device feature fingerprint. High precision fine-grained IoT device identification is realized on three types of devices: network camera, router and printer. However, this scheme is only applicable to devices using HTTP protocol and TCP protocol, and has certain limitations. Jiao et al. [11] proposed a multi-level IoT device identification framework and a IoT device identification method, which can improve the accuracy of new category detection in IoT device identification. The proposed IoT device identification method extracts the characteristics of IoT devices in terms of protocol, firmware and load, and has high availability and identification accuracy.

The above research schemes have made important sharing for physical device identification. However, these schemes are either based on the fixed features of network traffic, lack of analysis of important relevant traffic features, resulting in low identification accuracy, or are limited to one or two protocols, so that the schemes can only be applied to the identification of some IoT devices, with certain limitations. Therefore, we propose a general network device identification scheme, which is not limited to a certain network protocol, automatically selects features in the network traffic, and uses machine learning to learn the identification model to realize the network device identification of cloud data center.

3 Framework

To meet the requirements of network device identification in large cloud data centers, we propose a general network device identification scheme. This scheme is not limited to a certain network protocol or a single subnet. Through passive collection of network traffic, rather than network element information, network traffic feature selection and feature learning can be used to obtain a classifier with high accuracy for unknown large cloud data center network device identification. The framework is shown in Fig. 1.

First, we deploy network traffic probes in the target cloud data center network to collect network traffic data. Network traffic data includes data link layer data, network layer data, transport layer data and application layer data. Then, the network traffic data packets in PCAP format are converted to two dimensional data in CVS format for feature analysis. Network traffic data has dozens of features, and irrelevant features and redundant features will reduce the accuracy of model training. Therefore, it is necessary to filter features and select relevant features for model training to get a trained classifier. Finally, the unknown cloud data center network traffic is input to the classifier for network device identification.

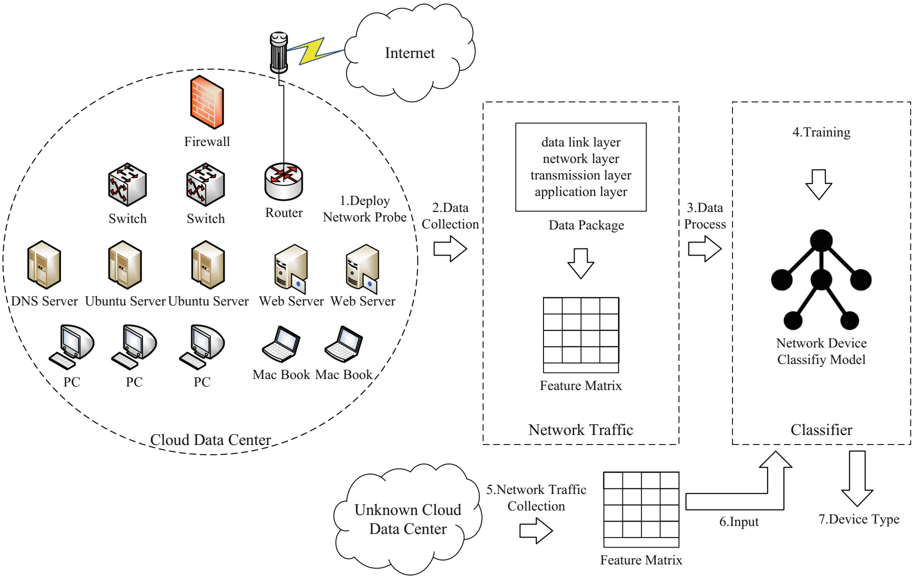


Fig. 1. Device identification framework.

4 Identification Scheme

This section introduces device identification scheme from three aspects: dataset, feature selection and device identification.

4.1 Dataset

In this scheme, we use the Intrusion Detection Evaluation Dataset (CIC-IDS2017) [12] dataset for traffic analysis. The network generating CIC-ISDS2017 dataset is similar to the cloud data center network, and has the characteristics of protocol diversification. Analyzing the network traffic of the dataset to identify devices can provide knowledge for network topology discovery of cloud data centers.

This dataset contains benign and common attacks, similar to real world data, and we only use benign datasets for analysis. The dataset builds the simulated behavior of 25 users based on multiple protocols such as HTTP, DNS, FTP, SSH and POP3, and generates natural benign background traffic. Its network topology is complete, including devices such as modems, firewalls, switches and routers, on which various operating systems such as Windows, Ubuntu, and Mac OS are deployed. It uses CICFlower to extract more than 80 network traffic characteristics from the generated network traffic, including timestamp, source and destination IP, source and destination port, protocol and other characteristics. We extracted the benign behavior data in the dataset and labeled the dataset with network devices. The quantity of network traffic information for each type of device in the dataset is shown in Table 1. Each dataset is the network traffic information of one day. From Table 1, we can see that these datasets are independent and distributed, similar to the natural network traffic in the real world. Taking Dataset2 as an example, the network traffic volume is shown in Fig. 2, which accords with the characteristics of each device. For example, the network traffic generated by the DNS server is much smaller than that of the PC or Ubuntu server. The DNS server stores mappings between domain names and IP addresses, and generates network traffic of a fixed size, containing domain names or IP addresses.

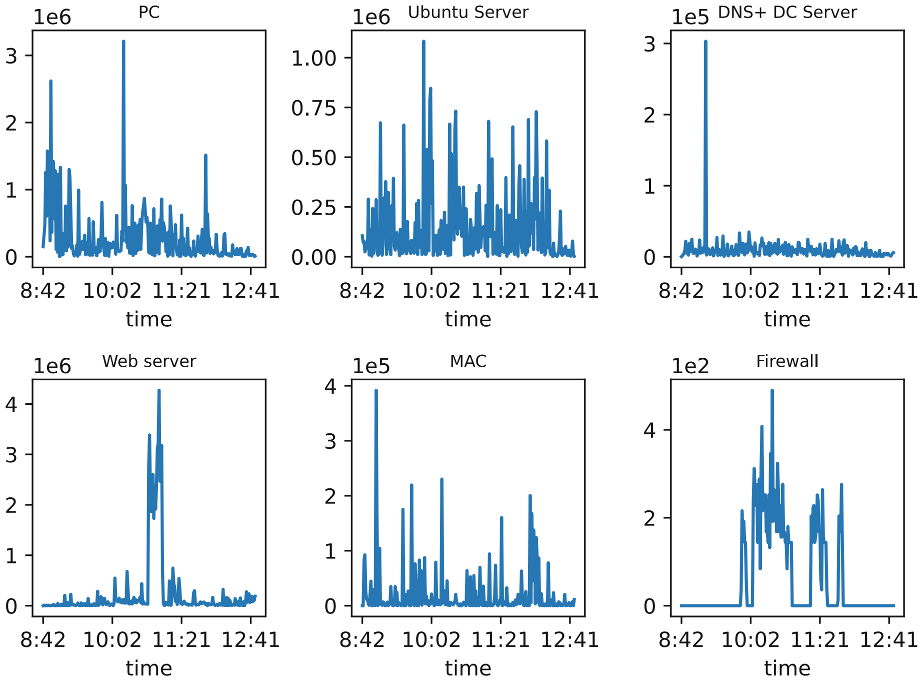


Fig. 2. Network traffic volume (Bytes).

Table 1. Number of traffic for each type of device

Device type	DNS+ DC server	Firewall	Macbook	PC	Ubuntu server	Web server
Dataset1	60801	196	154928	82976	30770	26726
Dataset2	60294	2145	152210	109930	37280	10281
Dataset3	55462	1088	205497	104171	18734	11420
Dataset4	36394	167	95872	70710	38354	8421

4.2 Features Selection

Network traffic data usually contains many features, among which, some features have nothing to do with the type of device or have little correlation, and some features can be inferred from other features. However, these features cannot improve the accuracy of model training, but increase the cost of model training. Feature selection refers to selecting the optimal feature subset from a set of original features to reduce the feature dimension and improve the classification accuracy [13]. Based on this, we propose a feature extraction method [14] of mixed filtering method and wrapping method. First, remove irrelevant features by filtering methods such as missing percentage method, and then select relevant features by using recursive feature elimination cross validation (RFECV) [15] features. The percentage of missing value is shown in Formula 1, and this feature is removed when the value is greater than the threshold value δ. RFE uses a base model (learner) to conduct multiple rounds of training [16]. After each round of training, a weight score list is obtained. After removing the features with low weight scores, the next round of training is conducted based on the remaining features until the number of features reaches the preset number. In this scheme, we use decision tree classifier to eliminate features. In order to obtain higher recognition accuracy, we perform RFE through cross validation to select the best number of features, as shown in Fig. 3.

$$Percentage\ of\ missing = \frac{sum(isNull(df))}{len(df)} \tag{1}$$

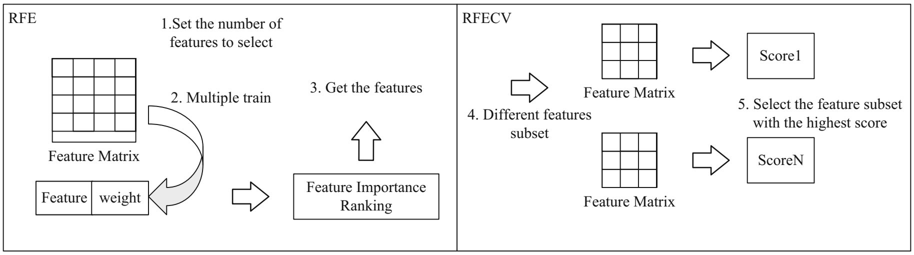

RFE
1.Set the number of features to select
Feature Matrix
2. Multiple train
3. Get the features
Feature
weight
Feature Importance Ranking
RFECV
Feature Matrix
Score1
4. Different features subset
5. Select the feature subset with the highest score
Feature Matrix
ScoreN

Fig. 3. Feature selection process.

4.3 Device Identification

After feature selection, the identification model is trained to identify devices. In the above dataset, firstly, the dataset is labeled with the device type, then the irrelevant features are filtered out by the missing percentage method, and the relevant features are automatically selected by RFECV algorithm. After that, the dataset is normalized and divided into the training set and the test set in the ratio of 80:20. The decision tree classifier is used for training on the training set, and the trained classifier is tested on the test set. The results of device identification are then compared with the device types in the test set to evaluate the classifier performance.

5 Experimental Evaluation

This section simulates our device identification scheme through experiments, and its performance is analysed. The laptop computer used in the experiment is configured with an Intel® Core™ i5-6200 CPU@2.30GHZ processor and 8GB of RAM running Windows 10 (64bit).

5.1 Metrics

The confusion matrix is a standard format for representing precision evaluation, from which four commonly used metrics, namely, accuracy, precision, recall and F1-score, are derived to evaluate the performance of the model on the test set [9]. The accuracy rate refers to the proportion of all correct predictions (positive and negative) in the total. As shown in Formula 2, it can judge the total accuracy rate, but it cannot be used as a good indicator to measure the results when the samples are unbalanced. The precision, that is, the proportion of correct predictions that are positive in all predictions, represents the precision of prediction in the results of positive samples, as shown in Formula 3. The recall refers to the proportion of correct prediction positive to all actual positive, as shown in Formula 4. F1-score is the harmonic average of the accuracy rate and recall rate. The larger the F1-score, the higher the model quality, as shown in Formula 5. Among them, TP, TN, FP and FN represent true positive, true negative, false positive and false negative respectively.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{2}$$

$$Precision = \frac{TP}{TP + FP} \tag{3}$$

$$Recall = \frac{TP}{TP + FN} \tag{4}$$

$$F1 - score = \frac{2 * TP}{2 * TP + FP + FN} \tag{5}$$

5.2 Simulation Result

We conducted experiments on the above datasets, and the results are shown in Table 2. From the overall test results, the precision, recall and F1-score have reached 96%, with good performance. In the identification results of each type of device, the precision of DNS+ CD Server and Web Server has reached 100%, and the precision of other devices is also at a high level.

Table 2. Dataset test results

Metrics	Precision	Recall	F1-score
DNS+ DC server	100%	99%	99%
Firewall	96%	96%	96%
Macbook	96%	87%	91%
PC	94%	94%	94%
Ubuntu server	91%	92%	92%
Web server	100%	99%	99%
Weighted avg	96%	96%	96%

5.3 Contrast Experiment

To illustrate the scientificalness of the scheme, we tested all dataset without feature selection and manually selected datasets with six features, 'Source Port', 'Destination Port', 'Protocol', 'Flow Duration', 'Total FWd Packets', and 'Flow Bytes/s', based on subjective experience, and compared the results with our scheme, as shown in Fig. 4. The accuracy of the test results with all the data is 3% higher than that with manually selected features, because the manually selected features lose some relevant features, resulting in a decline in accuracy. The accuracy of our scheme test results is 6% higher than that of training with all features datasets. This is because the original dataset contains irrelevant features and redundant features that interfere with the training. Our scheme automatically selects relevant features through RFECV algorithm, which has a high accuracy rate.

Next, we compare the test results of our scheme with scheme [7] and scheme [8], as shown in Table 3. In terms of device type identification, our scheme has obvious advantages.

Table 3. Comparison of schemes.

Schemes	Accuracy
Scheme [7]	88.1%
Scheme [8]	86.7%
Our shceme	96%

6 Conclusion

In order to meet the requirements of network device identification in cloud data center, this research proposes a network device identification scheme based on

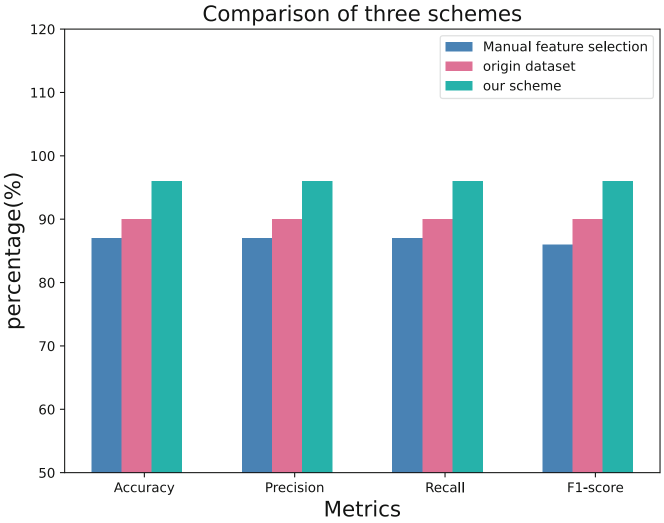


Fig. 4. Comparison of different feature selection schemes.

network traffic analysis. This scheme is not limited to a certain protocol. Network traffic is collected in a passive way, and relevant features are selected by feature filtering and feature selection algorithm to carry out device classifier training. Then, the trained model is applied to new traffic data to identify unknown cloud data center network devices. Finally, we carry out experiments on the proposed scheme, and the results show that the accuracy of the scheme is as high as 96%, and the performance metrics are excellent.

In the future work, we will consider adding the traffic dataset collected from the unknown network to the training set, and continuously optimize the identification model to obtain higher accuracy.

Acknowledgements. This work was supported by National Key R&D Program of China (2020YFB1807800).

References

1. Ammar, N., Noirie, L., Tixeuil, S.: Autonomous IoT device identification prototype, 2019 network traffic measurement and analysis conference (TMA), pp. 195–196. https://doi.org/10.23919/TMA.2019.8784517
2. Pashamokhtari, A., Okui, N., Miyake, Y., Nakahara, M., Gharakheili, H.H.: Inferring connected IoT devices from IPFIX records in residential ISP networks. In: 2021 IEEE 46th Conference on Local Computer Networks (LCN), pp. 57–64. https://doi.org/10.1109/LCN52139.2021.9524954
3. Chen, Y., Pan, J., Yu, D., Ma, Y., Yang, Y.: Retransmission-Based TCP Fingerprints for Fine-Grain IoV Edge Device Identification. IEEE Trans. Veh. Technol. **71**(7), 7835–7847 (2022). https://doi.org/10.1109/TVT.2022.3169090

4. Tamura, H., Yanagisawa, K., Shirane, A., Okada, K.: Wireless devices identification with light-weight convolutional neural network operating on quadrant IQ transition image. In: 2020 18th IEEE International New Circuits and Systems Conference (NEWCAS), pp. 106–109. https://doi.org/10.1109/NEWCAS49341.2020.9159777
5. Yuan, Y., Peng, L.: Wireless device identification based on improved convolutional neural network model. In: 2018 IEEE 18th International Conference on Communication Technology (ICCT), pp. 683–687. https://doi.org/10.1109/ICCT.2018.8600086
6. Imamura, Y., Nakamura, N., Yao, T., Ata, S., Oka, I.: A device identification method based on combination of multiple information. In: NOMS 2020—2020 IEEE/IFIP Network Operations and Management Symposium, pp. 1–4. https://doi.org/10.1109/NOMS47738.2020.9110448
7. Kawai, H., Ata, S., Nakamura, N., Oka, I.: Identification of communication devices from analysis of traffic patterns. In: 2017 13th International Conference on Network and Service Management (CNSM), pp. 1–5. https://doi.org/10.23919/CNSM.2017.8256018
8. Aneja, S., Aneja, N., Islam, M.S.: IoT device fingerprint using deep learning. IEEE Int. Conf. Internet Things Intell. Syst. (IOTAIS) **2018**, 174–179 (2018). https://doi.org/10.1109/IOTAIS.2018.8600824
9. Ali, Z., Hussain, F., Ghazanfar, S., Husnain, M., Zahid, S., Shah, G.A.: A generic machine learning approach for IoT device identification. Int. Conf. Cyber Warf. Secur. (ICCWS) 118–123 (2021). https://doi.org/10.1109/ICCWS53234.2021.9702983
10. Yu, D., Xin, H., Chen, Y., Ma, Y., Chen, J.: Cross-layer protocol fingerprint for large-scale fine-grain devices identification. IEEE Access **8**, 176294–176303 (2020). https://doi.org/10.1109/ACCESS.2020.3026818
11. Jiao, R., Liu, Z., Liu, L., Ge, C., Hancke, G.: Multi-level IoT device identification. In: 2021 IEEE 27th International Conference on Parallel and Distributed Systems (ICPADS), pp. 538–547. https://doi.org/10.1109/ICPADS53394.2021.00073
12. Sharafaldin, I., Lashkari, A.H., Ghorbani, A.A.: Toward generating a new intrusion detection dataset and intrusion traffic characterization. In: International Conference on Information Systems Security and Privacy
13. Xu, Z.Z., Shen, D.R., Nie, T.Z., Kou, Y.: Hybrid feature selection algorithm combining information gain ratio and genetic algorithm. Ruan Jian Xue Bao/J. Softw. **33**(3), 1128–1140 (in Chinese). http://www.jos.org.cn/1000-9825/6099.html
14. Yu-Lin, P., Xi-Wang, L.: Feature selection algorithm of network traffic based on SU and AMB. Comput. Syst. Appl. **31**(4), 281–287. https://doi.org/10.15888/j.cnki.csa.008410
15. Mustaqim, A.Z., Adi, S., Pristyanto, Y., Astuti, Y.: The effect of Recursive Feature Elimination with Cross-Validation (RFECV) feature selection algorithm toward classifier performance on credit card fraud detection. Int. Conf. Artif. Intell. Comput. Sci. Technol. (ICAICST) 270–275 (2021). https://doi.org/10.1109/ICAICST53116.2021.9497842
16. Zhao, J., Cong, S.: Research on property prediction of materials based on machine learning. In: 2020 3rd International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE), pp. 44–46. https://doi.org/10.1109/AEMCSE50948.2020.00017

Analysis of the Process of Public Opinion Dissemination Based on the SCT Model and Model Improvement

—Take the topic of “Small Town Exam-oriented Students” on Weibo as an example

Xuexiao Zhang[1(✉)], Wanshun Heng[1], Ming Lei[1], Li Xu[1,2], and Siwen Xu[3]

[1] College of computer Science and Technology, Harbin Engineering University,
Harbin 150001, China
3143498885@qq.com

[2] Modeling and Emulation in E-Goverment National Engineering Laboratory,
Harbin, China

[3] Université Paul Sabatier-Toulouse, Toulouse, France

Abstract. The SCT model, which was created based on the WD model and describes the diffusion of public opinion, is unable to fully capture the evolution of public opinion. We examined the development and affecting aspects of “Small Town Exam-oriented Students” using the preprocessing of crawler data. Based on this fundamental concept, we suggested an enhanced SCT model. Initially, using the interaction amplitude control parameters, we described the impact of official media on public opinion. The value of the parameters determining how attractive a topic is was then the subject of a classified conversation. The experiment shown that, when compared to the conventional SCT model, our improved SCT model has a faster rate of convergence with no differences in the evolving results. The final evolving outcome typically agrees with the microblog content LDA model analysis result.

Keywords: LDA topic model · SCT model · Information cocoons · Echo chamber situation · Evolution of public opinion communication

1 Introductione

The method that information is disseminated and public opinion is formed has changed significantly from how it was in the past with the flourishing development of the internet and new media today. Information is propagating in a more complicated internet environment as internet users are getting more and more vocal and are able to submit information and comment on events whenever and wherever they are using a variety of websites and community software. The Internet and new media have two sides to it. It can help incidents get resolved and encourage engaged public participation in social discourse. It also increases

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 68–80, 2024.
https://doi.org/10.1007/978-981-99-7161-9_6

exposure to views that individuals already agree with, which facilitates view polarization. Internet users are entrapped by the "information cocoons" and the "echo chamber problem" in the social media communication paradigm. We can only successfully encourage contact between various Internet users and transform the web into a space where people may expand their horizons and share various perspectives by busting the information cocoon. Users will be able to understand and evaluate news and social reality more thoroughly and accurately as a result, improving online public opinion.

2 Theoretical Background

From the 1960s to the start of the twenty-first century, researchers mostly used observational and small-group psychological experimental approaches to understand the mechanisms behind the sociological patterns underlying the phenomena of the evolution of public opinion. At this time, a lot of well-known theories regarding the evolution of public opinion were advanced [1]. Since the start of the twenty-first century up until the present, academics have concentrated their research on the empirical study of the evolution of public opinion using modelling and simulation methods, with mathematical and theoretical empirical evidence of public opinion phenomena serving as the main research content. Advanced research techniques or methods are used to realize the simulation or emulation of public opinion phenomena and summarize the laws related to public opinion evolution issues in the process of simulation and emulation. The evolution of public opinion is depicted using corresponding mathematical or physical models. The research findings from these two eras have various drawbacks because of the influence of elements like the historical context and technological foundation of the times, which can be summed up in the following two characteristics [2].

(1) The limits of the era of theoretical research
The formation mechanism and sociological laws of public opinion phenomena were the main topics of theoretical research from the middle of the 20th century to the beginning of the 21st [3]. Theories of public opinion explanation were proposed from the perspectives of social rules or steps of human cognitive decision-making methods on which public opinion phenomena are formed. The experimental process of many ideas, however, employs the small group psychological experiment approach due to the limits of technology. Although the operation is straightforward, the procedure is manageable, and the experimental outcomes are simple to analyze, this method is affected by the laboratory environment, the experimental site can only be confined to the laboratory, and the scale of the experimental group cannot be too large to cover a large number of experimental subjects. As a result, the small group psychological experiment method can only study the problem of small-scale public opinion evolution and is not suitable for studying larger-scale public opinion evolution [4]. Because public opinion concerns are broad and social in nature, the approach of small group psychological tests can only be

used to explore the topic of small-scale public opinion evolution. Second, the subjects of psychological studies are typically strangers with uncomplicated social relationships. Moreover, the experimental circumstances are frequently in control of how individuals interact, making it difficult to see complex interactions between subjects. Nonetheless, the interactions between those involved in shaping public opinion in the modern era are frequently complicated. It is apparent that the small group psychological experiment approach cannot explain and comprehend complicated network properties [5] . Also, to display discrete lagged panel values, small group psychological experiments need manual data processing, which is poor, and individual opinion values are influenced by the recording techniques and sentiment measuring scales. In reality, however, the information interaction process that contributes to the evolution of public opinion is frequently ongoing and real-time [6].

As a result, there are notable discrepancies between the features of the current social opinion environment and small group psychology experiments. Several academics have therefore questioned the logic and social interpretability of theoretical findings based on small group psychology tests, and the outdated theories urgently require new research methodologies to support, augment, or improve them.

(2) Technical limitations of new research methods

The stage of mathematical and empirical study on the development of public opinion has been ongoing from the beginning of the twenty-first century to the present [7]. In a study they released in 2006, Grabowski and KosiAski imaginatively suggested the idea of employing physical models to address sociological issues based on the conventional physical model. Using computer modeling to simulate the entire model evolution process, the process of using model simulation to explain social science problems was perfectly realized, bridging the gap between mathematical science research and social science research. Ising as an analogy to the process of communication and information exchange among individuals in human society [8]. The research divide between the social sciences and mathematics was removed. Since then, the concept of employing computer modeling and simulation methods to address social science issues has gained popularity in academia, and research into the pairing of simulation methods with public opinion has also begun. It is now possible to analyze large and complex networks, handle the laborious calculation steps of information interaction in the process of opinion interaction, and quickly grasp the process of dynamic changes in group opinion thanks to the powerful computing power of computer technology. This has significantly reduced the difficulty of researching issues in the field of public opinion [9].

The model simulation approach's social explanatory and theoretical persuasiveness, however, is frequently insufficient. Due to the difficulty of constructing models and the complexity of research, many models are unable to completely encompass all social aspects and adequately describe social rules. Models are rudimentary simulations of reality that are composed of mathematical formulas generated from formulas of social laws. The models' insufficient modeling of social reality, their flawed underlying theory, and their inadequate social justification all have an impact on the simulation findings [10]. Thus, concerns that must be addressed in the development of simulation methods include enhancing the social rules of simulation methods and expanding the social justifications of models. The theoretical research results concentrate on the elaboration and explanation of social rules and the mechanisms by which public opinion issues are formed, but their research methodologies are unable to grasp the features of today's social opinion environment and are unable to process data such as opinion information; as a result, many scholars question the validity of the old theories and their applicability to the modern era.

3 SCT Model Principle

Suppose the number of individuals in a population in which viewpoint evolution occurs is N. At any moment t, the views held by individual i in the group are given by the value of the view $O_i(t)(i = 1, 2, 3, \ldots, N)$ in the range of $[-1, 0) \cap (0, 1]$, where a viewpoint of $[-1, 0)$ indicates that the individual has a negative view and a viewpoint of $(0, 1]$ indicating that the individual has a positive viewpoint. For the set of individuals that can be directly associated with i, the number of individuals with the same sign as the viewpoint value of individual im. The set of views is expressed as $L_{i+}(x)$ $(x = 1123\ldots, m)$. The number of individuals with different signs from the value of viewpoint i is$n$. The set of views is expressed as $L_{i-}(x)$ $(x = 123\ldots, n)$, so it is easy to know that $m + n = k$. At each moment t, individuals i and j with the same sign on an edge in that population network are selected to interact with each other.The views of individuals i and j at time t + 1 are

$$\begin{cases} O_i(t+1) = O_i(t) + \mu(O_j(t) - O_i(t)) \\ O_j(t+1) = O_j(t) + \lambda(O_i(t) - O_j(t)) \end{cases} \tag{1}$$

For individual i, when n is 0, it means that the symbols of the views of the individuals directly associated with individual i are the same as those of individual i. then individual i and its neighbouring nodes have only the intra-cluster mean difference value, and the within-group difference value γ_i is calculated as

$$\gamma_i = \sum_1^M |O_i(t) - L_{i+}(x)| \,/M \tag{2}$$

When γ_i is not $0, \gamma_{igetsj}$ is used to denote the within-group variance of the viewpoint value of individual j in the relational network of individual i

$$\gamma_{i \leftarrow j} = (\sum_1^M |O_i(t) - L_{i+}(x)|)/M \tag{3}$$

If $\gamma_{i \leftarrow j} < \gamma_i$,then $\mu = k_1 |\gamma_i - \gamma_{i \leftarrow j}|$,otherwise $\mu = 0$. If γ_i is 0 then $\mu = 0$. If n is not 0 we make the metric pairwise ratio being δ_i

$$\delta_i = \frac{(\sum_1^N |O_i(t) - L_{i-}(x)|)/N}{(\sum_1^M |O_i(t) - L_{i+}(x)|)/M} \tag{4}$$

$\delta_{i\leftarrow j}$ denotes the value of the meta-ratio of the viewpoint of individual j in the population of i

$$\delta_{i\leftarrow j} = \frac{(\sum_1^N |O_i(t) - L_{i-}(x)|)/N}{(\sum_1^M |O_j(t) - L_{i+}(x)| + |O_j(t) - O_i(t)|)/M} \tag{5}$$

If $\delta_{i\leftarrow j} > \delta_i$, then $\mu = k_2 |\delta_{i\leftarrow j} - \delta_i|$, or $\mu = 0$ Similarly the model interaction formula for individual 1 to individual N can be obtained.

4 SCT Model Analysis

Weibo user discussion trends on these two topics were examined over time using the LDA topic model [r1]. The topic distribution of a document is frequently inferred using the LDA model. It provides the subject matter of each document in a document collection as a probability distribution, allowing you to do subject clustering or text classification based on the subject distribution by analysing a number of documents to extract their subject distribution.Because the LDA topic model enables us to perform topic clustering on the crawled set of Weibo, we believe that words can, to some extent, reflect the opinions and feelings of users. Analysis of the words contained within Weibo can, therefore, reflect the direction of opinion on a topic in one way or another. As a result, we have decided to analyse the topic's evolution using the LDA topic model.

According to the SCT model, the degree of perspective prototypicality between viewpoint sender I and viewpoint recipient j determines whether or not a viewpoint interaction takes place. The viewpoint of I influences the viewpoint of j when the viewpoint prototypicality of I within the viewpoint of j group is stronger than the viewpoint prototypicality of j within his own group. Contrarily, nothing happens. The interaction of viewpoints is described as follows:

$$\begin{cases} O_i(t+1) = O_i(t) + \mu(O_j(t) - O_i(t)) \\ O_j(t+1) = O_j(t) + \varepsilon(O_i(t) - O_j(t)) \end{cases} \tag{6}$$

The μ and ε are the interaction amplitude control parameters, $O_i(t+1)$ and $O_i(t)$ are the viewpoint values of individual i at moment t and t+1.The interaction amplitude control parameter is an important indicator of the attractiveness of a viewpoint.In the SCT model, when individual i has only within-group mean differences from neighbouring nodes,then $\mu = \frac{1}{2} |\gamma_i - \gamma_{i\leftarrow j}|$; when the meta-ratio exists, $\delta_i = |\phi_{i\leftarrow j} - \phi_i|$, $\mu = \frac{1}{2} \frac{\delta_i}{\delta_i+1}$ [DBLP:journals/access/YanYNLW20].

After getting the raw data using a Python program, we pre-processed the data in a straightforward manner. In the end, we were able to acquire 346470 valid pieces of information after removing 415764 invalid ones, including user links, user devices, image addresses, microblogging connections, etc. Because the gathered text data was not in a standard format and could not be used directly, we had to further process it after filtering and counting it. By word separation, creating a unique library, and turning off the word dictionary, we processed the text data. Even though the crawled Excel data had been filtered, its non-standard format prevented immediate use, necessitating additional processing. We divided the text data processing into three steps: word separation, word deactivation processing, and building a unique lexicon.

(1) Word separation: In the process of processing the text corpus, word separation is a crucial phase. While Chinese sentences typically consist of a series of words, it can be challenging to determine a word's lexical nature because words frequently have numerous meanings. We therefore carry out word separation processing. In the Python Chinese word separation component, jieba was employed. After word separation, the text file is saved and used for later calculations.

(2) Word deactivation processing: In order to conserve internal storage, increase the effectiveness of retrieval, and improve the precision of matching, some words must be filtered out during the processing of the original text. To further process the papers, we combined the HIT deactivation word list with the Chinese deactivation word list and the Baidu deactivation word list.

(3) Custom dictionaries: As civilization progresses, new terms are continually appearing online. Computers are not kept up to date enough, thus in case the computer is unable to accurately detect the meanings of the popular Internet words and their lexical features from the collation, they are entered manually. Within these 30 days, we carried out independent LDA thematic analyses of the microblogs, analyzing the process of opinion evolution through daily variations in the content of the microblogs.

The topic modeling procedure involves getting the probability of the distribution of document topics and the probability distribution of topic lexical items before utilizing the LDA topic model. These two crucial factors are the hyperparameters *alpha* and *beta*. The more balanced the topic distribution and the more uniformly distributed the documents are, the larger the *alpha*; the more lexical elements there are in the document, the larger the *beta*. Here, we make use of the ldamodel Python package's default values.

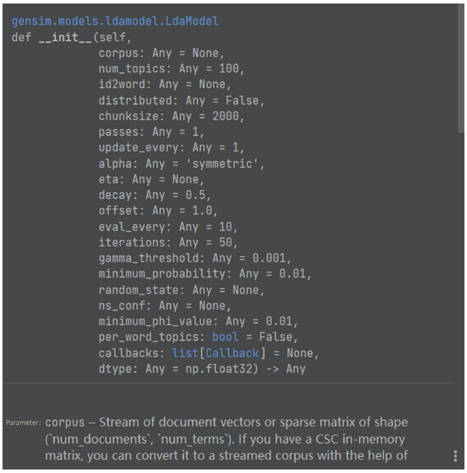
A confusion analysis and a consistency analysis were carried out to determine the ideal amount of topics for a more precise analysis.

In the confusion formula, M represents the total number of all texts in the corpus. N_m represents the number of lexical items in the mth document; W_m represents the number of lexical items in the mth document, i.e. the effect of model changes can be tested by varying the k-value.

$$P(W_m) = \prod_{i=1}^{N_\alpha} \sum_{z} p(w_{d,i}|z)p(z|d) \tag{7}$$

In Eq. (1) $P(W_m)$ denotes the probability of generating document m. $P(z|d)$ is the chance of an event occurring for each topic in the document. The total number of word items and the entire length of the test set are used as the denominators in the calculation of confusion.

$$Perplexity = exp\left\{-\frac{\sum_{m=1}^{M} logp(W_m)}{\sum_{m=1}^{M} N_m}\right\} \tag{8}$$



```
gensim.models.ldamodel.LdaModel
def __init__(self,
             corpus: Any = None,
             num_topics: Any = 100,
             id2word: Any = None,
             distributed: Any = False,
             chunksize: Any = 2000,
             passes: Any = 1,
             update_every: Any = 1,
             alpha: Any = 'symmetric',
             eta: Any = None,
             decay: Any = 0.5,
             offset: Any = 1.0,
             eval_every: Any = 10,
             iterations: Any = 50,
             gamma_threshold: Any = 0.001,
             minimum_probability: Any = 0.01,
             random_state: Any = None,
             ns_conf: Any = None,
             minimum_phi_value: Any = 0.01,
             per_word_topics: bool = False,
             callbacks: list[Callback] = None,
             dtype: Any = np.float32) -> Any
```

Parameter: corpus – Stream of document vectors or sparse matrix of shape (`num_documents`, `num_terms`). If you have a CSC in-memory matrix, you can convert it to a streamed corpus with the help of

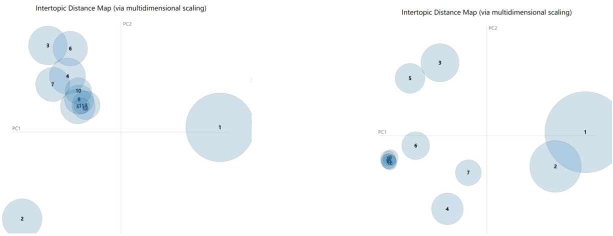
Fig. 1. Program default parameter settings

The most fundamental consistency analysis formula is as follows:

$$C_k = \sum_{m=2}^{M} \sum_{l=1}^{m} log \frac{D(v_m^k, v_l^k) + 1}{D(v_l^k)} \tag{9}$$

The $V^k = (v_1, \ldots, v_m^k)$ is a list of the M top words in topic k, the $D(v)$ is the number of tweet comments that contain the word v,the $D(v, v')$ is the number of tweet comments in which the words v and v' appear together at least once.

The perplexity and consistency were then calculated using the training models for various themes, and the best number of topics was chosen based on the perplexity and consistency change curves. The findings of our calculations for the two themes separately for confusion and consistency are displayed in Fig. 3.



(a) Results for days 1 and 2 obtained by model analysis

(b) Results for days 7 and 8 obtained by model analysis

Fig. 2. Rresults

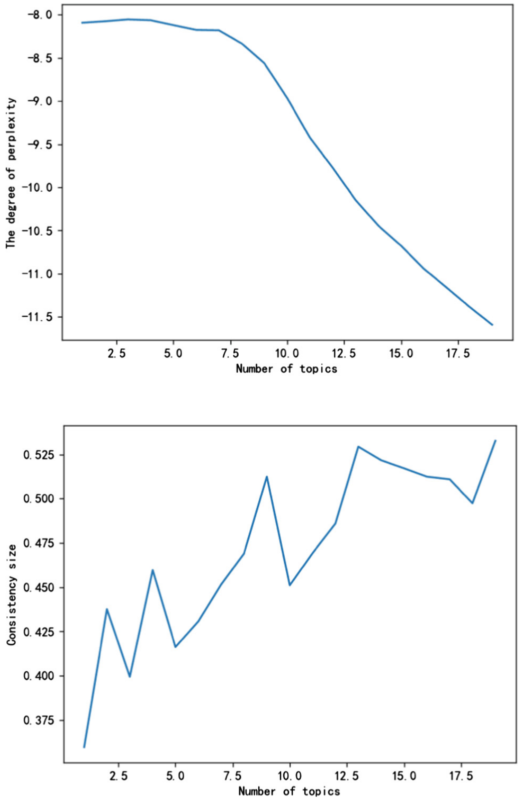


Fig. 3. Topic parameter setting chart

Using the topic "Small Town Exam-oriented Kids" as an example, we set the number of topics to 12 and evaluated the crawled tweets over a 48-hour period. The findings are displayed in Fig. 3.

As we can see, the most often used terms throughout the first six days of the topic were, and. The tweets' major ideas were around the phrase "Small Town Exam-oriented Students," as well as choices and outlooks on life. Days 7 and 8 show a sudden appearance and rise in the rankings of the keywords "Newsweek" and "Yi Qianxi," and at this time, the conversation centers on the article published by China Newsweek and the then-trending subject "Yi Qianxi's test preparation." The conversation centered on the article from China Newsweek and the current hot topic, "Yi Qianxi's editorial examination." Instead of "effort," "choice," and "life," the words "accusatory personality" and "star" were used frequently in the China Newsweek piece. The only terms that are as common as "small town question creator" are "choice" and "life."

We think that this was mostly brought on by a China Newsweek piece about the "editorial exam" of Yi Yan Qianxi. The release of this essay spurred discussion online and significantly influenced the development of public opinion on the subject. Although the frequency of "Newsweek" keyword mentions gradually decreased during the ensuing period, the nature of conversations and viewpoints expressed on the subject more dramatically changed. The graph shows how the primary keywords have changed. We might therefore presume that the posting by China Newsweek had a significant impact on the subject, influencing the course of the discussion.

Because China Newsweek is an official publication, its opinions are consistent and have a strong tendency to steer public opinion in a particular direction. Yet, the current SCT paradigm treats opinion leaders equally and without distinction, which is incompatible with the actual scenario, so we propose to improve the SCT model by introducing an influence factor β to focus on the influence of opinion leaders' views.

5 Improvements to the SCT Model

The SCT model's strength is that it progresses from modeling individual behavior to modeling group behavior, and the opinion interaction rules are focused on prototypical rules that take into account the influence caused by individual internal and external group relations on the development of public opinion. However, the SCT model pays less attention to the influence caused by Internet-related factors on the development of public opinion, so we start from that point. The interaction and development of collective viewpoints frequently involve opinion leaders in a significant way. We think that opinion leaders primarily take the following two forms on social media websites like Weibo: 2 messages released by official media, and opinions; 1 comments or answers with high likes and retweets.

The meta-pair ratio is employed in the SCT model to represent an opinion's capacity to sway other people's ideas. The influence of a viewpoint on other members of the same opinion group increases with the meta-pair ratio, whereas the likelihood that other members of the group will have an impact on the viewpoint decreases. We contend that Weibo's high like and retweet rates are more in line with the pattern of opinion interaction represented by the SCT model than they are with the pattern suggested by the meta-pair ratio. In another sense, the high Weibo likes and retweets are a representation of the plateau type. Also, tweets that receive a lot of likes and retweets have material that tends to stay the same over time, making them suitable for use as examples of independent thought.

The SCT model does not account for the ability of opinion leaders to frequently affect every member of a group without altering their own opinion values. The official media's opinions reflect official attitudes to some extent, thus they should be consistent in the sight of others, changing within an acceptable range, and having little effect on the group as a whole. People tend to ignite public opinion and have a more dramatic impact on the evolution of public opinion when they perceive official attitudes as changing more dramatically. This makes people in the group more susceptible to the more prototypical opinions of other people in the same group who share their views.

We contend that while internet users with opposing views frequently disregard these tweets, meaning that these opinion leaders' tweets have no impact on those users with opposing views, the opinions of these unofficial media opinion leaders frequently have a greater influence on internet users with similar fundamental attitudes toward the topic. This is the distinction between the influence of recognized opinions and the influence of the official media.

Additionally, as the LDA model's findings demonstrate, we think that when a topic is attractive, it has a wider and deeper coverage, more perspectives are available for general Internet users to participate in the discussion, and opinion leaders within a particular perspective have a stronger influence on other users who share that perspective; when a topic's appeal is low, it receives little coverage, and there are a large number of users involved Low topic appeal results in relatively little coverage of the topic and a small number of persons participating overall. Online opinion leaders can have a greater impact on a larger variety of users' viewpoints, but their influence is less powerful overall.

5.1 Improved Realisation

We believe that when the topic has just started to be discussed, these official media have not yet commented and guided the event in a timely manner, and the impact on other users is no different from that of ordinary microblogs. When $t > 1000$, we believe that the official media starts to play a role in influencing others. The maximum value of μ is 0.5, since people tend to change their opinions gradually and do not suddenly change their opinions drastically. When the topic is discussed in a large volume, the control parameter μ for the magnitude of the interaction of such opinion leaders on other users takes the following values.

$$\mu = \begin{cases} 0.5 \\ (0 \leq |Y - X| \leq 0.05) \\ 0.4 \\ (0.05 \leq |Y - X| \leq 0.1) \\ 0.25 \\ (0.1 \leq |Y - X| \leq 0.15) \\ 0.1 \\ (0.15 \leq |Y - X| \leq 0.20) \end{cases} \tag{10}$$

where Y is the opinion value of the opinion leader and X is the opinion value of user j. When $|Y - X| \geq 0.2$, μ takes 0.

When the volume of discussion on the topic is small, the control parameter μ for the magnitude of the interaction of the opinion leader with user j takes the value

$$\mu = \begin{cases} 0.3 \\ (0 < |Y - X| \leq 0.1) \\ 0.25 \\ (0.1 < |Y - X| \leq 0.15) \\ 0.2 \\ (0.15 < |Y - X| \leq 0.2) \end{cases} \tag{11}$$

when $|Y - X| \geq 0.2$, μ takes 0.

When individual i is not an opinion leader, if n is 0, then there is only an intra-cluster mean difference value between individual i and neighbouring nodes, and let the intra-cluster mean difference value be γ_i,

$$\gamma_i = \textstyle\sum_I^M \left| O_i(t) - L_{i^+}(x) \right| /M \tag{12}$$

when γ_i is not zero, denote the value of the within-group variation exhibited by the viewpoint value of individual j in the relation of individual i by $\gamma_{i \leftarrow j}$.

$$\gamma_{i \leftarrow j} = (\textstyle\sum_I^M |O_j(t) - L_{i^+}(x)| + |O_j(t) - O_i(t)|)/M \tag{13}$$

if $\gamma_{i \leftarrow j} < \gamma_i$,then $\mu = k_1 \left| \gamma_i - \gamma_{i \leftarrow j} \right|$,otherwise $\mu = 0$;

when γ_i takes 0, $\mu = 0$;

if n is not 0 let the dollar pair ratio be ϕ_i,

$$\phi_i = \frac{(\sum_1^N |O_i(t) - L_{i^-}(x)|)/N}{(\sum_1^M |O_i(t) - L_{i^+}(x)|)/M} \tag{14}$$

denoting by $\phi_{i \leftarrow j}$ the value of the meta-pair ratio that the viewpoint value of individual j exhibits in the eyes of individual i.

$$\phi_{i \leftarrow j} = \frac{(\sum_1^N |O_j(t) - L_{i^-}(x)|)/N}{(\sum_1^M |O_j(t) - L_{i^+}(x)| + |O_j(t) - O_i(t)|)/M} \tag{15}$$

if $\phi_{i \leftarrow j} > \varPhi_i$, then $\mu = k_2 \left| \phi_{i \leftarrow j} - \phi_i \right|$, otherwise $\mu = 0$. The model interaction equation for individual j is obtained in the same way.

5.2 Simulation Results of the Improved Model

On July 7, we randomly selected one tweet from the “Small Town Question Maker” topic, and we assigned a value to the tweet’s viewpoint based on the content of the tweet. Based on the model we developed, we wrote the program. Following a comparison with the results of the SCT model simulation, the model’s simulation was run using the processed Weibo opinion values.

As observed in the image, the convergence of the model accelerates in comparison to before the improvement following the addition of pertinent influencing factors like subject discussion degree and opinion leaders, but the outcomes of opinion evolution are not significantly different. Indicating that the netizens’ perspectives eventually diverge and stabilize, the viewpoint values converge into multi-stranded viewpoint clusters, with more users clustered around −0.75, 0.80. This is similar to the outcomes of the LDA topic model for microblog content.

6 Summary and Outlook

The LDA model was used to evaluate the development of the topic of “Small Town Question Maker” after first outlining the basic concepts of the SCT model.

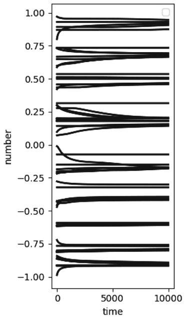


Fig. 4. Simulation results after SCT model improvement

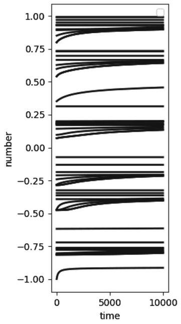


Fig. 5. Simulation results of the SCT model

We draw the conclusion that the modified SCT model can more accurately depict the evolution of public opinion on the subject of "small town question makers" given that the results of the improved SCT model are compatible with those of the LDA model.

The way information is shared and public opinion is formed is getting more complicated nowadays as a result of the growth of the Internet and new media. This implies that the findings of theoretical study need to be continuously checked, expanded upon, and improved. In order to develop a new model that is better suited for the distribution of public opinion in contemporary society, we analyze the strengths and shortcomings of the SCT model in this work. This approach can be used to study and enhance not only the SCT model but also other models of public opinion communication, leading to the development of a more modern model of public opinion communication.

References

1. Cheng, M.-M., et al.: Global contrast based salient region detection. In: IEEE CVPR. pp. 409–416 (2011)
2. Cheng, M.-M., et al.: RepFinder: finding approximately repeated scene elements for image editing. ACM Trans. Graph. **29**(4), 83, 1–8 (2010)
3. Proskurnikov, A.V., et al.: Opinion evolution in time-varying social influence networks with prejudiced agents. IFAC-PapersOnLine **50**(1), 11896–11901 (2017)
4. Ramage, D., et al.: Labeled LDA: a supervised topic model for credit attribution in multi-labeled corpora. In: Proceedings of the 2009 Conference on Empirical Methods in Natural Language Processing, pp. 248–256 (2009)
5. Rana, N.P., Dwivedi, Y.K.: Citizen's adoption of an e-government system: validating extended social cognitive theory (SCT). Gov.Ment Inf. Q. **32**(2), 172–181 (2015)
6. Sznajd-Weron, K., Sznajd, J.: Opinion evolution in closed community. Int. J. Modern Phys. C **11**(06), 1157–1165 (2000)
7. Taherdoost, H.: A review of technology acceptance and adoption models and theories. Procedia Manuf. **22**, 960–967 (2018)
8. Uthirapathy, S.E., Sandanam, D.: Predicting opinion evolution based on information diffusion in social networks using a hybrid fuzzy based approach. Int. J. Inf. Technol. 1–14 (2022)
9. Wang, Y.-S., et al.: Optimized scale-and-stretch for image resizing. ACM Trans. Graph. **27**(5), 118, 1–8 (2008)
10. Wei, X., Bruce Croft, W.: LDA-based document models for ad-hoc retrieval. In: Proceedings of the 29th Annual International ACM SIGIR Conferene on Research and Development in Information Retrieval, pp. 178–185

A Meta-Analysis of the Prevalence of Chronic Disease Co-morbidity Among the Elderly in China

Fang Xia[1], Shiyu Gao[1], Ziying Xu[1], Zongyi Xie[2], and He Wang[1](✉)

[1] School of Health Management, Changchun University of Chinese Medicine,
Changchun 130117, China
20935443@qq.com

[2] Special Services Section, Hospital No. 964, Changchun 130021, China

Abstract. Objective: This paper aims to assess the occurrence of chronic disease co-morbidity among the elderly in China. **Methods**: The databases of PubMed, Web of Science, CNKI, VIP and Wanfang were searched by computer. Single proportion studies on the prevalence of chronic disease co-morbidity among the elderly in China from June 2011 to June 2022. All included articles were quality assessed. The heterogeneity test was performed using the Mantel-Hasenzel algorithm. Comprehensive Meta-Analysis (CMA) software was used for meta-analysis. **Results**: A total of 31 cross-sectional studies containing 226209 patients were included. Meta-analysis results showed that The prevalence of chronic disease co-morbidity in China aged $\geq$60 years was 42.8% [95% CI (36.6, 49.3%)]. Subgroup analysis showed that the prevalence of chronic disease co-morbidity was 37.1% (95% CI (29.6, 45.3%)) in men and 39.5% (95% CI (30.4, 49.3%)) in women; the prevalence of 2 chronic diseases was 51.6% [95% CI (43.9, 59.3%)] and 3 chronic diseases was 25.5% [95% CI (21.0, 30.4%); the prevalence was 45.3% [95% CI (33.7, 57.4%)] in $<$ 2019 and 41.9% [95% CI (35.1, 49.0%)] in $\geq$ 2019; the prevalence was 74.4% [95% CI (37.6, 93.4%)] in North China and 52.5% [95% CI (33.9, 70.4%)] in East China. **Conclusion**: Current evidence suggests that the prevalence of chronic disease co-morbidity is high among the elderly in China, but there has been a downward trend in recent years, this study differed by sex, co-morbidity type, region, and time. Limited by the quality of included studies, further studies should be performed to confirm our findings.

Keywords: Chronic disease co-morbidity · Prevalence · Elderly · China · Meta-analysis

1 Introduction

As the global disease spectrum changes, chronic disease co-morbidity have become a major threat to human life health and quality of life [1], the elderly are a vulnerable population for chronic diseases and often with higher prevalence. The co-morbidity rate of chronic diseases among the elderly over 65 years of age in China is as high as 70%

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 81–94, 2024.
https://doi.org/10.1007/978-981-99-7161-9_7

[2], the incidence rate increases sharply with age, significantly reducing the health of the elderly, increasing readmission rates and potential social and economic burdens, even increasing the risk of death [3–8], which has become an important public health problem that needs to be addressed globally. It is of great significance to explore the prevalence of chronic disease co-morbidity in the elderly for disease prevention and management. The prevalence of chronic disease co-morbidity has been studied in depth in academia, but the sample size of individual studies is small, most of them are single-center research studies, the results are not representative. In this paper, we collected studies about the prevalence of chronic disease co-morbidity in China aged ≥60 years by searching databases. Meta-analysis was used to quantitatively analyze the prevalence studies to clarify the current status of the prevalence and the influencing factors to provide a basis for strengthening the disease preventive and management.

2 Materials and Methods

2.1 Inclusion Criteria and Exclusion Criteria

Inclusion criteria: (1) Study design: Cross-sectional study; (2) Research subjects: Chronic disease co-morbidity population aged ≥60 years in China; (3) The original literature clearly provides the total sample size and the number of patients; (4) Diagnosis of diseases according to the International Classification of Diseases (ICD-10); (5) Outcome indicators: Prevalence of chronic disease co-morbidity. Exclusion Criteria: (1) Studies for which the full text was not available or incomplete data; (2) Repeated publications; (3) Complications rather than co-morbidity.

2.2 Search Strategy

The databases of PubMed, Web of Science, CNKI, VIP and Wanfang were searched by computer. Single proportion studies on the prevalence of chronic disease co-morbidity among the elderly in China from June 2011 to June 2022. Database searches and manual searches were used and references included in the literature were traced. Search terms included: chronic disease co-morbidity, chronic co-morbidity, multi-morbidity, elderly, older adults, co-morbidity, multiple chronic conditions, chronic disease, chronic illness, comorbidity, China, Chinese.

2.3 Quality Assessment

We used the quality standards of the American Institute for Health Care Quality and Research (AHRQ) on cross-sectional studies for quality scoring [9], The AHRQ consists of 11 items, each item is evaluated by “yes”, “no” and “unclear”, “yes” is 1 point, “no” or “unclear” is 0 points, the scores of each item are added up to the total score (0–11 points), the set scores are 0–4 points for low-quality literature, 5–7 points for medium-quality literature and ≥8 points for high-quality literature.

2.4 Literature Screening and Data Extraction

Two graduate students independently screened the literature, extracted information and cross-checked. In case of disagreement, it is resolved through discussion or negotiation with the 3rd party. First, apparently irrelevant literature was eliminated by reading the title and abstract, followed by further reading of the full text to determine whether to include. Contents include: first author, year of publication, study site, age, sample size, number of patients and prevalence.

2.5 Statistical Methods

Meta-analysis was performed using Mantel-Haensel algorithm to test for Heterogeneity. $Q = \sum_{i=1}^{k} \hat{W}_i \left(\hat{J}_w - \hat{J}_{wi}\right)^2$ The statistic Q follows chi-square distribution with degrees of freedom $k - 1$. We choose k as the number of cross-sectional studies for this study, Wi as the inverse of the standard square of the effect size and Q as the total effect size. When heterogeneity test is statistically different, the heterogeneity index I^2 is further calculated and the random effects model corrected by the Der Simonian and Larird method was chosen.

$$\begin{cases} 0 & Q<K \\ \hat{\tau}^2 = \dfrac{Q-(k-1)\sum\limits_{i=1}^{k} W_i}{\sum\limits_{i=1}^{k} W_i^{2} - \sum\limits_{i=1}^{k} W_i^{2}} & Q>K \end{cases} \tag{1}$$

Weights of each study.

$$w_i^{'} = \frac{1}{SE_i^2 + \hat{\tau}^2} \tag{2}$$

Effect sizes for all studies combined and 95% *CI* (Take the *OR* value as an example).

$$OR_{MH} = \frac{\sum w_i^{'} OR_i}{\sum w_i^{'}} \tag{3}$$

$$95\%\text{CI} = OR_{MH} \pm 1.96 / \sqrt{\sum w_i^{'}}$$

CMA 3.0 software was used to evaluate the funnel plot, Begg's test and Egger's test for publication bias. Sensitivity analysis was used to evaluate the stability and reliability of the analysis results.

3 Results

3.1 Literature Search Results

A total of 2473 literatures, 582 in Chinese and 1891 in English were obtained through preliminary search, after a layer-by-layer screening. 31 literatures were finally included, including 27 Chinese literature and 4 English literatures (Fig. 1).

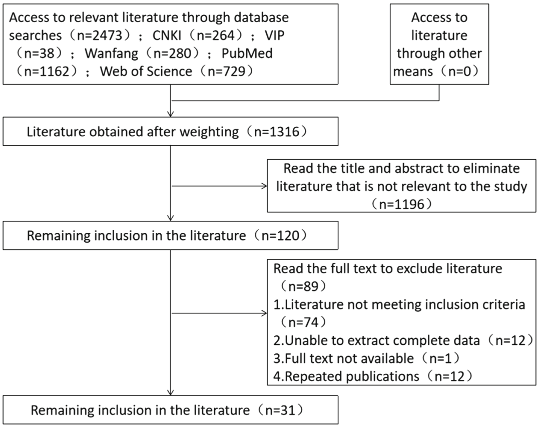

Access to relevant literature through database searches（n=2473）; CNKI（n=264）; VIP（n=38）; Wanfang（n=280）; PubMed（n=1162）; Web of Science（n=729）
Access to literature through other means（n=0）
Literature obtained after weighting（n=1316）
Read the title and abstract to eliminate literature that is not relevant to the study（n=1196）
Remaining inclusion in the literature（n=120）
Read the full text to exclude literature（n=89）
1.Literature not meeting inclusion criteria（n=74）
2.Unable to extract complete data（n=12）
3.Full text not available（n=1）
4.Repeated publications（n=12）
Remaining inclusion in the literature（n=31）

Fig. 1. Literature screening map

3.2 Basic Characteristics and Results of Risk of Bias Evaluation

The basic characteristics of the included studies and the results of the risk of bias evaluation are shown in Tables 1 and 2.

3.3 Results of Meta-Analysis

The 31 included studies were tested for heterogeneity, the results showed $I^2 = 99.87\%$ ($p < 0.01$), so the random-effects model was chosen for Meta-analysis (Fig. 2).

3.4 Subgroup Analysis

Subgroup analysis was performed using gender, type of chronic disease, publication time, and regional distribution as grouping factors, there was high heterogeneity in all subgroups, so a random-effects model was used to combine effect sizes. Subgroup analysis showed that the prevalence of chronic disease co-morbidity was 37.1% (95% CI (29.6, 45.3%)) in men and 39.5% (95% CI (30.4, 49.3%)) in women; the prevalence of 2 chronic diseases was 51.6% [95% CI (43.9, 59.3%)] and 3 chronic diseases was 25.5% [95% CI (21.0, 30.4%); the prevalence was 45.3% [95% CI (33.7%, 57.4%)] in <2019 and 41.9% [95% CI (35.1, 49.0%)] in ≥2019, In addition, the prevalence of chronic disease co-morbidity in different regions was also included (Table 3).

Table 1. Basic characteristics of the included literature

Authors	Year	Area	Age	Sample size (total/men/women)	Number of sick people (total/men/women)	Prevalence (%)
Cao [10]	2021	Henan	≥60	1336/645/691	490/233/257	36.68
Jin [11]	2019	China	60–104	5265/2923/2342	2341/–/–	44.46
Zhang [12]	2019	China	≥60	11707/5705/5993	5107/–/–	43.62
Chen [13]	2018	Chengdu	60–104	1970/839/1131	354/–/–	18
Chen [14]	2011	Beijing	72–92	160/150/10	139/–/–	86.88
Zhang [15]	2019	China	≥60	23718/10533/13185	13097/5250/7847	55.22
Fan [16]	2022	Henan	≥60	5570/2745/2825	1210/546/664	21.72
Chen [17]	2022	Jiangsu	≥90	172/125/47	156/115/41	90.7
Hua [18]	2021	Shanghai	≥60	68147/–/–	43953/17892/26061	64.5
Li [19]	2021	Guizhou	≥60	263/122/141	56/28/28	78.71
Xiao et al. [20]	2019	Yunnan	≥60	4833/2198/2635	776/334/442	16.1
Hou [21]	2020	Wuhan	≥65	622/264/358	317/120/197	50.96
Hu [22]	2020	Sichuan	≥60	1358/970/388	211/–/–	15.54
Li [23]	2021	China	≥60	10836/5288/5548	7059/3247/3812	65.14
Li [24]	2020	Henan	≥60	6094/2931/3163	770/369/401	12.64

(*continued*)

Table 1. (*continued*)

Authors	Year	Area	Age	Sample size (total/men/women)	Number of sick people (total/men/women)	Prevalence (%)
Lin [25]	2016	Shenzhen, Dongguan, Foshan	≥60	4281/2014/2267	1672/781/891	39.06
Liu [26]	2022	Guangdong	≥60	469/236/233	205/97/108	43.7
Sun [27]	2022	China	≥60	7062/3125/3937	1232/–/–	17.4
Zhang [28]	2020	Nanjing	≥60	2222/1099/1123	1021/530/491	45.9
Wang [29]	2020	Xinjiang	≥60	720/331/389	333/125/208	46.25
Wang [30]	2017	Shanghai	≥65	19185/8164/11021	4271/1747/2524	22.26
Yao [31]	2022	Zhengzhou	≥60	2506/1041/1465	566/271/295	22.6
Wang [32]	2018	Shenzhen	≥60	2705/1131/1574	1335/–/–	49.4
Wu [33]	2020	Jiangsu	≥65	523/–/–	228/–/–	43.59
Xu [34]	2021	China	≥60	9936/4896/5040	4563/2103/2460	45.92
Yan [35]	2019	China	≥60	11698/5705/5993	5106/2327/2779	43.65
Wang [36]	2016	Beijing	65–98	1187/561/626	676/–/–	56.95
Wang [37]	2018	Shenzhen	≥60	2603/1096/1507	1173/–/–	45.06
Su [38]	2016	Shanghai	≥80	2058/867/1191	1012/–/–	49.17
You [39]	2019	Zhejiang, Jiangsu	≥60	5296/2609/2687	2201/–/–	41.56
Zhang [40]	2019	China	60–107	11707/5705/6002	5107/–/–	43.62

Table 2. Results of the risk of bias evaluation of the included studies

Authors	1	2	3	4	5	6	7	8	9	10	11	Score
Cao [10]	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	9
Jin [11]	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	No	8
Zhang [12]	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	No	8
Chen [13]	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	9
Chen [14]	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	No	8
Zhang [15]	Yes	Yes	Yes	Yes	No	Yes	No	No	Yes	Yes	No	7
Fan [16]	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	8
Chen [17]	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	8
Hua [18]	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	No	7
Li [19]	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	No	8
Lii [20]	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	No	7
Hou [21]	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	9
Hu [22]	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	8
Li [23]	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	9
Li [24]	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	No	7
Lin [25]	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	9
Liu [26]	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	No	8

(*continued*)

Table 2. (*continued*)

Authors	1	2	3	4	5	6	7	8	9	10	11	Score
Sun [27]	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	No	8
Zhang [28]	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	8
Wang [29]	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	9
Wang [30]	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	No	7
Yao [31]	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	8
Wang [32]	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	9
Wu [33]	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	No	8
Xu [34]	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	No	8
Yan [35]	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	No	8
Wang [36]	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	9
Wang [37]	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	9
Su [38]	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	8
You [39]	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	8
Zhang [40]	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	8

Notes 1 is a clear source of information; 2 is a list of inclusion and exclusion criteria for the exposed and unexposed groups or reference to previous publications; 3 is given to identify the time stage of the patient; 4 is whether the study population is continuous if it is not a population source; 5 is that the subjective element of the evaluator overshadows other aspects of the subject of the study; 6 is a description of any assessment undertaken for quality assurance; 7 is an explanation of the rationale for excluding any patient from the analysis; 8 is a description of how measures to evaluate and/or control confounding factors; 9 is an explanation of how missing data is handled in the analysis, if possible; 10 is a summary of patient response rates and the completeness of data collection; 11 is to identify the percentage of patients with incomplete data expected or the outcome of the follow-up, if any

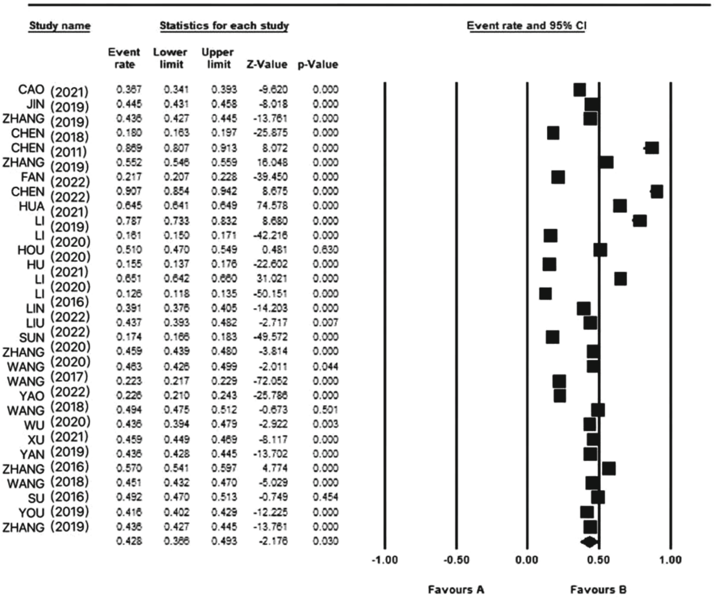


Fig. 2. Forest plot of the total prevalence

3.5 Sensitivity Analysis

Sensitivity analysis was performed using a literature-by-literature exclusion method. The study results did not change significantly before and after excluding literature, the findings of this study were more stable.

3.6 Publication Bias Analysis

The results of the funnel plot show that the symmetry of the distribution of the left and right points of each study is poor, however, the p-values of Egger's and Begg's tests were 0.063 and 0.126, suggesting a low likelihood of publication bias (Fig. 3).

Table 3. Subgroup analysis

Subgroup	Number of studies	Heterogeneity test		Model	Prevalence (95%CI) (%)
		I^2 (%)	P		
Gender					
Male	17	99.6	<0.001	Random	37.1 (29.6,45.3)
Female	17	99.8	<0.001	Random	39.5 (30.4,49.3)
Types of chronic diseases					
2	22	99.7	<0.001	Random	51.6 (43.9,59.3)
3	13	99.4	<0.001	Random	25.5 (21.0,30.4)
≥3	11	99.5	<0.001	Random	41.9 (30.9,53.9)
≥4	11	98.8	<0.001	Random	24.6 (20.5,29.2)
Area distribution					
North China	2	97.8	<0.001	Random	74.4 (37.6,93.4)
East China	7	99.9	<0.001	Random	52.5 (33.9,70.4)
South China	4	96.0	<0.001	Random	44.3 (39.2,49.5)
Central China	5	99.4	<0.001	Random	27.0 (17.6,39.0)
South West	4	99.2	<0.001	Random	28.7 (16.5,45.2)
China	8	99.8	<0.001	Random	44.2 (36.2,52.5)
Publish time					
<2019	8	99.7	<0.001	Random	45.3 (33.7,57.4)
≥2019	23	99.9	<0.001	Random	41.9 (35.1,49.0)

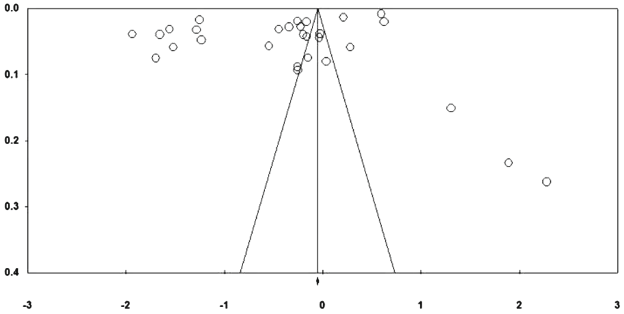


Fig. 3. Publication bias funnel plot

4 Conclusion

With the accelerated aging of the global population, the increase in life expectancy and the widespread prevalence of risk factors, the base of patients with chronic disease co-morbidity in China is gradually increasing [41–43], many problems caused by co-morbidity are posing a great challenge to the development of the economy and society. Previous studies were mainly limited to small sample surveys with poorly representative outcomes. A total of 31 cross-sectional studies involving 226209 patients were included in this paper, with literature quality scores ranging from 7 to 9, indicating that the quality of the included studies was moderate and above. Individual studies were excluded one by one for sensitivity analysis. Egger's and Begg's tests were performed to verify publication bias. Meta-analysis showed that the prevalence of chronic disease co-morbidity among the elderly in China was 42.8% [95% CI (36.6, 49.3%)],the prevalence was lower than in Switzerland [44] and the United States [45] and higher than in Italy [46] and Indonesia [47], which may be related to differences in geography, economic conditions, study setting and sample size. In order to study the true variability of co-morbidity, more in-depth studies are needed in China in the future. The prevalence is still at a high level, which may be related to the Chinese people's health level, while the elderly have poorer physical resistance compared to younger people and poor lifestyle habits such as excessive smoking and alcohol consumption and lack of exercise can lead to the occurrence of chronic disease co-morbidity [48].

The prevalence of co-morbidity was higher in women (39.5%) than in men (37.1%), which is consistent with the results of previous studies and may be related to the higher life expectancy and longer exposure to risk factors in women than in men [49], so women should pay more attention to their chronic disease co-morbidity status [48] and enhance their self-management awareness. Subgroup analysis of different chronic disease categories showed that the prevalence of 2 chronic diseases (51.6%) was higher than the prevalence of 3 chronic diseases (25.5%), the prevalence ≥3 chronic diseases was 41.9%, and the prevalence ≥4 chronic diseases was 24.6%.The results of subgroup analysis in different regions showed that the prevalence was highest in northern China (74.4%), followed by eastern China (52.5%), which may be related to the different dietary habits and lifestyles in each region. Subgroup analysis of different publication times showed a higher prevalence of chronic disease co-morbidity in <2019 (45.3%) than in ≥2019 (42.7%). In recent years, the problem of co-morbidity has attracted national attention and people's awareness of co-morbidity has gradually increased, changing bad habits and lifestyles can reduce the occurrence of disease.

This study also has some limitations: (1) There may be publication bias due to under-inclusion of literature. (2) Limited by the characteristics of individual rate Meta-analysis, there was high heterogeneity among the included literature, although subgroup analysis was conducted by gender, type of chronic disease, region, and time, it still could not reduce the heterogeneity, which may have affected the accuracy of the results. (3) The included studies were cross-sectional studies, selection and measurement biases were inevitable due to the limitations of the study design.

In summary, the prevalence of chronic disease co-morbidity among the elderly in China was 42.8%, with a higher prevalence among women than men. The above findings need to be confirmed by additional high-quality studies, influenced by the quality and number of included studies.

References

1. Chen, Y., Li, H., et al.: Development and challenge of monitoring chronic diseases and risk factors in China. Chin. J. Prev. Med. **46**(5), 389–391 (2012)
2. Held, F.P., Blyth, F., Gnjidic, D., et al.: Association rules analysis of comorbidity and multimorbidity: the concord health and aging in men project. J. Gerontol. A Biol. Sci. Med. Sci. **71**(5), 217–223 (2015)
3. Yiping, W., Yanlin, H., et al.: Research progress of chronic comorbidity treatment burden in maintenance hemodialysis patients. Nurs. Res. **36**(17), 3085–3090 (2022)
4. Williams, J.S., Egede, L.E.: The association between multimorbidity and quality of life, health status and functional disability. Am. J. Med. Sci. **352**(1), 45–52 (2016)
5. Mcphail, S.M.: Multimorbidity in chronic disease: impact on health care resources and costs. Risk Manag. Healthc. P **9**(30), 143–156 (2016)
6. Zhang, L., Li, Y., et al.: Current status and research progress of senile comorbidities. Chin. J. Senile Multiorgan Dis. **20**(1), 67–71 (2021)
7. Wang, Y., Chen, X., et al.: A cohort study on the relationship between morbidity and mortality in elderly people in community. Chin. J. Chronic Dis. Prev. Control **28**(9), 649–652, 658 (2020)
8. Navickas, R., Petric, V.K., Feigl, A.B., et al.: Multimorbidity: what do we know? what should we do? J. Comorb. **6**(1), 4–11 (2016)
9. Zeng, X., Liu, H., et al.: Meta-analysis series 4: quality assessment tool for observational studies. Chin. J. Evid. Based Cardiovasc. Med. **4**(4), 297–299 (2012)
10. Cao, M., Li, Y., et al.: Investigation on the status of chronic diseases and comorbidities among the elderly in hospitals and nursing institutions in Henan Province. J. Zhengzhou Univ. (Med. Sci.) **56**(6), 800–804 (2021)
11. Jin, X., Lu, Y.: Study on comorbidities of the elderly in China and its impact on health care expenditure. Chin. J. Gen. Pract. **22**(34), 4166–4172 (2019)
12. Zhang, R., Lu, Y., et al.: Analysis on the pattern and correlation of chronic disease comorbidities in the elderly in China. Chin. J. Publ. Health **35**(08), 1003–1005 (2019)
13. Chen, J., Yang, X., et al.: Analysis on the status and comorbidity of chronic diseases in elderly residents in Xindu District of Chengdu. Chin. J. Publ. Health Adm. **35**(08), 573–575+615 (2018)

14. Chen, J., Du, W., et al.: The preliminary research on the relationship between common disease and cognitive function in the elderly. China Clin. Health J. **14**(061), 566–568 (2014)
15. Zhang, H., Qi, S., et al.: Status of common chronic diseases comorbidized elderly in six provinces and cities in 2015. Cap. Publ. Health **13**(03), 122–125 (2019)
16. Fan, X., Chen, M., et al.: Study on the influence of chronic disease comorbidity on social interaction ability of the elderly in Henan Province. Med. Soc. **35**(05), 55–59 (2021)
17. Chen, Y., Yang, X., et al.: Investigation on chronic diseases and comorbidity of long-lived elderly people. Chin. J. Geriatr. Multi-Organ Dis. **21**(02), 86–90 (2021)
18. Hua, M., Jin, H., et al.: Analysis of disease types and characteristics of elderly patients with multiple diseases in Jing' an District of Shanghai. Chin. J. Gen. Pract. **20**(08), 838–844 (2011)
19. Li, Z., Lin, X., et al.: Epidemiological survey of chronic disease comorbity among Yao Ethnic Group in Guizhou. J. Qiannan Ethnic Med. College **34**(1), 33–35 (2021)
20. Xiao, L., Cai, L., et al.: Prevalence of five common chronic diseases and their comorbidities and their relationship with socioeconomic status in rural elderly in Yunnan Province. Chin. J. Dis. Control **23**(06), 630–634 (2019)
21. Hou, Y., Jiang, D., et al.: Analysis of chronic disease comorbidity and its influencing factors among the elderly in Wuhan. Publ. Healthy China **36**(11), 1604–1607 (2020)
22. Hu, H., Liu, M., Tian, X.B.: Investigation of comorbity rate and its relationship with depression in aged people aged 60 and above. J. Prev. Med. Inf. 20, **36**(10), 1291–1295
23. Li, Y., Wang, Y.: Study on the status and mode of chronic disease comorbidities in the elderly in China. Chin. J. Gen. Med. 201, **24**(31), 3955–3962+3978
24. Li, Y., Li, Y., et al.: Analysis of common chronic diseases in the elderly in Henan Province Modern Prev. Med. **47**(15), 2797–2800 (2020)
25. Lin, W.: Study on the status and mode of chronic disease comorbidity in the elderly in Pearl River Delta. Guangzhou Medical University (2016)
26. Liu, G., Xue, Y.: Study on the status and influencing factors of chronic disease comorbidities in the elderly in Guangdong Province. Chin. J. Hosp. Stat. 202, **29**(02), 103–107
27. Sun, D., Huang, R., et al.: Effects of chronic disease comorbidities on health status of the elderly in China. J. Wuhan Univ. (Med.) 202, **43**(02), 302–306
28. Zhang, Q., Jin, L., et al.: Status and influencing factors of chronic disease comorbidities in the elderly in Xuanwu District of Nanjing. Occup. Health, 20, **36**(11), 1496–1499
29. Wang, J., Fan, Q., et al.: Analysis on the status quo of chronic disease comorbiditis of elderly farmers and herdsmen in Nanshan Pasturing area of Xinjiang. Modern Prev. Med. 20, **47**(17), 3088–3091
30. Wang, J., Zhang, Z., et al.: Analysis of patterns and influencing factors of comorbity among elderly people in some communities in Shanghai. Geriatr. Med. Health Care **23**(02), 97–101 (2017)
31. Yao, Y., Hu, Q., et al.: Analysis of common chronic diseases in the elderly in Guancheng Hui District of Zhengzhou. J. Henan Med. Res. **31**(11), 1930–1933 (2022)
32. Wang, X.: Study on comorbidities of chronic diseases and their effects on functional status of elderly people in community. Henan University (2018)
33. Wu, T., Lu, Y., et al.: Study on the prevalence of senile comorbidities and health-related quality of life in Jiangsu Province: based on the measurement of utility value of EQ-5D scale. Chin. Gen. Pract. (2020)
34. Xu, X., Li, D., et al.: Analysis of chronic disease comorbidities in Chinese elderly based on association rules. Prev. Control Chronic Dis. China 201, **29**(11), 808–812
35. Yan, W., Lu, Y., et al.: Current status of comorbity in elderly people based on CHARLS data analysis. Chin. J. Dis. Control **23**(04), 426–430 (2019)
36. Zhang, K.: Investigation and analysis of chronic disease and geriatric syndrome in some communities of the elderly in Beijing. Med. Health Sci. Technol. (2017)

37. Wang, X.X., Chen, Z.B., Chen, X.J., et al.: Functional status and annual hospitalization in multimorbid and non-multimorbid older adults: a cross-sectional study in southern China. **16**(1), 33 (2018)
38. Su, P., Ding, H.S., Zhang, W., et al.: The association of multimorbidity and disability in a community-based sample of elderly aged 80 or older in Shanghai, China. BMC Geriatr. **16**(1), 178 (2016)
39. You, L., Yu, Z., Zhang, X., et al.: Association between multimorbidity and depressive symptom among community-dwelling elders in eastern China. Clin. Interv. Aging **14**, 2273–2280 (2019)
40. Zhang, R., Lu, Y., Shi, L.Y., et al.: Prevalence and patterns of multimorbidity among the elderly in China: a cross-sectional study using national survey data. BMJ Open **9**(8), e024268 (2019)
41. Palladino, R., Pennino, F., Finbarr, M., et al.: Multimorbidity and health outcomes in older adults in ten European health systems 2006–15. Heal. Aff. Proj. Hope **38**(4), 613–623 (2019)
42. National Health Commission, Bureau of Disease Control and Prevention. Report on Nutrition and Chronic Diseases in China (2020). People's Medical Publishing House, Beijing (2021)
43. Yan, J., Lu, Y.: Enlightenment of British comorbidities management policy to China. Modern Comm. Trade Ind. **39**(6), 66–68 (2018)
44. Anindya, K., Ng, N., Atun, R., et al.: Effect of multimorbidity on utilisation and out-of-pocket expenditure in Indonesia: quantile regression analysis. BMC Health Serv. Res. **21**(1), 427 (2021)
45. Baehler, C., Huber, C.A., Bruengger, B., et al.: Multimorbidity, health care utilization and costs in an elderly community-dwelling population: a claims data based observational study. BMC Health Serv. Res. **15**, 23 (2015)
46. Gupta, S.: Burden of multiple chronic conditions in Delaware, 2011–2014. Prev. Chronic Dis. **13**, e160 (2016)
47. Menotti, A., Mulder, I., Nissinen, A., et al.: Prevalence of morbidity and multimorbidity in elderly male populations and their impact on 10 year all cause mortality: the FINE study (Finland, Italy, Netherlads, Elderly). J. Clin. Epidemiol. **54**(7), 680–686 (2001)
48. Wang, M., Zhou, X., et al.: Meta-analysis of the prevalence of chronic disease comorbidities among middle-aged and elderly people in China from 2010 to 2019. Chin. J. Gen. Pract. 201, **24**(16), 2085–2091
49. Wang, H., Zhang, L., et al.: Study on the status and spatial distribution of chronic disease comorbidities in middle-aged and elderly people in China. Chin. J. Gen. Pract. **25**(10), 1186–1190, 1196 (2022)

Overview of Non-Fungible Token Eco-Regulation, Traceability and Data Right Confirmation Security

Zixuan Liu[1,3], Haoyu Gao[1,3], Hong Lei[1,2](✉), Chuan Liu[1,3], and Chao Liu[4]

[1] Hainan University, Haikou 570228, China
zixuan@hainanu.edu.cn, haoyu@ssc-hn.com, leiluono1@163.com
[2] SSC Holding Company Ltd, Chengmai 571924, China
[3] Oxford-Hainan Blockchain Research Institute, Chengmai 571924, China
[4] The Blockhouse Technology Limited, Oxford OX2 6XJ, UK
liuchao@tbtl.com

Abstract. As a new technology, Non-Fungible Token (NFT) has sparked a surge in asset digitization. NFT, which is unique, irreplaceable, and indivisible, can be used for investment, traceability, data storage, and so on. However, the application of NFT is not solid—risks such as wash trading and broken links abound, and data cannot be confirmed. In response to the aforementioned issues, previous authors proposed some policy solutions; however, few academic studies on NFT risks have been published. First, this paper examines the current transaction risks of the NFT ecology before proposing a regulatory approach to financial market fraud. Then we investigate two common applications of NFT—supply chain traceability and data right confirmation—and propose methods to improve security based on existing research risks. Finally, we summarize the work of this paper and provide an outlook on NFT. To the best of our knowledge, we have conducted the first exploration of NFT ecological regulation approaches, as well as studied the security risks of two major application scenarios: traceability and data right confirmation.

Keywords: NFT ecological regulation · NFT traceability · NFT data right confirmation · Non-fungible token

1 Introduction

With the rise of blockchain in recent years, questions about digital object ownership and usage have arisen. Purchasers of digital goods are only users, not owners, under the rules of intellectual property licensing and online contracts designed by the Internet in the 21st century [1]. The emergence of Non-Fungible Token (NFT), which uses distributed technology to confirm rights, has changed this.

Digital collections were one of the first applications of NFT technology. Because of the ease of demonstrating NFT ownership and the climbing mentality of most people, the NFT trading market is exceptionally hot. The total global market value of NFTs was approximately $12 billion in November 2022 [2]. The massive trading market poses

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 95–109, 2024.
https://doi.org/10.1007/978-981-99-7161-9_8

regulatory challenges; illegal transactions involving NFTs have been staged secretly and quietly around the world. NFTs' unique and traceable nature allows them to demonstrate advantages in terms of traceability and data right confirmation in addition to financial transactions. While academic research on using NFT to solve various problems has been conducted, the application of NFT is not solid, such as the problem of broken links for off-chain data reading, the authenticity of NFT corresponding to physical asset traceability, and access control of NFT data storage. Despite the fact that the NFT market is booming, few academic studies have been published to address the aforementioned issues.

In summary, the main contributions of this article can be listed as follows.

- The current research on NFT is more concerned with digital art and the economic benefits of NFT; however, this paper aims to analyze the financial risks in the current NFT ecology and propose a regulatory approach as well as policy solutions from the perspectives of cryptography and data analysis.
- This paper summarizes the history of the NFT supply chain, investigates the broken link problem and data access control in the traceability process, and provides security strategies in response.
- This study examines the application scenarios of NFT data right confirmation, examines the potential risks encountered from the standpoint of copyright protection, and provides relevant risk mitigation recommendations.

The remainder of this paper is organized as follows. Section 2 discusses the relevant theoretical background of NFT. Section 3 introduces the NFT ecology and outlines the financial regulation process. Section 4 discusses NFT traceability and risk avoidance methods. The methods of NFT data corroboration and risk avoidance are then investigated in Sect. 5. Finally, Sect. 6 summarizes the work of this paper, analyzes the current challenges confronting NFT, and provides an outlook.

2 Background

2.1 Theoretical Basis

Several technical elements, including blockchain and smart contracts, are required for the practical implementation of NFT.

Blockchain is a decentralized, distributed database that records transactions or other information efficiently between two or more parties [3]. The two main features of blockchain are decentralization and the difficulty of tampering with data. Based on these two features, the data stored by the blockchain is more trustworthy and authentic, which can aid in resolving the issue of mutual mistrust [4].

Ethereum is a new open blockchain public chain platform that allows anyone to build and use decentralized applications that run on the platform using blockchain technology [5]. Ethereum has Turing completeness, which enables the smart contract mechanism. Smart contracts are programs that are stored on the blockchain and run when certain conditions are met. The data on the blockchain is transparent and tamper-proof, and it can run indefinitely.

Smart contracts provide transparency and efficiency because there is no third party involved and the cryptographic records of transactions are shared among the participants. The NFT principle, on the other hand, is to choose a blockchain for the development of a smart contract and to extend the NFT properties based on various underlying criteria. The structure of the NFT smart contract based on the ERC-721 standard is depicted in Fig. 1.

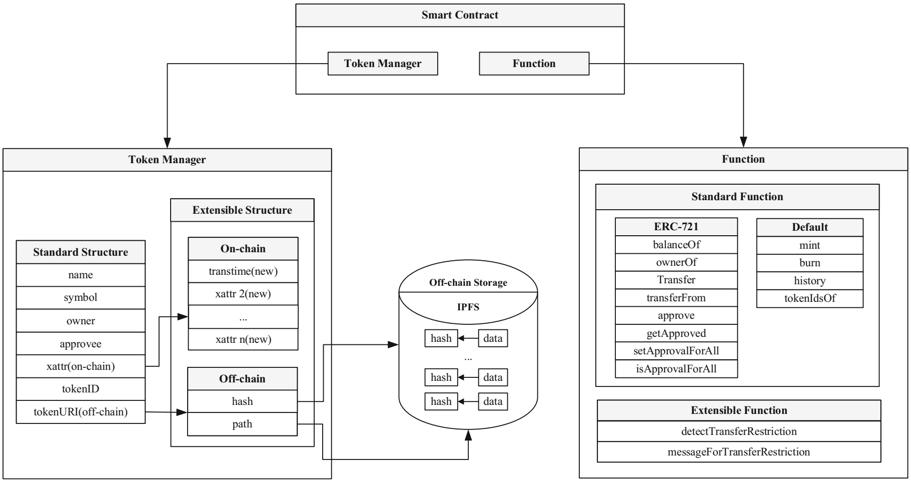


Fig. 1. The structure of the NFT smart contract based on the ERC-721 standard.

2.2 NFT Introduction

NFT is also known as "Non-Fungible Token" and it is used to identify unique items. It also has the characteristics of non-exchangeability and non-separability [6], which distinguish it from Fungible Token (FT). Transactions require a single smart contract invocation and are primarily developed and exchanged using three underlying standard protocols: ERC-721 [7], ERC-1155, and ERC-998.

ERC-721 was the first standard for non-homogeneous digital assets and is now the most commonly used password format in ecological scenarios. The ERC-721 protocol is used as the underlying protocol by the once popular crypto cat "CryptoKitties" [8]. The ERC-721 protocol specifies four types of NFT metadata: global ID, NAME, SYMBOL, and Uniform Resource Identifier (URI). The tracking and transfer of items can be quickly implemented using the ERC-721 protocol, and the trajectory can be recorded on the chain [6].

ERC-1155 extends ERC-721 to allow the issuance of any type of NFT asset in a single contract; the ID is now a class rather than an item. Sending smart contracts based on a class can achieve a large number of multi-class asset transfers, etc., at the same time, which significantly improves transfer speed and can also meet the flexible application requirements in different scenarios [9].

ERC-998 stands for Composable NFTs (CNFT), and the underlying protocol standard is designed to contain multiple ERC-721 and ERC-20 token forms. When this underlying protocol standard is used to generate tokens, a single transfer can package all different types of tokens. The comparison of these three standards is shown in Table 1.

Table 1. The comparison of ERC-721, ERC-1155 and ERC-998.

Name	Standard	Applicable platforms	Transfer efficiency	Gas	Degree of decentralization	Degree of information loss	Frequency of use
Non-Fungible Token (NFT)	ERC-721	Ethereum	Low	Low	High	Low	High
Semi-Fungible Token (SFT)	ERC-1155	Ethereum and others	Medium	Medium	Medium	Medium	Medium
Composable NFTs (CNFT)	ERC-998	Ethereum and others	High	High	Low	High	Medium

2.3 NFT Categories

As shown in Table 2, NFT can be divided into three categories: the first is the digital identity of the entity, which encrypts the existing physical items; blockchain technology can ensure that it will not be tampered with or copied in the process of buying, selling, and collecting; and the NFT of the goods can be queried to confirm the authenticity of the goods by the complete production history record of the goods and the relevant certificates. The second category is the digitized form of physical items on the chain, which is equivalent to physical item derivatives and traditional art work digitization. The third category includes the use of NFT and other blockchain technologies to create native digital artworks [10], which are virtual products created with blockchain and smart contract technologies and are commonly found in blockchain games [11].

The inherently immutable, indivisible, and irreplaceable nature of NFT remains unchanged regardless of the form of presentation. This is why NFT is commonly used to chain traditional artworks: to solve the problem of traceability, a robust, decentralized digital art market infrastructure is used. While NFT is currently being researched in the financial sector, NFT applications are also applicable to other areas such as global authentication, supply chains, data sharing, data trust, access control, and creating incentives for NFT creators.

2.4 NFT Workflow

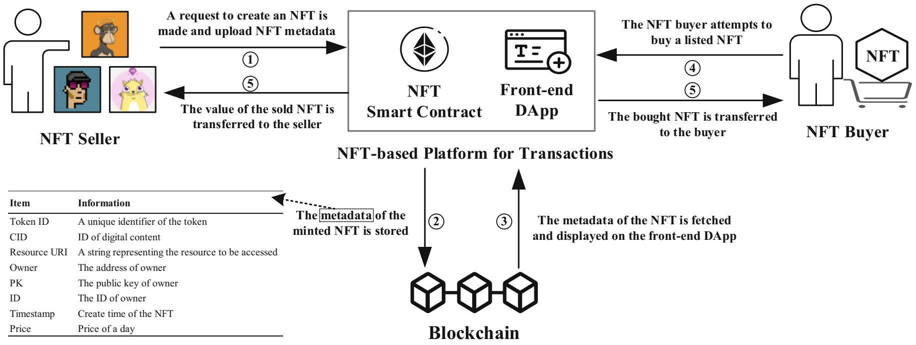
To create an NFT, you must first create a digital wallet in which the NFT will be stored. There are numerous wallets available, including MetaMask, Trust Wallet, Phantom, Coinbase, and others. A private key, which will be used to access the wallet, must also be created.

Figure 2 depicts the NFT minting, uploading, and trading workflow. The seller must first create a marketplace account that supports NFT, and then connect the wallet to the

Table 2. NFT categories and attributes.

NFT categories	Physical subject matter	Value added	Commodity anti-counterfeiting	Traceability
Digital identification of entities	√	×	√	√
Entities in digital form on the chain	√	√	×	√
Virtual blockchain products	×	√	×	√

marketplace account and send a request to mint NFT before uploading the digital file of NFT. It is critical to note that the NFT description, which is called “metadata” as shown in Fig. 2, must be provided when uploading the file. For NFT minting, the seller chooses a marketplace-supported blockchain. Minting is the process of creating a new NFT using the NFT smart contract and listing it at a price determined by the seller. Any interested buyer will be able to view the listed product and attempt to purchase it via the front-end Decentralized Application (DApp). Finally, if the transaction is completed successfully, the NFT will be transferred to the buyer, and the seller will receive revenue.


A request to create an NFT is made and upload NFT metadata
①
⑤
The value of the sold NFT is transferred to the seller
NFT Seller
NFT Smart Contract
Front-end DApp
NFT-based Platform for Transactions
The NFT buyer attempts to buy a listed NFT
④
⑤
The bought NFT is transferred to the buyer
NFT
NFT Buyer
The metadata of the minted NFT is stored
②
③
The metadata of the NFT is fetched and displayed on the front-end DApp
Blockchain

Item	Information
Token ID	A unique identifier of the token
CID	ID of digital content
Resource URI	A string representing the resource to be accessed
Owner	The address of owner
PK	The public key of owner
ID	The ID of owner
Timestamp	Create time of the NFT
Price	Price of a day

Fig. 2. The workflow of NFT minting, uploading, and trading.

3 NFT Ecology and Regulation

With the wave of digitization, NFT, particularly the digital copyright value of artworks, is rising. Sun et al. assetize physical objects on the chain using smart contracts and automatic safe deposit boxes, achieving a strong binding of physical assets off-chain with virtual assets on-chain [12]. Yatipa et al. provide technical details for implementing NFT based on the ERC-1155 standard because assets must be broken down into small, risk-parity parts for resale [13]. However, current NFTs use consensus that is mostly dominated by Proof-of-Work (PoW) algorithms, which waste a lot of resources. Dan et al. proposed environmental smart contracts, a new type of NFT smart contract, to address the ethical quandary faced by environmentally conscious digital artists [14].

3.1 Market Transaction Risk

Financial attacks through market manipulation are possible due to the centralized management of exchanges, opaque trading processes, and transparency of the blockchain. Due to the fact that bids are visible to other network participants, attackers can offer higher prices, allowing malicious transactions to be executed before the victim trades. This is referred to as “frontrunning” [15]. The authors of Flashboys demonstrate how arbitrage bots can generate a small amount of revenue by front-loading trades on Decentralized Exchanges (DEX) [16]. By applying both front and back office to the victim’s trades, the Sandwich Attack increases the risk of arbitrage. Zhou et al. calculated the likelihood of carrying out such an attack as well as the potential profit [17]. In fact, a 21-year paper reported a staggering $28.8 million in blockchain profits extracted in just two years using leveraged entrapment, clearing, and arbitrage [18].

3.2 Financial Fraud Regulation

The pseudo-anonymity of NFT, as well as the unpredictability of its market capitalization, increase its potential for use in money laundering. The Ethereum platform is currently used for the majority of NFT transactions, but it only provides pseudo-anonymity, not strict anonymity or privacy. Users can only partially hide their identity, but if the public knows the link between their true identity and the corresponding address, they can directly observe all of the user’s activities under that address. Furthermore, because the foundation of NFT is a token, “virtual currency” or “virtual currency derivatives” the associated crowdfunding project is likely to be considered illegal crowdfunding. NFT carries the risk of illegal fund raising, as well as fund raising fraud. Victims can also fall victim to simple social engineering scams by investing NFT in bogus state trust funds [19].

Platform venues that cast or auction NFT transactions are currently in charge of NFT transaction regulation. Do a good job of Know Your Client (KYC) and have strict control over customer real-name authentication; complete a good anti-money laundering strategy or purchase some anti-money laundering outsourcing technology; do a good job of reporting to the net messaging or net security department in a timely manner, report NFT online products, and send reports to regulators on a regular basis [20]. Meanwhile, complex encryption principles and security assumptions, such as the existing homomorphic encryption, zero proof of knowledge, ring signatures, and multi-party computation, can improve the security of financial transactions. A qualified security company can conduct a security audit before the project goes live. A whitelist mechanism is established during project operations to restrict NFT transactions.

The first study on market dynamics and security issues in the NFT financial ecosystem was conducted by Nicola et al. In the case of Wash Trading, the primary goal of the traders is to increase the NFT pool’s sales volume in order to create a false boom in NFT [21]. Brunet et al. identify NFT owners and track their transaction flows using network topology and transaction-following features [22]. Oleg et al. offer the concept of “embedded regulation” where the regulatory approach can be included into Decentralized Finance (DeFi), decreasing the complexity and expense of using DeFi software for consumers [23]. We think that Oleg et al.’s method may be applied to the NFT transaction process (Table 3).

Table 3. Summary of NFT ecological safety regulatory approach.

Policies and regulations	(a) Strict controls on the real name authentication of customers; (b) Anti-money laundering strategies or outsourcing techniques; (c) NFT product reporting to cyber trust or cyber security authorities; (d) Sending reports to regulators on a regular basis

Cryptography	(a) Homomorphic encryption;
	(b) Zero-knowledge proofs;
	(c) Ring signatures;
	(d) Multi-party computation;
	(e) Security audits prior to project implementation;
	(f) Whitelisting mechanism during project operation

Transaction data analysis	(a) Nicola et al. proposed features for wash trading transactions [21]; (b) Brunet et al. use network topology and transaction-following features to identify NFT owners and track their transaction flows [22]; (c) Oleg et al. propose "embedded supervision" with supervision methods built into DeFi [23]

4 NFT Traceability Applications and Risk Avoidance

Growing consumer awareness and internal quality requirements at manufacturers have created a new demand for supply chain traceability. Customers who buy food are willing to buy more and pay higher prices if they can establish a source for the product [24]. When multiple parties are involved, existing centralized solutions are plagued by data silos and a lack of trust. The primary goal of implementing traceability systems is to increase customer confidence in the delivered product. Blockchain technology and NFT combine to provide common characteristics such as decentralization, verifiability, uniqueness, and non-fungibility, which are thought to improve data traceability [25–28].

4.1 NFT Supply Chain Traceability Investigation

Figure 3 depicts current blockchain-based supply chain traceability solutions that enable multi-level tracking of goods through the use of tags like RFID and QR codes [29]. Such linkage mechanisms are commonly found in post-retail supply chains [30] or can demonstrate the counterfeit origin of high-value goods such as diamonds and pharmaceuticals [31]. However, because they do not consider the manufacturing process, these methods are limited to goods that have already been processed—that is, they cannot be traced while the product is being processed, nor can they trace the production chain of the end product and its main components.

Chronicled, a technology company that released an improvement to the network that allows users to verify the authenticity of healthcare products using a blockchain-based private chain, proposed the traceability solution [32]. Sadri et al. [33] propose a solution to the problem of poor visibility in the blood donation supply chain in order to trace data in the blood donation supply chain. However, neither of the two preceding solutions systematically models supply chain traceability. Martin et al. propose a blockchain-based supply chain management system based on the timber sales process, in which

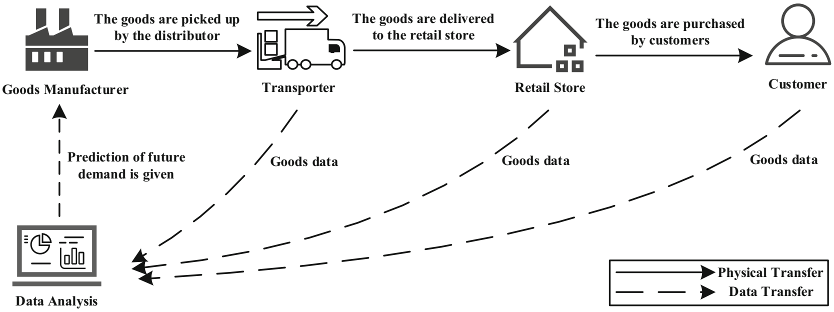

The goods are picked up by the distributor
The goods are delivered to the retail store
The goods are purchased by customers
Goods Manufacturer
Transporter
Retail Store
Customer
Prediction of future demand is given
Goods data
Goods data
Goods data
Data Analysis
Physical Transfer
Data Transfer

Fig. 3. Flow showing typical supply chain.

the product components are projected as NFTs onto the blockchain and smart contracts are used to track the goods, including their transformation during the manufacturing process [6]. This mechanism ensures supply chain transparency and easy-to-understand production data. The solution can serve as the foundation for a blockchain-based supply chain management system, but it needs to be expanded to cover realistic issues like payment for goods, goods loss, and goods ownership.

In response to the aforementioned challenges, Noura et al. proposed a solution in their supply chain work for fine jewelry NFT, in which the participating entities are divided into four categories: jewelry certificate authorities, jewelry retail stores, courier services, and customers [34]. On Ethereum, three smart contracts are created: the ERC-721 smart contract, which predefines the casting and management of NFTs; the bidding smart contract, which finds the highest bidder in the auction and announces the result of the bid; and the physical delivery smart contract, which ensures secure and reliable package delivery. The Certificate Authority evaluates the jewelry, generates the jewelry NFTs, and grants the jeweler ownership. Once a jewelry retailer or customer purchases the physical twin of a jewelry NFT, ownership of the jewelry NFT is transferred according to the ERC-721 standard.

4.2 NFT Traceability Risk and Avoidance

Through the use of NFT, the supply chain management system ensures the authenticity and dependability of the traceability process. It is critical that the information sources be trustworthy in order to improve the reliability of traceability. To address the issue of NFT source trust, Haya et al. incorporate registration, reputation, and incentives into the NFT ecosystem. However, there is a risk of data leakage as well as unreadability in the process of data traceability [35].

The Broken Link Problem. The Broken Link Problem is a fundamental flaw in existing blockchain NFT representations [36]. Because NFT files are frequently too large and the cost of on-chain gas storage is prohibitively expensive, NFT-linked hashes are provided in smart contracts. However, these off-chain storage solutions (i.e., external websites) do not require an immutable ledger: simply not updating the website is enough to cause NFT links to “break” and point anywhere. There is no practical way to avoid the broken link problem with digital NFTs until they are secured on a platform similar to the blockchain itself [37]. We believe that hosting NFTs on the Interplanetary File System (IPFS), a web-based peer-to-peer (P2P) file system that helps ensure file distribution, can solve this problem. However, IPFS relies on the popularity of seed files for storage, which means that if the NFT is not of interest, it may suffer from broken links as well.

Data Access Management. The use of blockchain technology allows entities to share information in an efficient manner, eliminating the need for multiple centralized databases, which frequently leave data fragmented and inaccessible. All participating entities have equal access to the blockchain. Madine et al. proposed allowing users to upload encrypted content and cast it as NFT for sale to prevent data owners' data from being used without their knowledge [38]. However, the purchaser can only access the private data on the NFT for a limited time before it is automatically deleted. Because it is not possible to save the data in Madine's proposed solution, Ramyasri et al. proposed a blockchain-based solution for access control of medical data without the need for a central authority or third party. The proposed solution has only two phases: entity registration and access to medical data. However, the solutions presented above are not based on NFT for data access control. Ahmad et al. proposed an NFT-based solution in which the owner of a medical product can be easily identified at any point in time, allowing regulators to implement accountability measures and standards [39].

5 Right Confirmation of NFT Data and Risk Avoidance

Meten Holding Group Ltd. (METX.US) used NFT technology to copyright protect courseware as early as June 14, 2021. NFT technology is now being considered as a copyright protection technology, and ownership is becoming a public concern. It is necessary to use NFT to prove data ownership and avoid the risks that may arise as a result of it (Table 4).

Table 4. Comparison of data traceability and data access solutions.

References	Applications	Block-chain	Trace-ability	NFT-based	The broken link problem	Data access management
Chronicled [32]	Healthcare product traceability	Private chain	√	×	√	×
Sadri [33]	Blood donation information traceability	Private chain	√	×	×	√
Martin [6]	Wood production traceability	Ethereum	√	√	√	√
Noura [34]	Jewelry certification and purchase traceability	Ethereum	√	√	√	√
Madine [36]	Personal data access	Ethereum	√	×	√	×
Ramyasri [40]	Personal medical Data access	Ethereum	√	×	√	×
Ahmad [39]	Medical product Data access	Ethereum	√	√	√	×

5.1 Right Confirmation Research Using NFT Data

Because of the open and shared nature of the Internet, copyright protection has faced significant challenges in the Internet era, and emerging NFT technology is expected to provide an effective solution for copyright protection. At the moment, NFT technology has been widely adopted by artists and music publishers, who use blockchain technology's decentralization, timestamp, and encryption algorithm to store the created works in the blockchain after minting and generate a unique digital ownership certificate corresponding to the work, thereby achieving the goal of copyright protection [41].

Zhao et al. proposed a Blockchain-based Digital Rights Management (BMDRM) scheme that incorporates NFT and smart contracts in a related study [42]. All processing data is stored in the Ethereum private chain, a highly secure distributed ledger based on encryption and signatures that ensures the security and efficiency of transactions and authorizations. Imran Ush Shahid et al. identified news copyright and used it to combat the spread of fake news by issuing it as NFT [43]. To begin, a scoring system is established based on the Ethereum platform using the ERC-1155 standard to cast the news as NFT and distribute it. Each user can rate the news, and finally, the news is judged to be credible based on the calculated percentage of news authenticity. The authors' authenticity scoring formula is as follows.

$$R_a = \frac{P}{U \times 4} \times 100 \tag{1}$$

R_a is the percentage of authentic ratings, P is the total number of user ratings (ranging from 0 to 5), and U is the total number of rated users. Although the publisher of the news, i.e., the NFT creator, is identifiable, it is not stated which platform the users who rated the news's authenticity were on. The rating mechanism is entirely under the control of the users, and if the users are unable to judge the authenticity of the news or the number of controlled bot users increases, the authenticity rating will suffer and the news will remain vulnerable to manipulation.

The ownership ruling of data is central to the copyright discussion of works, and Shae et al. proposed a scheme in which NFT was used to solve the problem of data rights in the health care field. Shae et al. used NFT to model healthcare data in order to solve the problem of healthcare data silos by managing, accessing, and exchanging them on a blockchain platform [44]. Initially, blockchains were intended to be anonymous, but true identity requirements are critical for auditability, traceability, and accountability in blockchains used for healthcare data.

Figure 4 depicts the NFT exchange process in healthcare data sharing. The data provider (patient) first registers the medical data on the blockchain as an NFT. As the NFT owner, the blockchain platform will record its ID. After that, the data provider can send the NFT to the hospital. When a transaction is authenticated and authorized, a Strong Kidney (SK) token, an ERC-20 token, is transferred to the account of the data provider. The SK token grants access to VIP services such as fast-track queue access and discounted fees during the visit. SK Tokens can be bought with real money at SK token exchanges (such as hospitals).

The use of SK tokens to pay for VIP services during medical visits is a simple business model. According to Shae et al. [44], the scope of pass use should be expanded

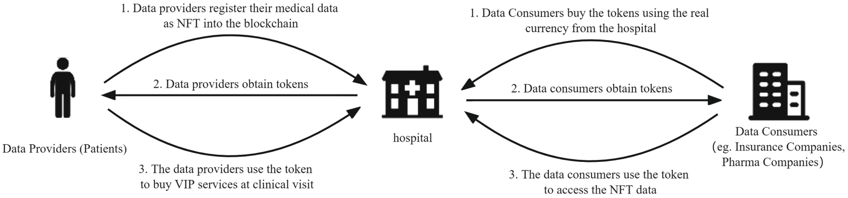

1. Data providers register their medical data as NFT into the blockchain
2. Data providers obtain tokens
3. The data providers use the token to buy VIP services at clinical visit
Data Providers (Patients)
hospital
1. Data Consumers buy the tokens using the real currency from the hospital
2. Data consumers obtain tokens
3. The data consumers use the token to access the NFT data
Data Consumers
(eg. Insurance Companies, Pharma Companies)

Fig. 4. NFT healthcare data sharing process.

to incentivize data providers (patients) to provide data, for example, SK tokens can be exchanged for some hard-to-buy concert tickets or soccer game tickets. However, we believe that the ERC-20 token can provide incentives on its own, so the actual utility of the SK pass has yet to be determined.

5.2 Data Rights Confirmation Risk and Avoidance

Copyright infringement is a common practice in the monetization of digital media. There are at least ten popular NFT platforms, and ownership of digital collections on the blockchain is only valid after they have been chained. If you want to declare the collection's copyright, you must upload the work to each platform. This, however, will significantly increase the labor and time costs.

Adopting Decentralized Identity (DID) to determine the ownership of NFTs can effectively address the issues of fraud and plagiarism that plague artists and creators. Lee et al. propose NextAuction, a next-generation NFT auction service that can reliably trade the ownership of individual content using DID technology [45]. The NextAuction service uses DID throughout the auction process to provide users with proof of identity in a transparent and consistent manner, improving the reliability of service participants. Buyers and sellers will be able to verify the provenance of digital artwork, and DID can facilitate interactions between artists and communities, such as limiting NFT ownership to community members to limit scalping or providing exclusive NFT content to specific groups of people.

Watermarking, one of the oldest but most widely used authentication techniques, can also be used. In the case of digital collections [46], the discrete cosine transform (DCT) is used to incorporate and retrieve input images. The images in the feature space are first transformed using the Fourier transform. The DCT algorithm is fed the digital collection image and the watermark image; the digital collection image is then segmented into 88 squares, and the watermark image is added to them, completing the watermark embedding; and finally, the user sees the image information with a reasonable balance of robustness and transparency. The Inverted DCT (IDCT) method is required to retrieve the watermarked image from the source image because it has a significant power compressibility feature, which means that the majority of the information set is contained in a few low-frequency elements of the DCT. The JPEG compression algorithm employs this feature to extract and eliminate unnecessary harmonic information from the image. Real-time multimedia, in addition to images, can be watermarked, increasing the scalability of NFT applications (Table 5).

Table 5. Comparison of data traceability and data access solutions.

References	Description	Block-chain	Role	Trace-ability	Authen-tication
Zhao [42]	Trading and licensing digital rights, automating the process of determining the security and efficiency of trading and licensing	Ethereum private chain	Digital copyright protection	√	√
Imran Ush Shahid [43]	Distribution of news into NFT, determination of news copyright, and establishment of a system to score the authenticity of news	Public chain	News copyright protection	√	×
Shae [44]	Model medical data as NFT, manage, access, and exchange it on the blockchain platform	Federated chain	Medical data rights	√	√
Lee [45]	Adopt DID for NFT confirmation to solve the plagiarism problem	Klaytn chain	Digital artwork rights	√	√
Ankala [46]	Use DCT to add a watermark to multimedia to solve the problem of infringement	–	Digital artwork rights	×	×

6 Conclusion

Because of its uniqueness, transactability, and traceability, NFT technology and its supporting blockchain infrastructure have been investigated as a potential solution to improve existing industrial applications. Aside from NFT transactions, prominent NFT application scenarios include supply chain traceability and data corroboration. The NFT eco-supervision approach is investigated for the first time in this work, as are the security risks of the two application scenarios of traceability and corroboration. This paper examines the current financial risks in the NFT ecosystem before proposing a regulatory approach based on cryptography and data analysis. The current security risks in two major scenarios of traceability and data confirmation are analyzed, and corresponding solutions are provided by summarizing the development history and research progress of NFT. This work can assist NFT practitioners in understanding the benefits of NFT applications.

Only two NFT application scenarios are analyzed for risk in this study, and future work may propose more detailed countermeasures for other NFT application risk states. Such as security flaws in stacking and smart contract layout; the risk of prophecy machine manipulation during data transmission; NFT diminishes its incentive role as a pass-through and must address liquidity issues; and the NFT trading market is still subject to centralized control. Furthermore, in many jurisdictions, NFT is untested, and the scope of NFT regulation is unclear.

Acknowledgements. This work was supported in part by the National Key R&D Program of China (No. 2021YFB2700601); 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. Fairfield, J.A.: Tokenized: The law of non-fungible tokens and unique digital property. Ind. LJ **97**, 1261 (2022)
2. Top 100 NFT Coins by Market Capitalization. https://www.coingecko.com/en/categories/non-fungible-tokens-nft. Last accessed 29 Dec 2022
3. Blockchain Explorer. https://www.blockchain.com/explorer/. Last accessed 29 Dec 2022
4. Nakamoto, S.: A peer-to-peer electronic cash system. Bitcoin **4**, 2 (2008)
5. Ethereum, https://ethereum.org/zh/. Last accessed 29 Dec 2022
6. Kshetri, N.: Scams, frauds, and crimes in the nonfungible token market. Computer **55**(4), 60–64 (2022)
7. EIP-721. https://eips.ethereum.org/EIPS/eip-721. Last accessed 29 Dec 2022
8. CryptoKitties. https://www.cryptokitties.co/. Last accessed 29 Dec 2022
9. EIP-1155. https://github.com/ethereum/EIPs/issues/1155. Last accessed 29 Dec 2022
10. Martinod, N. J., Homayounfar, K., Nachtigall L.: Towards a secure and trustworthy imaging with non-fungible tokens. In: Applications of Digital Image Processing XLIV, p. 47. SPIE, San Diego, United States, (2021)
11. Jiang, Z., Peng, Z.: Regulatory logic in the development of cryptographic digital art industry – research on rapid propagation and industry impact based on NFT art. Acad. Forum **4**, 122–132 (2021)
12. Sun, L., Li, X., Zhao, H.: NFT based physical on chain asset method. J. Zhejiang Univ. (Eng. Edn.) **56**, 1900–1911 (2022)
13. Chaleenutthawut, Y., Davydov, V., Kuzmin, A.: Practical blockchain-based financial assets tokenization. In: 2021 4th International Conference on Blockchain Technology and Applications, pp. 51–57. Xi'an, China (2021)
14. Ross, D., Cretu, E.: NFTs: Tulip mania or digital renaissance? In: 2021 IEEE International Conference on Big Data (Big Data), pp. 2262–2272. Orlando, FL, USA (2021)
15. Zhou, L., Qin, K.: High-frequency trading on decentralized on-chain exchanges. In: 2021 IEEE Symposium on Security and Privacy (SP), pp. 428–445. IEEE, (2021)
16. Qin, K., Zhou, L.: Quantifying blockchain extractable value: How dark is the forest? In: 2022 IEEE Symposium on Security and Privacy (SP), pp. 198–214. IEEE, (2022)
17. Gebreab, S. A., Hasan, H. R., Salah, K.: NFT-based traceability and ownership management of medical devices. IEEE Access (2022)
18. Westerkamp, M., Victor, F., Küpper, A.: Blockchain-based supply chain traceability: token recipes model manufacturing processes. Preprint at http://arxiv.org/abs/1810.09843 (2018)
19. Weijers, D., Turton, H. J.: Environmentally Smart Contracts for Artists Using Non-Fungible Tokens. In: 2021 IEEE International Symposium on Technology and Society (ISTAS), pp. 1–4. Waterloo, ON, Canada (2021)
20. Su, Y., Li, H., Chen, J.: NFT Policy Research Report. In: 2022 World Artificial Intelligence Conference Youth Forum on Rule of Law Shanghai 11, 142–160 (2022)
21. Das, D., Bose, P., Ruaro, N.: Understanding security Issues in the NFT Ecosystem. arXiv preprint arXiv:2111.08893 (2021)
22. Casale-Brunet, S., Ribeca, P., Doyle.: Networks of Ethereum Non-Fungible Tokens: A graph-based analysis of the ERC-721 ecosystem. In: 2021 IEEE International Conference on Blockchain (Blockchain), pp. 188–195. IEEE, Melbourne, Australia, (2021)

23. Ryabov, O., Golubev, A., Goncharova, N.: Decentralized Finance (DeFi) as the basis for the transformation of the financial sector of the future. In: 3rd International Scientific Conference on Innovations in Digital Economy, Saint—Petersburg Russian Federation, pp. 387–394. (2021)
24. Choe, Y.C., Park, J., Chung, M.: Effect of the food traceability system for building trust: Price premium and buying behavior. Inf. Syst. Front. **11**(2), 167–179 (2009)
25. Korpela, K., Hallikas, J., Dahlberg, T.: Digital supply chain transformation toward blockchain integration. In: Proceedings of the 50th Hawaii International Conference on System Sciences (2017)
26. Glaser, F.: Pervasive decentralization of digital infrastructures: a framework for blockchain enabled system and use case analysis. In: Proceedings of the 50th Hawaii International Conference on System Sciences (2017)
27. Wüst, K., Gervais, A.: Do you need a blockchain? In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), pp. 45–54. IEEE, (2018)
28. Kim, H.M., Laskowski, M.: Toward an ontology-driven blockchain design for supply-chain provenance. Intell. Syst. Account., Finance Manag. **25**(1), 18–27 (2018)
29. Abeyratne, S.A., Monfared, R.P.: Blockchain ready manufacturing supply chain using distributed ledger. Int. J. Res. Eng. Technol. **5**(9), 1–10 (2016)
30. Toyoda, K., Mathiopoulos, P.T., Sasase, I.: A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. IEEE Access **5**, 17465–17477 (2017)
31. Hackius, N., Petersen, M.: Blockchain in logistics and supply chain: trick or treat? In: Proceedings of the Hamburg International Conference of Logistics (HICL), pp. 3–18. GmbH, Berlin (2017)
32. Alnuaimi, N., Almemari, A., Madine, M.: NFT certificates and proof of delivery for fine jewelry and gemstones. IEEE Access **10**, 101263–101275 (2022)
33. Hasan, H.R.: Incorporating registration, reputation, and incentivization into the NFT ecosystem. IEEE Access **10**, 76416–76433 (2022)
34. Dash, A.: NFTs weren't supposed to end like this. The Atlantic 2, (2021)
35. Yan, C.: Exploring the regulatory path of NFT and the meta universe in the digital era. Shanghai Legal Res. **11**, 79–89 (2022)
36. Madine, M., Salah, K., Battah, A.: Blockchain and NFTs for time-bound access and monetization of private data. IEEE Access **10**(2022), 94186–94202 (2022)
37. Musamih, A., Yaqoob, I., Salah, K.: Using NFTs for product management, digital certification, trading, and delivery in the healthcare supply chain. IEEE Trans. Eng. Manage. 1–22 (2022)
38. Mattke, J., Hund, A., Maier, C.: How an enterprise blockchain application in the us pharmaceuticals supply chain is saving lives. MIS Quart. Executive 18(4), (2019)
39. Sadri, S., Shahzad, A., Zhang, K.: Blockchain traceability in healthcare: Blood donation supply chain. In: 2021 23rd International Conference on Advanced Communication Technology (ICACT), pp. 119–126. IEEE, (2021)
40. Ramyasri, G., Hussain, S. J.: Access control of healthcare data using blockchain technology. In: 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), pp. 353–357. IEEE (2021)
41. Qin, R., Li, J., Wang, X.: NFT: Blockchain based heterogeneous authentication and its application. J Intell Sci Technol **3**, 234–242 (2021)
42. Zhao, L., Zhang, J.: Blockchain-enabled digital rights management for museum-digital property rights. Intell Automat Soft Comput **34**(3), 1785–1801 (2022)
43. Ush Shahid, I., Anjum, Md. T.: Authentic facts: a blockchain based solution for reducing fake news in social media. In: 2021 4th International Conference on Blockchain Technology and Applications, pp. 121–127. ACM, Xi'an, China (2021)

44. Shae, Z., Tsai, J. J.: On the Design of Medical Data Ecosystem for Improving Healthcare Research and Commercial Incentive. In: 2021 IEEE Third International Conference on Cognitive Machine Intelligence (CogMI), pp. 124–131. IEEE, (2021)
45. Lee, Y., Kim, H., Lee, M.: NextAuction: A DID-based robust auction service for digital contents. J Korea Soc Comput Inform **27**(2), 115–124 (2022)
46. Kumar, K. P., Prabha, B.: Hidden image watermarking based on frequency domain technique. In: 2022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), pp. 1–6. IEEE, Bhilai, India (2022)

When Blockchain Meets Domain Specific Language: A Review

Chuan Liu[1,3], Jun Li[1,3], Hong Lei[1,2(✉)], Xiang Xu[1], and Chao Liu[4]

[1] Hainan University, Haikou 570228, China
liuchuan072@126.com, junli@hainanu.edu.cn, leiluono1@163.com,
21220854000106@hainanu.edu.cn
[2] SSC Holding Company Ltd., Chengmai 571924, China
[3] Oxford-Hainan Blockchain Research Institute, Chengmai 571924, China
[4] The Blockhouse Technology Limited, Oxford OX2 6XJ, United Kingdom
liuchao@tbtl.com

Abstract. In recent years, blockchain has become popular for its characteristics, such as decentralization, data immutability, and easy traceability, and has been used in the financial industry, IoT, law, etc. However, smart contracts for blockchain are highly professional and poorly readable for users. As a result, several domain-specific languages (DSLs) based on smart contracts have been proposed to reduce the cost of communication between users and contract developers, and even enable users to write reliable smart contracts by themselves. Domain-specific languages for smart contracts are proposed to achieve the goal of being able to automatically translate to universal smart contract programming languages while retaining the readability, critical writing style and enhanced semantic clarity of natural language. Therefore, we investigate the emergence of DSLs based on smart contracts since Blockchain 2.0, analysis and discuss the advantages and disadvantages of existing DSLs. We classify these DSLs by different intermediate abstract structure, and propose to design a quantitative evaluation framework of DSL features to evaluate. Finally, we conclude the existing DSLs' characterstics and propose future the development direction of DSL based on smart contract.

Keywords: Blockchain · Smart contract · Domain-specific language

1 Introduction

Ethereum has become one of the most popular platforms for smart contract development since the Web2.0. So, the smart contract programming language Solidity [1] become naturally the most popular language, and the other two languages, Serpent and Mutan [2] are also supported in Ethereum. In addition, universal programming languages(UPLs) such as C++, Rust, Golang, Java and Python, etc. [3,4] are also widely used for the design and development of smart contracts for various blockchain platforms. For the above smart contract languages, they all have many common language features, which means developers

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 110–125, 2024.
https://doi.org/10.1007/978-981-99-7161-9_9

can develop the smart contract proficiently by learning the extra knowledge of blockchain and smart contract design specifications. However, due to the increasing requirement of blockchain, the application of blockchain are becoming more and more extensive [5], and the requirements for smart contract development vary greatly from the different scenarios, which means requiring developers to not only be familiar with smart contract languages, but also need to understand the domain and behaviour of smart contracts in the current application scenario to meet the needs of the current. As the developers do not understand well the domain knowledge of the requirements and domain experts do not know how to develop smart contract. So the cost of communication is expensive between the two, and the productivity has low efficency. According to van Deursen [6] et al. 'A domain-specific language (DSL) is a programming language or executable specification language that offers, through appropriate notations and abstractions, expressive power focused on, and usually restricted to, a particular problem domain.' Thus, a smart contract DSL has the readability like natural language, a specification-writing paradigm, semantic clarity, and the ability to automatically translate into a realistic smart contract. In general, DSLs have many advantages over GPLs [7].

The main advantage of DSLs based on smart contracts is that domain experts don't need to learn an additional programming language or software engineering, just only need to focus on themselves domain to write usable smart contracts that meet their needs. Figure 1 shows the general framework of DSL for generating finance-related smart contracts, which differs from traditional smart contracts that users just need to focus on writing similar realistic contracts, and then it can convert to the real smart contract. Although DSLs can only execute a specific task by a limited extent, they perform well in their respective domains, due to their outstanding expertise ability. We provide a structural survey of the current state of the development of DSLs that are developed for blockchain smart contracts, and evaluate each of them in different domains and characteristics. Our main purpose is to provide a reference for smart contract developer or relevant users, and to propose a quantifiable evaluation framework, which based on FQAD (Framework for Qualitative Assessment of DSLs, FQAD) [8], which aims to reduce the cost between the domain experts and smart contract developer,while evaluating existing DSLs for smart contract, and to provide recommendations for the future development of smart contract-based DSLs.

Firstly, we propose the qualitative evaluation framework for DSLs, FQAD in Sect. 1. We classifies smart contract-based DSLs in different domains, analysis them by aboved framework. We provide a comparative analysis between DSLs based on their attribute characteristics in Sect. 3. Finally, we summarize the advantages and disadvantages of existing smart contract-based DSLs, and provide a summary and outlook for the future development of smart contract-based DSLs

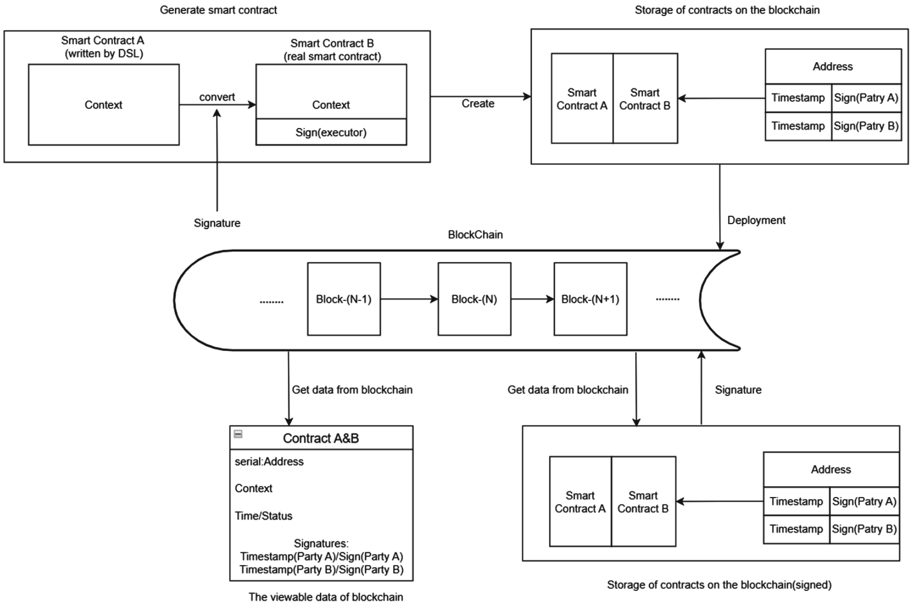


Fig. 1. The general framework of DSL

2 Quantification Evaluation Framework QFQAD

FQAD is a framework for DSL evaluation based on ISO/IEC 25010:2011, which defines a set of attributes for evaluating the quality of DSLs, including:functional suitability, usability, reliability, maintainability, productivity, extendability, compatibility, expressiveness, reusability and integrability. But it does not give a uniform quantitative standard based on the definitions. There are many metrics for reliability evaluation, such as MTBF(Mean Time Between Failure) [41]. MTBF is a reliability metric used to evaluate electronic products, and this quantification scheme is widely used in many applications including electronic products [42], including the application to the blockchain [43].

This section, we propos a DSL quantification evaluation framework 'QFQAD' based on FQAD and reliability metric quantification schemes. The evaluation framework is shown in Table 1.

2.1 Properties of QFQAD

Functional Suitability It refers to the extent to which a DSL is fully developed and determines whether the DSL contains all the necessary functionality in the domain and does not contain extra unnecessary function. This property is used to describe the extent to which the DSL has been developed to meet the needs of the domain.

Table 1. QFQAD framework

Properties	Calculate	Describe	Total
Functional suitability	Accumulation	Functional completeness (5), Functional correctness (5)	10
Usability	Accumulation	Robustness (3), Operability (4), Recognisability (3)	10
Reliability	Accumulation	Maturity (4), Fault tolerance (4), Recoverability (2)	10
Extendability	Condition	Not support (0), Partly support (5), Fully support (10)	10
Integrability	Condition	Not support (0), Partly support (5), Fully support (10)	10
Maintainability	Accumulation	Structural modularity (4), Testability (3), Modifiability (3)	10
Productivity	Condition	Contract template (5), Executable contracts (10)	10
Compatibility	Condition	Unsuitable (0), Partly suitable (5), Fully suitable (10)	10
Reusability	Condition	Not available (0), Partly available (5), Fully available (10)	10
Expressiveness	Condition	Not achieved (0), Partly achieved (5), Fully not achieved (10)	10

Usability It refers to how easy it is for users to use the DSL to achieve a stated goal. The DSL should be designed to use easily and convenient to achieve the expression of domain. We invite several users from within and outside the domain to evaluate the DSL in order to conclude fairer conclusions. This property are mainly used to describe whether the DSL is easy to use at the level of use and operation and easy to learn.

Reliability It refers to the property of generating a reliable programmable smart contract. It determines whether a DSL has a complete and standard syntax definition, whether it has a syntax detector. This property describes whether the statements written by that DSL are accurately and reliably converted into the programmable smart contract code correctly.

Maintainability It refers to how easy it is to maintain the DSL after it is completed. It determines how easy it is to modify DSL components to correct errors, improve performance or other attributes, or adapt to changing circumstances. This type of property mainly describes how clear and cohesive the structure of the DSL is. This attribute is generally related to the design model and code transformation of the DSL, and choosing the right development framework will make it easier to maintain later.

Productivity It refers to the extent to which a DSL improves programming efficiency. It determines how much more efficient a DSL is compared to the original general purpose programming language. This type of property focuses on programming efficiency within a specific domain. This property is generally related to the design model and code transformation of the DSL, and programming efficiency varies from domain to domain. This type of property mainly describes the advantages of the DSL over the general purpose programming language in the domain.

Extendability It refers to how easy it is to add new function to this DSL. It determines whether the DSL has modules or interfaces to allow users to customize the DSL to add new functionality. This attribute is generally related to the design tool or development method of the DSL. This property describes whether the DSL can be extended to meet the different scenarios needs for the user.

Compatibility It refers that the degree to which the DSL, domain and development process. The degree of suitability between the DSL, the domain and the development process is judged. This type of property is primarily a judgment of the importance of the DSL within the domain and the ease of development. This attribute is generally related to the choice of the design framework of the DSL, where the choice of a suitable framework and the ability to logically conceptualise the domain can increase the domain compatibility of the DSL.

Expressiveness It refers to the ease with which a domain problem solution can be mapped into a program. This property is used to evaluate the ability of DSL to solve problems in that domain. The syntax rules of different DSLs are closely related to the domain problems they solve. This is because DSLs are designed to improve domain-specific expressiveness. A good DSL should be able to map problems easily to the appropriate program.

Reusability It refers to the extent to which the language structure of a DSL can be used in other languages. It is a matter of determining how applicable a DSL is and whether it is straightforward for the average person to use. Generally speaking, different DSLs have their own specific language structure, but the automatic mapper that generates the code is reusable and can be converted to a different language by modifying the mapping rules.

Integrability It refers to the ease with which a DSL can be integrated with other languages and modeling tools. It determines whether the DSL can be adapted to other tools, such as formal verification tools. This property is generally related to the design model and code transformation of the DSL, and the choice of design tools for DSL development allows developers to select different plug-ins depending on the framework. This type of property mainly describes whether the DSL has the ability to work with other tools.

3 DSLs

In this section, we survey different DSLs based on smart contracts, classified according to two types of DSL intermediate abstraction: **Formal Models**: Extract the information of entity linkage and logic rules in the contract, establish the mapping model of formal model and smart contract language and specific statement mapping relationship, and generate the corresponding executable contract code. **Contract Template**: DSL has set up corresponding contract code templates for different application scenarios, and the executable smart contract code can be generated by setting relevant parameters and adding corresponding logic.

3.1 Formal Models

Marlowe Marlowe [9] is mainly designed for financial smart contracts. The users can write smart contracts by using only 'single' Marlowe language, but also by directly referencing Marlowe code into the Haskell [10] programming language, using its features for different situations, which makes them easier to read and reuse. Typically, Marlowe contracts are built by linking different blocks, which are functional modules that describe contract execution, monitoring real-world events as trigger conditions, etc. Marlowe contracts are compiled into serialized Plutus core code using the PlutusTx compiler [11] so as to create a validator script of Cardano [12] to execute the real contract. The strength of this DSL is that it supports the static validation of contracts before it runs and the language is able to perform formal verification via the Isabelle theorem provers to ensure the security of the funds. However, as of writing this paper, Marlowe has still not proposed an official semantic specification.

Das Contract Das Contract [32] is an open source DSL project that allows for writing smart contracts by graphical which is beneficial for reducing the semantic errors or misunderstandings in text. It supports that users create contracts by BPMN(Business Process Model and Notation) [44]. The translator of this DSL can translate 'Das Contract' into corresponding solidity codes. The authors used DEMO(Design and Engineering Methodology for Organizations) [45] and BPMN to analysis the target domain and design process of DSL. The strength of this DSL has strong expressiveness on scenarios of writing complex contract by combing block. The project provides a demonstration of Eurpoean Union election process [33].

iContractML iContractML [34] is developed to solve the heterogeneity of different blockchain platforms and reduce the developer's workload. This DSL is an open source project and the style of writing contract is based on graphic(UML metamodel). Nowadays, it can develop corresponding smart contract for Ethereum, Hyperledger Composer, and Azure Blockchain Workbench with this DSL. The implementation of abstraction is by creating corresponding mapping on UML model convert to executable smart contract.The syntax of DSL is designed by using OBEO Designer, and creating validation rules for the model instances by Acceleo. The project has three cases for evaluating its contract correctness and usability. The weakness of this DSL is that it can only specify the structure of contract, not the execution condition of the parties.

FsolidM FSolidM [35] is designed for contract validation and the generation of smart code is by Finite State Machine (FSM) [39] model graphs. The author developed an open source web tool based on WebGME [40] for improving graphical development efficiency. The web tool is applicated in translator of DSL and formal validation tool VeriSolid [36]. The weakness of this DSL is that the FSM to Solidity translation is semi-automatic and it requires human secondary writing to perform to be executable Solidity code. This FSM model-to-smart contract translation is improved by [37] FsolidM's design structure 'primary-secondary separation', which identifies patterns in which contracts can be executed out-of-chain to decrease the runtime overhead of smart contracts.

LATTE LATTE [38] is a visual DSL based on Ethereum smart contracts, that allows users to build a contract by manipulating visual objects in a direct manipulation-based interface without writing Solidity code. At the same time, LATTE's gas awareness allows for a straightforward representation of gas consumption during contract construction, giving users a more intuitive sense of what they are spending to generate a smart contract. But LATTE is only suitable for creating a single smart contract, not multiple templated contracts. The platform also supports a single contract logic, and cannot support smart contracts with complex logic or using complex algorithms.

Psamathe Psamathe [15] is specifically designed for dealing with asset management contracts on Ethereum and to avoid the associated vulnerabilities that arise as a result (smart contract design). The language was developed by performing a new abstraction, called 'flow'. The strength of Psamathe is that it can automatically build universal contract templates over traditional smart contract code. Because it is built around 'flow', it facilitates contract syntax condition checking, workflow modification, and contract compilation errors, providing advantages such as quick start-up and contract security for experts in different domains. The authors set up several test cases to test the language, but did not perform an overhead analysis, robustness and performance test from the user's perspective.

ADICO ADICO: Frantz [21] proposed a high-level abstract textual DSL with syntactic support from ADICO [22] and a built-in syntax-based semi-automatic translator that converts the ADICO contract to its corresponding smart contract which consists of Solidity code. Its translator of DSL is developed by Scala, and its action of conversion to Solidity is defined by a mapping structure from the DSL to its corresponding Solidity template. ADICO is a declarative DSL, providing an extra abstraction of intermediate that makes it easy for users. However, ADICO can only generate corresponding solidity smart contract templates. It still requires the user to edit it based on it and manually add extra logic functions to satisfy its compilation rules.

DAML DAML [24] is an available DSL project of Digital Asset, which purposed to perform multi-domain, complex business application development. It can be developed and integrated with different blockchain platforms on its abstract ledger, such as Sawtooth, Fabric, Corda, etc. The writing type of DAML smart contracts is textual and follows the UTXO model [25] as well as integrating Ethereum smart contracts [26]. The development language of this DSL is Scala and programming language Haskell is used as for developing the compiler. Therefore, it is not only operationally friendly but also independently interoperable in meeting the privacy protection needs among different platforms of blockchain.

Archetype Archetype [27] is developed for the Tezos blockchain platform with the support of the Tezos Foundation by Edukera company. It is designed for smart contract formal validation to enhance security. This DSL is mainly developed by the OCaml [28]. The archetype contract supports to be translated into various scripts, such as ligo, markdown, google script and why3. The characteristics of Archetype contract are: logic clear, strict exceuation conditions,explicit state machines, standalone development API. The language is still in development and has more than 26 releases.

ink! ink! [29] is developed for the blockchain platform Substrate by Parity Technologies. This DSL is open source and development language is using Rust. It has a high-level abstraction of writing style, which makes it easier to use and execute than the WebAssembly language [30].

Lity Lity [31] is a DSL developed from a Solidity-based design with new syntax extensions, it is highly optimized for business users and easy to use for developers in the financial industry. The user interface is designed to be friendly and easy to operate. Besides, its built-in functions can reduce gas consumption and improve execution efficiency. At present, the language only supports the Ethereum platform, and the level of abstraction is not high. Using its built-in contract template is not complete and needs to be written twice according to the Solidity syntax structure, which is not friendly enough for users outside the computer domain.

3.2 Contract Template

Findel Findel [14] is a DSL for financial which based on ideas, and its editing style is declarative. Findel contracts have three components: the contract description, the issuer, and owner. And the issuer and owner are role as the parties in the contract. Findel contracts are translated into executable code and applicable to any blockchain platform, such as Fabric, Ethereum, etc. Findel is useful in smart for complex condition-oriented Findel requires a low level of abstraction when writing computer programming-related contracts, but it also makes Findel excellently extensible.

SPESC SPESC [13] is a finanicial domain specific language that creates an contract template layer on intermediate of the conversion of smart contracts, with the aim of enabling experts in the financial domain to design and write smart contracts without having a programming background. SPESC has a natural language-like syntax that specifies smart contracts in a form similar to real-world contracts, where the parties (defined as ‘contract parties’) and a description of their obligations and rights (defined as ‘execution’), specify the structure and syntax of the DSL, and implement the expression of relevant terminology, as well as the transaction rules for each cryptocurrency. However, it is not directly convertible into a usable smart contract and needs to be populated with its contractual content according to the original smart contract language syntax and structure, and the DSL can only generate the corresponding contract template.

CML CML [23] is a highly abstract UML-based DSL with a declarative and imperative approach for editting contract. The DSL is not just limited to a single domain, it covers areas such as: law, finance, asset trading, etc. The contract is edited by CML is an easily understandable, editing style like real clauses and formal contract to describe the respective behaviors (or commitments) of contract participants. The DSL is designed to address the unified modeling and behavior designation of unstructured legal contracts to enhance the automatic conversion and interpretation of smart contract.

Tateishi Tateishis [20] contracts are written from contract templates and a set of controlled natural languages (CNL) that undergo a transformation process of formal models, state graphs, etc. and are finally translated into a smart contract written in a programming language. By summarizing a large number of contracts, the developer's predefined contract document templates, formal model templates, and transformation rules can be used for many similar contracts. This not only reduces the development cost of smart contracts, but the contract documents are also easily understood by business people or lawyers. It is important to note that when dealing with the context of CNL sentences, it is necessary to specify explicit parameter mappings for unclear pronouns such as 'it' to avoid ambiguity.

Ergo Ergo [16] is designed for commercial legal smart contract. This DSL is open source and available as one part of the Accord project, which is supported by the Linux Foundation. The Contracts can be written in Ergo(online WebIDE) are generic across blockchain platforms, meaning they can be executed on different distributed ledger platforms and it also supports that is executed off-chain. Ergo is designed by Coq [17] which means it has a strict syntax definition. Also, Coq can be used as a tool for the formal specification and validation for ergo contracts. Nevertheless, Ergo is still on the development stage and its robustness is poor, with more than 122 versions released.

SLCML SLCML (Smart Legal Contract Markup Language) [18] is designed as a contract specification language that includes legal knowledge and characteristics of business collaboration for decentralized autonomous organization (DAO) contracts. SLCML is designed for developing CCBCs(complex collaborative business contracts) and to eliminate technical barriers in legal and business structures to draft contracts that are legally binding. This DSL was designed originally as plugin for eSourcing markup language (eSML) [19]. It also supports defining the configuration of smart contracts for DAO collaboration (rather than its development) and it involves the legal concept of collaborative business behaviors such as obligations, rights and performance. SLCML contract can be easy to understand and have the advantage of being configurable for a wide range of contract types. The disadvantage of this is the lack of domain integrity in contract.

4 Comparing

Figure 2 shows the score of the above DSLs evaluated by QFQAD. And we will discuss and compare the attributes of DSLs in language and development in this section.

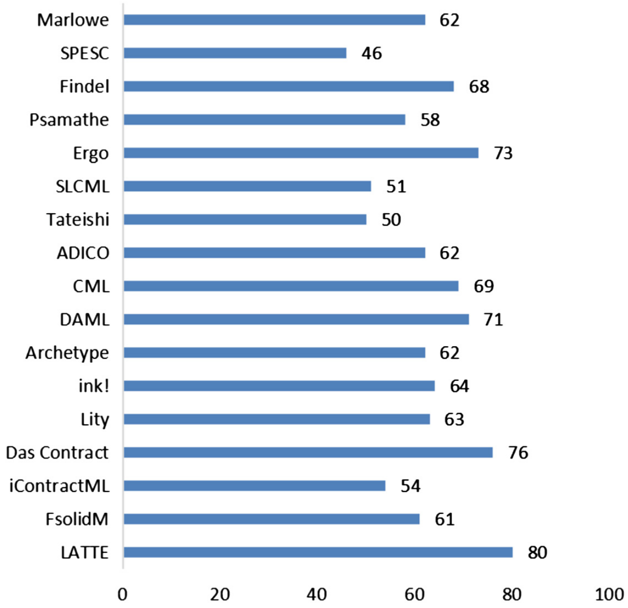


Fig. 2. DSLs' score

4.1 Language Attribute

Table 2 shows the comparative of the aboved DSLs based on the language attributes of DSLs: (a) **User interface**: This defines the type of interaction with DSL; (b) **Target domain**: This tells about what application scenarios for; (c) **Target language**: This defines the target language what the DSL translate into; (d) **Blockchain platform**: This means what platform the smart contract are deployed; (e) **Platform type**: The blockchain platforms are generally classfied two types: Public, Private; (f) **Domain ability**: This tells about if the DSL has ability to solve completely solve the problems of target domain; (g) **Time**: This means when the DSL is proposed.

4.2 Development Attribute

Table 3 shows the comparative of the aboved DSLs based on the development attributes of DSLs: (a) **Type**: This tells the DSL how to be developed; (b)

Table 2. Language attributes of DSLs

DSL	User interface	Target domain	Target language	Blockchain platform	Platform type	Domain ability	Time
Marlowe	Textual	Financial	Haskell/Plutus	Cardano	Public	✓	2020
SPESC	Textual	Financial	–	–	–	✓	2018
Findel	Textual	Financial	Solidity	Ethereum	Public	✓	2017
Psamathe	Textual	Fniancial	Solidity	Ethereum	Public	✕	2020
Ergo	Textual	Legal	Muti-language	Muti-Platform	Public & Private	✕	2021
SLCML	Textual	Muti-domain	–	–	–	✓	2021
Tateishi	Textual	Muti-domain	Solidity	Ethereum	Public	✕	2019
ADICO	Textual	Muti-domain	Solidity	Ethereum	Public	✓	2016
CML	Textual	Muti-domain	Solidity	Ethereum	Public	✕	2020
DAML	Textual	Muti-domain	DAML	Digital Asset Ledger	Public & Private	✓	2022
Archetype	Textual	Muti-domain	Muti-language	Tezos	Public & Private	✓	2019
ink!	Textual	Muti-domain	WebAssembly	Substrate	Public	✓	2019
Lity	Textual	Financial	Solidity	Ethereum	Public	✕	2018
Das Contract	Graphic	Muti-domain	Solidity	Ethereum	Public	✓	2020
iContractML	Graphic	Muti-domain	Solidity	Ethereum	Public	✕	2022
Fsolidm	Graphic	Contract Verification	Solidity	Ethereum	Public	✕	2018
LATTE	Graphic	Muti-domain	Solidity	Ethereum	Public	✕	2020

Table 3. Development attributes of DSLs

DSL	Type	Implementation	Contract-Validation	Maintenance	Test	Open source
Marlowe	Internal	PlutusTx, SBV	✓	✓	✓	✓
Midrule SPESC	External	–	✓	✗	✓	✗
Findel	External	JavaScript	✗	✗	✓	✗
Psamathe	External	Haskell	✗	✓	✓	✓
Ergo	External	Coq, Ocaml	✓	✓	✓	✓
SLCML	External	XML	✗	✗	✓	✗
Tateishi	External	JavaScript	✗	✗	✓	✗
ADICO	Internal	Scala	✗	✗	✓	✗
CML	External	Xtext, ANTLR	✓	✗	✓	✓
DAML	External	Scala, Haskell	✓	✓	✓	✓
Archetype	External	Ocaml	✓	✓	✗	✓
ink!	Internal	Rust	✓	✓	✗	✓
Lity	External	C++, JavaScript	✓	✓	✓	✓
Das Contract	External	C#	✗	✓	✓	✓
iContractML	Internal	Obeo designer	✓	✗	✗	✓
Fsolidm	Internal	WebGME	✓	✓	✓	✓
LATTE	Internal	JavaScript	✗	✗	✓	✓

Implementation: This tells the DSL is developed by what programming language is; (c) **Contract-Validation**: This means if the smart contract generated by the DSL can pass contract validation; (d) **Maintenance**: This tells about if the development team or author maintained to the DSL after it was released; (e) **Test**: This tells if the DSL was tested in the proper application scenario; (f) **Open source**: This defines source code of the DSL are pubilc or private.

5 Conclusion

In this paper, We present a systematic survey and analysis of the DSL based on blockchain from 2017. We classify the above DSLs by user-interface, describe the advantages and disadvantages of each of them. We proposed a quantified FQAD framework for the DSLs. Finally, we compare them by the language attributes and development attributes. We found that: (1) Most of the DSLs have strong functional suitability and expressiveness in their domain. (2) There are only a few DSLs that support graphical interface, the others are textual. (3) Most of the DSLs' target blockchain platform is Ethereum, and their target language is Solidity. (4) Most of the DSLs are developed for financial and muti-domain. (5) Many DSLs are available and open source on GitHub and the official website. We believe that the development of DSL should focus on multi-domain and multi-platform blockchains, which include platform heterogeneity and cross-domain in the future.

Acknowledgement. This work was supported in part by the National Key R&D Program of China (No. 2019YFB2101601 and 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. Ethereum. https://ethereum.org/zh/. Last accessed 29 Dec 2022
2. Gramlich, B.: Smart Contract Languages: A Thorough Comparison (2020)
3. Androulaki, E., et al.: Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the 13th EuroSys Conference (EuroSys'18). ACM, Portugal, pp. 30:1–30:15 (2018)
4. Spoto, F.: A java framework for smart contracts. In: Proceedings of the Financial Cryptography and Data Security Workshop on Trusted Smart Contracts (WTSC'19). Springer LNCS 11599, pp. 122–137 (2019)
5. Praitheeshan, P., Pan, L., Yu, J., Liu, J., Doss, R.: Security analysis methods on ethereum smart contract vulnerabilities: a survey (2019)
6. Van Deursen, A., Klint, P., Visser, J.: Domain-specific languages: an annotated bibliography. ACM Sigplan Notices **35**(6), 26–36 (2000)
7. Kosar, T., Bohra, S., Mernik, M.: Domain-specific languages: a systematic mapping study. Inf. Softw. Technol. **71**, 77–91 (2016)

8. Sharif Razavian, A., Azizpour, H., Sullivan, J., Carlsson, S., et al.: CNN features off-the-shelf: an astounding baseline for recognition. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. USA, pp. 806–813 (2014)
9. Seijas, L., et al.: Marlowe: implementing and analysing financial contracts on blockchain. In: Financial Cryptography and Data Security. Springer LNCS, pp. 496–511 (2020)
10. Cardone, F.: From curry to haskell: paths to abstraction in programming languages. Philos. Technol. 1–18 (2020)
11. Plutus, T.X.: https://playground.plutus.iohkdev.io/doc/haddock/plutus-tx/html/PlutusTx.html. Last accessed 29 Dec 2022
12. C. community, Cardano documentation, https://docs.cardano.org/introduction. Last accessed 29 Dec 2022
13. He, X., Qin, B., Zhu, Y., Chen, X., Liu, Y.: Spesc: A specification language for smart contracts. In: IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). IEEE, pp. 132–137 (2018)
14. Biryukov, A., Khovratovich, D., Tikhomirov, S.: Findel: secure derivative contracts for ethereum. In: Financial Cryptography and Data Security, pp. 453–467 (2017)
15. Oei, R.: Psamathe: a dsl for safe blockchain assets. In: Proceedings of the International Conference on Systems, Programming, Languages, and Applications: Software for Humanity (2020)
16. Roche, N., Hernandez, W., Chen, E., et al.: Ergo-A programming language for Smart Legal Contracts.
17. The coq proof assistant. https://coq.inria.fr/. Last accessed 29 Dec 2022
18. Dwivedi, V., Norta, A., Wulf, A., et al.: A formal specification smart-contract language for legally binding decentralized autonomous organizations. IEEE Access **9** (2021)
19. Norta, A., Ma, L.X., Duan, Y.C., Rull, A., Kolvart, M., Taveter, K.: eContractual choreography-language properties towards cross-organizational business collaboration. J. Internet Serv. Appl. **6**(1), 1–23 (2015)
20. Tateishi, T., Yoshihama, S., Sato, N., et al.: Automatic smart contract generation using controlled natural language and template. IBM J. Res. Dev. **63**(2/3), 6:1–6:12 (2019)
21. Frantz, C.K., Nowostawski, M.: From institutions to code: towards automated generation of smart contracts. In: 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W). IEEE, pp. 210–215 (2016)
22. Crawford, S.E.S., Ostrom, E.: A grammar of institutions. Am. Polit. Sci. Rev. **89**(3), 582–600 (1995)
23. Wöhrer, M., Zdun, U.: Domain specific language for smart contract development. In: 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, pp. 1–9 (2020)
24. Daml. https://github.com/digital-asset/daml. Last accessed 29 Dec 2022
25. Hearn, M.: Rationale for and tradeoffs in adopting a utxo-style model. https://www.corda.net/blog/rationalefor-and-tradeoffs-in-adopting-a-utxo-stylemodel/. Last accessed 29 Dec 2022
26. Wood, G., et al.: Ethereum: a secure decentralised generalised transaction ledger. Ethereum Proj. Yellow Pap. **151**, 1–32 (2014)
27. Archetype. https://github.com/edukera/archetype-lang. Last accessed 29 Dec 2022
28. Balestrieri, F., Mauny, M.: Generic Programming in OCaml. In: Electronic Proceedings in Theoretical Computer Science, vol. 285 (2018)

29. ink! https://github.com/paritytech/ink. Last accessed 29 Dec 2022
30. Haas, A., Rossberg, A., Schuff, D.L., et al.: Bringing the web up to speed with WebAssembly. In: Proceedings of the 38th ACM SIGPLAN Conference on Programming Language Design and Implementation, pp. 185–200 (2017)
31. second-state/lity: A rule-based contract-oriented high-level language. https://github.com/second-state/lity. Last accessed 29 Dec 2022
32. Skotnica, M., Pergl, R.: Das contract-a visual domain specific language for modeling blockchain smart contracts. In: Enterprise Engineering Working Conference. Springer, Cham, pp. 149–166 (2020)
33. Skotnica, M., Aparício, M., Pergl, R., Guerreiro, S.: Process digitalization using blockchain: Eu parliamentelections case study. In: MODELSWARD. SciTePress, pp. 65–75 (2021)
34. Hamdaqa, M., Met, L.A.P., Qasse, I.: iContractML 2.0: A domain-specific language for modeling and deploying smart contracts onto multiple blockchain platforms. Inf. Softw. Technol. **144**, 106762 (2022)
35. Mavridou, A., Laszka, A.: Tool demonstration: Fsolidm for designing secure ethereum smart contracts. In: Principles of Security and Trust, L.
36. Mavridou, A., Laszka, A., Stachtiari, E., Dubey, A.: Verisolid: Correct-by-design smart contracts for ethereum. In: 23rd International Conference on Financial Cryptography and Data Security, pp. 446–465 (2019)
37. Bodorik, P., Liu, C., Jutla, D.: Using fsms to find patterns for off-chain computing. In: Proceedings of 3rd International Conference on Blockchain Technology (ICBCT'21). IEEE (2021)
38. Tan, S., Bhowmick, S., Chua, H.E., et al.: LATTE: visual construction of smart contracts. In: Proceedings of the 2020 ACM SIGMOD International Conference on Management of Data, pp. 2713–2716 (2020)
39. Seshu, S.: Introduction to the theory of finite-state machine. Proc IEEE **51**(9), 1275 (1963)
40. Maróti, M., Kereskényi, R., Kecskés, T., Völgyesi, P., Lédeczi, A.: Online collaborative environment for designing complex computational systems. Procedia Comput. Sci. **29**(2014), 2432–2441 (2014)
41. Chen, P.: Overview and application of mean time between failures (MTBF). Electron. Prod. Reliab. Environ. Test. **030**(B05), 272–276 (2012). (in Chinese with English abstract)
42. Wu, J.: Establishment and application of experimental model based on mean time between failure (MTBF). Electron. World **28**(1), 24–25 (2018) (in Chinese with English abstract)
43. Tsai, W.T., Wang, R., He, J., Deng, E.Y.: Decentralized digital asset exchanges: issues and evaluation. Ruan Jian Xue Bao/J. Softw. **33**(2): 410–433 (2022) (in Chinese). https://www.jos.org.cn/1000-9825/6329.html
44. Chinosi, M., Trombetta, A.: BPMN: An introduction to the standard. Comput. Stand. Interfaces **34**(1), 124–134 (2012)
45. Wood, M.F., Scott, A.: DeLoach. An overview of the multiagent systems engineering methodology. In: International Workshop on Agent-Oriented Software Engineering. Springer, Berlin (2000)

Blockchain Anomaly Transaction Detection: An Overview, Challenges, and Open Issues

Zhiwei Liu[1,3], Haoyu Gao[1,3], Hong Lei[1,2](✉), Zixuan Liu[1,3], and Chao Liu[4]

[1] Hainan University, Haikou 570228, China
liuzhiwei@hainanu.edu.cn, {haoyu,zixuan}@ssc-hn.com,
leiluono1@163.com
[2] SSC Holding Company Ltd, Chengmai 571924, China
[3] Oxford-Hainan Blockchain Research Institute, Chengmai 571924, China
[4] The Blockhouse Technology Limited, Oxford OX2 6XJ, UK
liuchao@tbtl.com

Abstract. In recent years, the rapid development of blockchain technology has attracted a great deal of attention from academia and industry, as it can be applied to a variety of traditional financial and non-financial domains. Blockchain provides decentralized, tamper-evident, and traceable characteristics that enhance the security of these domains. Recent researches have revealed, however, that there are some security abnormalities in the blockchain transaction process, and in order to solve these issues, the detection of the behavior of anomaly transaction is required. In this paper, we initially explore typical and abnormal transactions in blockchain technology before delving deeply into the integration of anomaly transaction detection algorithms in blockchain applications. Then, we examine conventional approaches for anomaly identification and blockchain-based techniques for transactional anomaly detection. Then, a thorough analysis of blockchain anomaly detection models in the financial domain and its application in non-financial domains was presented. Finally, based on the results of the survey, we conclude with future research directions and challenges.

Keywords: Blockchain · Transaction behavior · Anomaly detection · Detection model

1 Introduction

Blockchain, a booming and revolutionary technology, is decentralized, secure, anonymous, traceable, and tamper evident. The successful application of blockchain to digital currencies such as Bitcoin and Ethereum has led to its widespread development in the fintech sector. Blockchain technology is becoming one of the most promising technologies in the next-generation Internet interaction system [1]. In addition to cryptocurrencies, blockchain is proposed as one of the emerging digital industries in the Outline of the 14th Five-Year Plan and 2035 Visionary Goals for National Economic and Social Development of the People's Republic of China, which proposes "to develop blockchain service

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 126–140, 2024.
https://doi.org/10.1007/978-981-99-7161-9_10

platforms and financial technology, supply chain finance, and government services with a focus on alliance chains." As a result, blockchain technology has been applied to social services, risk management, medical care, and other fields [2]. However, most of the current research focuses on exploring the applications of blockchain technology in these fields, and although the characteristics of blockchain can solve the security and privacy problems that exist in these applications, abnormal behaviors may occur in the blockchain during transactions, reducing the security, privacy, and reliability of these applications. Although there are some studies on the security and privacy issues of blockchain, there is still a lack of systematic investigation into the security issues during the transactions of blockchain systems [3].

Based on the existing studies, blockchain-related application scenarios can be broadly classified into two categories, which are financial domain-related applications [4, 5, 6] and non-financial domain-related applications [7, 8, 9]. Since blockchain technology has natural financial attributes since its inception, it has more extensive and mature applications in the fintech field, and some relevant studies exist on the issue of security [10, 11, 12]. In the applications related to the blockchain financial field, users are making a large number of transactions every day, which are packaged by miners into blocks on the chain, however, there are inevitably some abnormal behaviors in the transaction process, and these behaviors, if not curbed, will disrupt the normal transaction order and harm the personal interests of users. In order to avoid these abnormal transaction behaviors, these studies detect the abnormal transaction behaviors existing in blockchain networks. However, in non-financial fields, such as social governance and government and livelihood scenarios, blockchain-related applications are mostly still in the exploration stage, and relatively few studies have been conducted for the detection of abnormal behaviors in these applications. Therefore, this paper discusses the anomalous behavior of blockchain-related application scenarios in financial and non-financial domains.

The rest of the paper is structured as follows. In Sect. 2, the concept of blockchain transactions is outlined, and blockchain normal and abnormal transactions are discussed separately. Section 3 discusses the anomaly detection methods in the traditional cybersecurity domain, and the characteristics and detection methods of blockchain anomalous transaction behavior. Next, Sect. 4 discusses the use of anomaly detection methods in different scenarios of blockchain, and Sect. 5 discusses future research approaches and challenges. Finally, in Sect. 6 we conclude on the basis of the survey.

2 Blockchain Transaction Behavior Overview

Transactions are a core concept in blockchain systems, and in this section, we discuss the concepts of blockchain normal and abnormal transactions, respectively.

2.1 Blockchain Transaction Definition

Transaction is a very important concept in the blockchain system. We usually regard the blockchain as a distributed ledger that is constantly synchronized in real time, in which any action can be considered as a transaction. After the introduction of smart contracts in blockchain, the contract call can also be regarded as a transaction, so the transaction in blockchain has gone beyond the definition of "value exchange", and a more precise definition is that the transaction is a record of a transaction in the blockchain. And no matter how big or small the transaction is, it needs the participation of transaction.

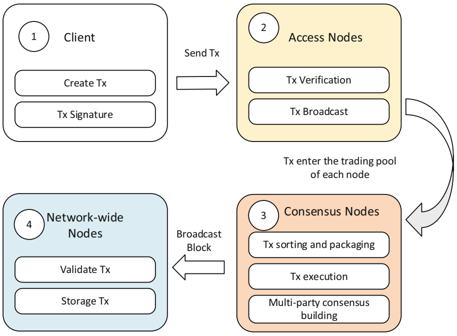


Fig. 1. Blockchain transaction process.

Figure 1 shows how a transaction is added to the blockchain as shown in the transaction flow in the blockchain. The user's request is given to the client, and the client creates a transaction and digitally signs the transaction; after sending the transaction to the access node, the node verifies the signature of the transaction to determine whether the transaction is legitimate, and the legitimate transaction will be broadcast to other nodes known to the node; next, the transaction is packaged as a block to be consensus, and then sent to each node, and after the node receives the block, it calls the block verifier After receiving the block, the node will call the block verifier to take out the transaction from the block one by one and execute it. Then the blockchain requires the nodes to reach consensus on the execution result of the block before the block can be released, and the node will start to release the block after reaching final consistency through different consensus algorithms; after the block is released by consensus, the node will verify the transaction and store the transaction and execution result in the block to the hard disk permanently.

2.2 Blockchain Abnormal Transaction Definition

In this paper, the complete process of a normal transaction in blockchain is discussed in Sect. 2.1, however, in the actual transaction process, there may be some anomalies, and we call the anomalies that exist in the blockchain transaction process as blockchain anomalous transactions, and in this section, we will introduce the definition of anomalous behavior and the classification of anomalous transactions in blockchain. Anomalous behavior exists widely in various fields, and there are different definitions for anomalies in different application fields. The book [13] classifies exceptions into three categories in the following manner, namely, point exceptions, contextual exceptions, and set exceptions.

Different from the above abnormal classification methods, blockchain abnormal transactions can be divided into two categories, one is the abnormal behavior generated by blockchain transactions themselves due to technical risks, and the other is the abnormal behavior that exists through analysis based on the data generated by blockchain transactions. The first category is the vulnerability arising from the risk of technical vulnerability or imperfect design of consensus algorithm in the process of blockchain transactions. Typical abnormal transaction behaviors exist due to technical risk, such as double flower attack, routing attack, 51% attack, etc. The second category is to analyze the data generated in blockchain transactions to conclude the existence of abnormal transactions, and such typical abnormal transaction risks include money laundering transactions, Ponzi schemes, fraudulent transactions, extortion transactions, etc.

3 Blockchain Abnormal Transaction Detection Analysis

This section first introduces the analysis framework of traditional anomalous behavior detection techniques, and then introduces the characteristics of blockchain anomalous transaction behavior and the corresponding detection methods.

3.1 Traditional Anomaly Detection Methods

In the traditional field of cybersecurity, anomaly detection is a very important data analysis task, which detects anomalous behavior from a given data set, and the increasing complexity of the network environment of the Internet has prompted the continuous updating of detection tools. Anomaly detection has been extensively studied in statistics and machine learning [14], while it is also known as outlier detection, novelty detection, deviation detection, and anomaly mining. Researchers have different definitions of anomalies in different fields, and Hawkins [15] gives a more universal definition: “An anomaly is an observation that deviates so much from other observations that it raises suspicion that it was generated by a different mechanism”. In addition to the field of cyber security, anomaly detection techniques are also widely used in healthcare, public health, fraud detection, intrusion detection, image processing, and other fields [16].

Figure 2 shows the traditional framework for network anomaly detection, where the input data is processed and then anomaly detection is performed in two ways (supervised, unsupervised), and the output results obtained are evaluated using a score-following-label situation [17]. The advantage of this generic framework for network anomaly detection is its simplicity, and the disadvantage is that the input data needs to be processed and only a single anomaly detection can be performed for different data types. This detection framework is also applicable in the field of blockchain anomaly transaction behavior detection due to the more uniform blockchain transaction data types. There are still some research challenges in the area of traditional network anomaly detection [17], despite the many available detection techniques, and current intrusion detection techniques are time-sensitive [18]. Anomaly detection techniques need to be continuously updated.

This section introduces that anomaly detection is widely used in various fields and there are some challenges in the traditional network security anomaly detection field, which also exist in blockchain anomalous transaction behavior detection. The next section focuses on how to extract and detect anomalous transaction behavior features of blockchain.

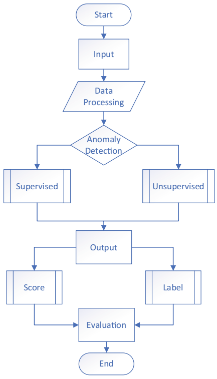


Fig. 2. General framework for traditional network anomaly detection

3.2 Blockchain Abnormal Transaction Behavior Feature Extraction and Detection

The literature [19] summarizes and analyzes the abnormal transaction behavior in blockchain from the basic features of smart contracts and the topology of blockchain networks, and the paper mentions that the behavioral features of Ponzi scheme, game gambling contract and social network contract in smart contracts can be constructed by the 14 basic features proposed by Hu et al. [20] to improve the recognition rate of smart contract classification. The study is to identify abnormal transactions by analyzing the features of the transactions to make judgments on the transaction patterns.

How to extract the features of abnormal trading behavior, different methods are used in [21], and to study whether there is market manipulation due to the drastic price fluctuations of cryptographic digital currencies, it uses complex networks to model users and transactions, proposes a framework for dynamic trading network analysis, uses Singular Value Decomposition (SVD) method to analyze the trading fluctuations of the network and found a great correlation between abnormal user behavior and price fluctuations, as shown in Abnormal transaction behavior Table 1, for six abnormal trading behaviors of users. These abnormal trading behaviors, except for the self-loop, each transaction between users is a normal transaction, but because there are too many transactions in a short period of time, the set of these transactions is judged as abnormal, which is also mentioned in the literature [13] for the set of abnormalities. However, the pattern of abnormal trading behavior obtained in this way to determine the abnormal behavior has some problems, and if a large number of accounts are created for trading at the same time, they can avoid being detected by this method, because there are a large number of accounts in the hands of some institutions.

To solve the problem of multiple account transactions, the attribution of accounts needs to be clarified, and the complex holding, and trading relationships in the market should be clarified, and the accounts in the virtual space should be related to the entities in reality. The complex relationships between entities and various accounts in the token ecosystem are revealed in the literature [22] by describing the characteristics of token creators, holders, and trading transfer activities, and by constructing an Ethereum token

Table 1. Abnormal transaction behavior

Abnormal transaction behavior	Description	Anomaly factors	Detected anomaly
Self-circulation	An account made 749 trades with itself	Self-Tx Tx frequency	Illegal Tx
Unidirectional	Account A made 322 sell trades to account B	Tx frequency	Malicious Tx
Bidirectional	Account A and account B traded with each other more than 150 times	Tx frequency	Malicious users
Triangular	There is a triangle-like structure between the three accounts	Recurring Tx	Malicious Tx
Polygonal	Many accounts form a polygon-like group	Recurring Tx	Malicious Tx group
Star-shaped	The star model has a core account that buys or sells bitcoins to many accounts	Tx Number	Malicious accounts

transaction network framework, using graph analysis, and proposing an algorithm to discover the potential relationships between tokens and other accounts. The literature [21] answers the association relationship between entities and accounts but does not explain why these entities hold these accounts.

When an account is determined to be an abnormal account, it is clear that transactions between abnormal accounts are abnormal transactions, and therefore the identification of abnormal accounts has been the focus of research in recent years. Previously machine learning methods [12, 23] were used to automatically detect anomalous contract accounts, however it was difficult to accurately identify the characteristics of anomalous contracts and obviously statistical analysis based on that contract was also invalid, and secondly overfitting of the model was caused by ignoring the imbalance and repetitiveness of smart contract accounts. In Ref. [24], the authors propose a data-driven robust method for detecting abnormal contract accounts in Ethereum, which first collects both abnormal and normal contract data from Ethereum to solve the problem of data imbalance. Next three types of feature sets are defined and combined to obtain a more comprehensive set of features.

4 Blockchain Anomaly Transaction Detection

In this section, we have discussed the blockchain anomaly transaction checking model in the financial domain and the blockchain application in the non-financial domain, respectively.

4.1 Financial Field

Blockchain technology has natural advantages in the field of fintech, so it has also been very widely used in the field of finance [4, 5, 6], bringing a brand new change to the development of the financial industry. However, the rapid development has also generated many related security and business risks, such as money laundering transactions, financial fraud, Ponzi schemes, market manipulation and other problems, which have brought heavy obstacles to the development of blockchain in the field of fintech. This section provides an in-depth study on the financial application scenarios of money laundering transactions and abnormal transactions detection in Ponzi schemes. The research related to transaction detection is analyzed in depth, as shown in Table 2.

Money Laundering Transactions. Due to the decentralized, and anonymous nature of blockchain, etc., It facilitates the transfer of funds for unscrupulous individuals. With the emergence of bitcoin and ethereum, it has further facilitated money laundering transactions and other illegal and criminal acts. In all major digital currency exchanges, there are unusual transactions for money laundering, and how to discern which transactions are money laundering transactions is gradually becoming a focus of blockchain researchers.

Teichmann et al. [25] showed that cryptocurrencies are a very suitable tool for money laundering, terrorism financing and corruption and that current compliance efforts in the field of cryptocurrencies are ineffective. The literature [26] specifically analyzes the risks associated with the uncontrolled use of blockchain technology by civil society, financial organizations, regulators, and law enforcement agencies, with a particular focus on the risks of money laundering through blockchain technology. Guerra et al. [27] analyze the problem of money laundering through crypto-assets and propose an approach to transnational anti-money laundering operations that uses tracking and reverse engineering anonymity techniques to track cryptocurrency transaction history, as well as employing a global blacklist of crypto-asset prefixes to prevent money laundering. Maksutov et al. [28] investigated transaction anonymization methods using a decentralized approach based on Coin Join transactions and showed that tracking Coin Join transactions is feasible to determine the fact that users are involved in creating transactions, providing additional advantages. Alarab et al. [29] performed a comparative analysis of the performance of classical supervised learning methods by using a recently published dataset from the Bitcoin blockchain to predict legal and illegal transactions in the network. Oad et al. [30] proposed a Blockchain-enabled Transaction Scanning (BTS) method to detect anomalous behavior, the BTS method specifies rules for outlier detection and fast flow of funds to limit anomalous behavior in transactions, and according to experimental results, the proposed BTS method automates the process of investigating transactions and limits the incidents of money laundering. Karasek-Wojciechowicz et al. [31] proposed Distributed Ledger Technology (DLT) based permissionless network, while ensuring the protection of personal data according to the EU General Data Protection Regulation (GDPR) rules, addressing the risk of money laundering and terrorist financing arising from anonymous blockchain spaces or exchanges with strong pseudonyms. Because virtual asset service providers are unable to identify originators and beneficiaries, Park et al. [32] propose a distributed ledger technology (DLT) based customer identification service model that enables virtual asset service providers to verify the identity of originators and beneficiaries. Other influential work includes [33], which explores the extent to which permissionless blockchain transactions can disrupt the current anti-money laundering (AML) regime and enforcement efforts, respectively.

Ponzi Scheme. In the financial field, blockchain is more likely to be packaged by unscrupulous elements as a ponzi scheme for fraud due to its complex technical principles and various financial projects. a ponzi scheme is a typical financial investment fraud scam that gives old investors lucrative interest and returns by continuously absorbing new investors' funds to create the illusion of making money to pull in more investments until the capital chain breaks and collapses, the organizers are unable to repay the principal and interest, and investors are left with nothing; Ponzi schemes have been found to scam considerable assets on the blockchain, which brings a very negative impact on blockchain technology.

To help deal with these problems, Chen et al. [23] proposed an approach to detect Ponzi schemes on the blockchain by using data mining and machine learning methods. Jung et al. [34] proposed an improved approach to provide a detection model for Ponzi schemes on Ethereum using data mining to benchmark several classification algorithms using Weka to obtain a model that simultaneously achieving high accuracy and high recall. Chen et al. [12] collected real-world samples to propose a classification model to detect smart Ponzi schemes, and by using the proposed approach, it is estimated that there are more than 500 smart Ponzi schemes running on Ethereum. Lou et al. [35] proposed an improved convolutional neural network as a detection model for Ponzi schemes in smart contracts. Bian et al. [36] proposed an image-based scam detection method using an attention capsule network focused on Ethereum. Chen et al. [37] proposed a semantic-aware Ponzi scam detection method for identifying Ponzi scams in Ethereum smart contracts. Fan et al. [38] introduced a new method to detect smart Ponzi schemes in blockchain, proposing an Anti-leakage Smart Ponzi Schemes Detection (Al-SPSD) model based on the idea of ordered boosting. Yu et al. [39] proposed a graph convolutional network (GCN)-based detection model to accurately distinguish Ponzi schemes contracts on different real-world Experiments on the Ethereum dataset show that the proposed model is effective in detecting Ponzi schemes compared to general machine learning methods.

Jin et al. [40] proposed a generic Heterogeneous Feature Augmentation module (HFAug) that can be combined with existing Ponzi scheme detection methods, and the experimental results showed the effectiveness of heterogeneous information for detecting Ponzi schemes. In their latest study, Jin et al. [41] introduced the Time-aware Metapath Feature Augmentation (TMFAug) module as a plug-and-play module that can help existing Ponzi scheme detection methods achieve significant performance improvements on Ethereum net datasets. TMFAug module, as a plug-and-play module, TMFAug can help existing Ponzi scheme detection methods achieve significant performance improvements on the Ethereum dataset, demonstrating the effectiveness of heterogeneous temporal information for Ponzi scheme detection.

4.2 Non-Financial Field

With the in-depth research on blockchain technology, its development in non-financial fields has also been rapid. Most of the current research is aimed at the exploration of blockchain technology in these application scenarios, with less attention to security

Table 2. Blockchain anomaly transaction detection in financial application scenarios.

Ref no	Main objective	Detected anomaly	Methods/Algorithm	Dataset
[27]	Proposes a framework of anti-money laundering principles with a focus on cryptocurrencies	Money laundering consolidation	Global crypto asset prefix blacklist	N/S
[28]	Detecting transactions involved in money laundering schemes	Money laundering transactions	Track coin join transactions	N/S
[29]	Compare classical supervised learning methods	Illegal Transactions	Aggregate Learning	Bitcoin Dataset
[30]	Blockchain-enabled Transaction Scanning	Money laundering transactions	Transaction scanning	N/S
[31]	License-free networks based on distributed ledger technology	Money laundering transactions	Unlicensed networks	N/S
[23]	Detecting Ponzi schemes on the blockchain through machine learning	Ponzi scheme	Machine learning	N/S
[34]	Using data mining to provide a detection model for Ponzi schemes on Ethereum	Ponzi scheme	Data mining	Ethereum
[12]	Detecting Ponzi Schemes Implemented as Smart Contracts on Blockchain	Ponzi scheme	Extraction of two types of features from the transaction history and operation code of smart contracts	Ethereum
[35]	An Intelligent Ponzi Scheme Detection Model Based on Improved Convolutional Neural Network	Ponzi scheme	Improved convolutional neural network	Ethereum

(*continued*)

issues. This section introduces the traceability and deposition applications of blockchain

Table 2. (*continued*)

Ref no	Main objective	Detected anomaly	Methods/Algorithm	Dataset
[36]	An image-based scam detection method	Ponzi scheme	Attention Capsule Network (SE-CapsNet)	Ethereum
[37]	A Semantic-Aware Ponzi Scheme Detection Method	Ponzi scheme	Semantic perception	Ethereum
[38]	An anti-leakage intelligent Ponzi scheme detection model based on the idea of ordered lifting is proposed	Ponzi scheme	Target statistics	Ethereum
[39]	A graph convolutional network (GCN) based detection model is proposed to accurately distinguish Ponzi scheme contracts	Ponzi scheme	GCN	Ethereum
[40]	Propose a generic heterogeneous feature enhancement module	Ponzi scheme	Capturing heterogeneous information related to account behavior patterns	Ethereum

technology in the non-financial field and discusses the challenges and future research directions in this field in the next chapter.

Supply Chain Traceability. With the rapid development of internet technology, a large number of emerging technologies have been applied to supply chain traceability systems; however, these current systems are centralized, opaque and monopolistic, which can lead to trust problems [42]. Blockchain technology has been applied to the field of supply chain traceability as a novel approach due to its decentralized and information traceability characteristics. However, the current blockchain-related research for supply chain traceability focuses on the exploration of applications and ignores the security risks in the blockchain transaction process, which brings certain obstacles to the development of blockchain technology.

Gálvez et al. [43] investigated the potential of blockchain technology to guarantee traceability and authenticity in the food supply chain. Caro et al. [44] proposed AgriBlockIoT, a fully decentralized, blockchain-based traceability solution for agri-food supply chain management that seamlessly integrates IoT devices that produce and consume digital data. Westerkamp et al. [45] proposed a blockchain-based supply chain traceability system using smart contracts. Salah et al. [46] proposed a method to efficiently execute business transactions using Ethereum blockchain and smart contracts for soybean tracking and tracing throughout the agricultural supply chain. The current prefabricated component supply chain management often faces challenges such as fragmentation, poor traceability, and lack of real-time information. To address these challenges, Wang et al. [47] developed a novel blockchain-based information management framework for precast supply chains that extends the application of blockchain in the construction supply chain domain. The contribution of Behnke et al. [48] is to identify boundary conditions for sharing guaranteed information to improve traceability. Shahid et al. [49] developed a novel blockchain-based information management framework for agricultural and food (Agri-Food) supply chain proposed a complete solution, the proposed traceability system writes all transactions to the blockchain and uploads the data to the Interplanetary File System (IPFS) to ensure the efficiency, security and reliability of the system.

Electronic Evidence. Blockchain technology solves some problems that arise in the collection, identification, storage and application of traditional electronic evidence, such as the possibility of tampering with evidence by forensic personnel cannot be ruled out, and the credibility of forensic tools is not verified and it is difficult to obtain evidence in a timely manner; using blockchain technology for forensics can reduce manual participation and exclude falsification by forensic personnel, and the credibility of forensic tools will be verified first during forensics. it can collect evidence quickly and prevent evidence from being replaced.

To ensure the authenticity, invariance, and auditability of electronic evidence, existing studies have used blockchain and related extensions. Tsai et al. [50] proposed a regulatory blockchain framework to facilitate the security and transparency of digital evidence during criminal investigations, which is implemented on an Ethereum smart contract to support the authenticity and digital evidence in the preliminary investigation, case management, and courtroom phases. Tian et al. [51] proposed a secure digital evidence framework using blockchain, which has a loosely coupled structure in which evidence and evidentiary information are maintained separately and only evidentiary information is stored in the blockchain while evidence is stored in a trusted storage platform. Kim et al. [52] proposed a two-level blockchain system that separates digital evidence into a hot blockchain and a cold blockchain in the process of criminal investigation, frequently changing information is stored in the hot blockchain, while unchanging data such as videos are stored in the cold blockchain. Miao et al. [53] address the data authenticity and integrity problems of traditional electronic evidence storage methods and the failure of existing blockchain storage schemes to consider storage cost and efficiency well; proposed an electronic evidence storage model that uses directed acyclic graph to optimize the on-chain storage efficiency of electronic evidence.

5 Challenges and Future Research Directions

5.1 Blockchain in Finance for Abnormal Transaction Detection

Key Challenge. According to our analysis of anomalous transaction detection models for blockchain-based applications related to the financial sector, we did not find any discussion on privacy protection in the related work. Stakeholders in blockchain networks are reluctant to share their complete data because complete privacy guarantees are not available.

Future Research Directions. The problem of protecting user privacy in anomalous transaction detection in blockchain needs to be addressed, and how to balance the relationship between privacy issues and anomaly detection issues is an urgent problem for relevant researchers to solve. To solve these problems, researchers can adopt methods such as differential privacy and zero-knowledge proof.

5.2 Blockchain in the Non-Financial Sector for Anomalous Transaction Detection

Key Challenges. The research on blockchain in the non-financial field mainly focuses on application-related exploration, and not enough attention is paid to the security issues in it. As the application of blockchain in the non-financial field gradually increases, the next research needs to increase the research on the security of blockchain in this field, especially the research on the abnormal transaction behavior in the non-financial application of blockchain is often easily ignored by the researchers.

Future Research Direction. Research is needed on the detection of abnormal behavior of blockchain transactions in the non-financial field, and how to solve the regulatory problems in blockchain transactions is an important problem that researchers need to solve.

6 Conclusion

With the emergence and popularity of digital cryptocurrencies, applications related to blockchain technology have attracted great interest from academia and industry. The decentralized nature of blockchain makes it a secure and trustworthy application platform, and it is widely used in various fields. Although blockchain is more secure and reliable compared to ordinary computer networks, it still has some vulnerabilities and is susceptible to malicious attacks. In order to ensure the safe operation of blockchain application platforms, abnormal transaction behaviors need to be identified in a timely manner. Therefore, anomaly detection techniques have started to be studied to identify abnormal behaviors in blockchain networks. In this paper, we dive into a comprehensive survey of anomalous transaction detection models in blockchain. First, we present the development of theoretical approaches related to anomaly detection in the traditional network security domain. Then, we discuss the researches related to the area of blockchain anomalous behavior detection and provide a detailed survey of anomalous transaction detection in the financial domain and related application research in the non-financial domain. Finally, we provide a comprehensive discussion of the challenges and future research directions that researchers in the area of anomalous transaction detection in blockchain systems need to focus on.

Acknowledgements. This work was supported in part by the National Key R&D Program of China (No. 2021YFB2700601); 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. Zheng, Z., Xie, S., Dai, H.N., Chen, X., Wang, H.: Blockchain challenges and opportunities: A survey. Int. J. Web Grid Serv. **14**(4), 352–375 (2018)
2. Monrat, A.A., Schelén, O.: A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access **7**, 117134–117151 (2019)
3. Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q.: A survey on the security of blockchain systems. Futur. Gener. Comput. Syst. **107**, 841–853 (2020)
4. Karagiannis, I., Mavrogiannis, K., Soldatos, J., Drakoulis, D., Troiano, E., Polyviou, A.: Blockchain based sharing of security information for critical infrastructures of the finance sector. In: International Workshop on Information and Operational Technology Security Systems. International Workshop on Model-Driven Simulation and Training Environments for Cybersecurity, International Workshop on Security for Financial Critical Infrastructures and Services pp, pp. 226–241. Springer, Cham (2020)
5. Huckle, S., Bhattacharya, R., White, M., Beloff, N.: Internet of things, blockchain and shared economy applications. Proc. Comput. Sci. **98**, 461–466 (2016)
6. Moncada, R., Ferro, E., Favenza, A., & Freni, P.: Next Generation Blockchain-Based Financial Services. In: European Conference on Parallel Processing pp. 30–41. Springer, Cham (2021)
7. Wang, Z., Wang, L., Chen, Q., Lu, L., Hong, J.: A traditional chinese medicine traceability system based on lightweight blockchain. J. Med. Internet Res. **23**(6), e25946 (2021)
8. Kumar, R., & Tripathi, R.: Traceability of counterfeit medicine supply chain through Blockchain. In: 2019 11th international conference on communication systems & networks (COMSNETS) pp. 568–570. IEEE, (2019)
9. Wang, L., Ma, Y., Zhu, L., Wang, X., Cong, H., Shi, T.: Design of integrated energy market cloud service platform based on blockchain smart contract. Int. J. Electr. Power Energy Syst. **135**, 107515 (2022)
10. Badawi, E., Jourdan, G.V.: Cryptocurrencies emerging threats and defensive mechanisms: A systematic literature review. IEEE Access **8**, 200021–200037 (2021)
11. Chatzigiannis, P., & Chalkias, K.: Proof of assets in the diem blockchain. In International Conference on Applied Cryptography and Network Security pp. 27–41. Springer, Cham (2021)
12. Chen, W., Zheng, Z., Ngai, E.C.H., Zheng, P., Zhou, Y.: Exploiting blockchain data to detect smart ponzi schemes on ethereum. IEEE Access **7**, 37575–37586 (2019)
13. Ben-Gal, I.: Outlier detection. In Data mining and knowledge discovery handbook pp. 131–146. Springer, Boston, MA (2005)
14. Pathan, A. S. K. (Ed.).: The state of the art in intrusion prevention and detection (Vol. 44). Boca Raton, CRC press (2014)
15. Hawkins, D.: Identification of Outliers (Monographs on Statistics and Applied Probability) (2013)
16. Ahmed, M., Anwar, A., Mahmood, A. N., Shah, Z., & Maher, M. J.: An investigation of performance analysis of anomaly detection techniques for big data in Scada systems. EAI Endorsed Trans. Ind. Networks Intell. Syst., 2(3), e5 (2015)

17. Ahmed, M., Mahmood, A.N., Hu, J.: A survey of network anomaly detection techniques. J. Netw. Comput. Appl. **60**, 19–31 (2016)
18. Chao, H.C.: Dependable multimedia communications: Systems, services, and applications. J. Netw. Comput. Appl. **34**(5), 1447–1448 (2011)
19. Han, H., Chen, Y., Guo, C., & Zhang, Y.: Blockchain Abnormal Transaction Behavior Analysis: a Survey. In International Conference on Blockchain and Trustworthy Systems pp. 57–69. Springer, Singapore (2021)
20. Hu, T., Liu, X., Chen, T., Zhang, X., Huang, X., Niu, W., ... & Liu, Y.: Transaction-based classification and detection approach for Ethereum smart contract. Inform. Process. Manag. 58(2), 102462 (2021)
21. Chen, W., Wu, J., Zheng, Z., Chen, C., & Zhou, Y.: Market manipulation of bitcoin: Evidence from mining the Mt. Gox transaction network. In: IEEE INFOCOM 2019-IEEE conference on computer communications pp. 964–972. IEEE, (2019)
22. Chen, W., Zhang, T., Chen, Z., Zheng, Z., Lu, Y.: Traveling the token world: A graph analysis of ethereum erc20 token ecosystem. In Proceedings of The Web Conference **2020**, 1411–1421 (2020)
23. Chen, W., Zheng, Z., Cui, J., Ngai, E., Zheng, P., & Zhou, Y.: Detecting ponzi schemes on ethereum: Towards healthier blockchain technology. In: Proceedings of the 2018 world wide web conference, pp. 1409–1418 (2018)
24. Aljofey, A., Rasool, A., Jiang, Q., Qu, Q.: A feature-based robust method for abnormal contracts detection in ethereum blockchain. Electronics **11**(18), 2937 (2022)
25. Teichmann, F. M. J., & Falker, M. C.: Cryptocurrencies and financial crime: solutions from Liechtenstein. J. Money Launder. Control (2020)
26. Amosova, N., Kosobutskaya, A. Y., & Rudakova, O.: Risks of unregulated use of blockchain technology in the financial markets. In 4th International Conference on Economics, Management, Law and Education (EMLE 2018) pp. 9–13. Atlantis Press (2018)
27. Guerra, G.R., Marcos, H.J.B.: Legal remarks on the overarching complexities of crypto anti-money laundering regulation. Revista Juridica **4**(57), 83–115 (2019)
28. Maksutov, A. A., Alexeev, M. S.: Detection of blockchain transactions used in blockchain mixer of coin join type. In: 2019 IEEE conference of russian young researchers in electrical and electronic engineering (EIConRus) pp. 274–277. IEEE, (2019)
29. Alarab, I., Prakoonwit, S., & Nacer, M. I.: Comparative analysis using supervised learning methods for anti-money laundering in bitcoin. In Proceedings of the 2020 5th International Conference on Machine Learning Technologies, pp. 11–17 (2020)
30. Oad, A., Razaque, A., Tolemyssov, A., Alotaibi, M., Alotaibi, B., Zhao, C.: Blockchain-enabled transaction scanning method for money laundering detection. Electronics **10**(15), 1766 (2021)
31. Karasek-Wojciechowicz, I.: Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces. J. Cybersecurity 7(1), tyab004 (2021)
32. Park, K., Youm, H.Y.: Proposal for customer identification service model based on distributed ledger technology to transfer virtual assets. Big Data Cogn. Comput. **5**(3), 31 (2021)
33. Hughes, S. J.: 'Gatekeepers' are vital participants in anti-money-laundering laws and enforcement regimes as permission-less blockchain-based transactions pose challenges to current means to 'Follow the Money'. Indiana Legal Studies Research Paper, (408) (2019)
34. Jung, E., Le Tilly, M., Gehani, A.: Data mining-based ethereum fraud detection. In: 2019 IEEE International Conference on Blockchain (Blockchain), pp. 266–273. IEEE (2019)
35. Lou, Y., Zhang, Y., & Chen, S.: Ponzi contracts detection based on improved convolutional neural network. In: 2020 IEEE International Conference on Services Computing (SCC) pp. 353–360. IEEE (2020)

36. Bian, L., Zhang, L., Zhao, K., Wang, H., Gong, S.: Image-based scam detection method using an attention capsule network. IEEE Access **9**, 33654–33665 (2021)
37. Chen, W., et al.: Sadponzi: Detecting and characterizing ponzi schemes in ethereum smart contracts. Proc. ACM Meas. Anal. Comput. Syst. **5**(2), 1–30 (2021)
38. Fan, S., Fu, S., Xu, H., Cheng, X.: Al-SPSD: Anti-leakage smart Ponzi schemes detection in blockchain. Inf. Process. Manage. **58**(4), 102587 (2021)
39. Yu, S., Jin, J., Xie, Y., Shen, J., & Xuan, Q.: Ponzi scheme detection in ethereum transaction network. In: International Conference on Blockchain and Trustworthy Systems pp. 175–186. Springer, Singapore (2021)
40. Jin, C., Jin, J., Zhou, J., Wu, J.: Heterogeneous Feature Augmentation for Ponzi Detection in Ethereum. Express Briefs, IEEE Transactions on Circuits and Systems II (2022)
41. Jin, C., Zhou, J., Jin, J., Wu, J., & Xuan, Q.: Time-aware metapath feature augmentation for ponzi detection in ethereum. arXiv preprint arXiv:2210.16863 (2022)
42. Tian, F. (2017, June). A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In: 2017 International conference on service systems and service management pp. 1–6. IEEE (2017)
43. Galvez, J.F., Mejuto, J.C.: Future challenges on the use of blockchain for food traceability analysis TrAC. Trends Anal. Chem. **107**, 222–232 (2018)
44. Caro, M. P., Ali, M. S., Vecchio, M., & Giaffreda, R.: Blockchain-based traceability in Agri-Food supply chain management: A practical implementation. In: 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany) pp. 1–4. IEEE (2018)
45. Westerkamp, M., Victor, F., & Küpper, A.: Blockchain-based supply chain traceability: Token recipes model manufacturing processes. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1595–1602. IEEE (2018)
46. Salah, K., Nizamuddin, N., Jayaraman, R., Omar, M.: Blockchain-based soybean traceability in agricultural supply chain. IEEE Access **7**, 73295–73305 (2019)
47. Wang, Z., Wang, T., Hu, H., Gong, J., Ren, X., Xiao, Q.: Blockchain-based framework for improving supply chain traceability and information sharing in precast construction. Autom. Constr. **111**, 103063 (2020)
48. Behnke, K.: Boundary conditions for traceability in food supply chains using blockchain technology. Int. J. Inf. Manage. **52**, 101969 (2020)
49. Shahid, A., Almogren, A., Javaid, N., Al-Zahrani, F.A., Zuair, M., Alam, M.: Blockchain-based agri-food supply chain: A complete solution. IEEE Access **8**, 69230–69243 (2020)
50. Tsai, F.C.: The application of blockchain of custody in criminal investigation process. Proc. Comput. Sci. **192**, 2779–2788 (2021)
51. Tian, Z., Li, M., Qiu, M., Sun, Y., Su, S.: Block-DEF: A secure digital evidence framework using blockchain. Inf. Sci. **491**, 151–165 (2019)
52. Kim, D., Ihm, S.Y., Son, Y.: Two-level blockchain system for digital crime evidence management. Sensors **21**(9), 3051 (2021)
53. Miao, Z., Ye, C., Yang, P., Chen, Y., & Chen, Y.: Blockchain-based electronic evidence storage and efficiency optimization. In: 2021 international conference on artificial intelligence and blockchain technology (AIBT) pp. 109–113. IEEE (2021)

Detection Method of Insulation Gloves Wearing in Complex Scenes Based on Improved YOLOX

Tao Wang[1,2,3], Pengyu Liu[1,2,3](✉), and Xiao Wang[1,2,3]

[1] Beijing University of Technology, Beijing 100124, China
liupengyu@bjut.edu.cn
[2] Laboratory of Advanced Information Networks, Beijing 100124, China
[3] Beijing Key Laboratory of Computational Inteligence and Inteligent System, Beijing 100124, China

Abstract. Supervision of wearing insulation gloves during electrical equipment inspection is the top priority of safety protection in indoor and outdoor high-voltage power areas. However, in the actual scene, there are usually incomplete features of monitoring targets and insufficient feature information of small-scale targets caused by factors such as occlusion and distance, which leads to low accuracy of inspection personnel wearing insulation gloves. In view of the above situation, this paper proposes an improved testing model for insulation gloves. Firstly, SCAM attention mechanism and M-MHSA module were integrated into the feature extraction network to improve the ability of the model to extract global information and target channel features combined with multi-head attention mechanism. Adding small target detection layer and using weighted bidirectional feature pyramid network (BiFPN) to carry out multi-scale feature fusion can improve the detection ability of the model on different scale targets. The experimental results show that the improved algorithm achieves 93.27% average accuracy and 32frame/s detection speed in indoor and outdoor high-voltage electricity usage scenarios, which has good performance in the detection task of insulation gloves.

Keywords: Insulation gloves detection · Multi-head attention · BiFPN · Feature fusion

1 Introduction

High voltage rooms and outdoor distribution areas are the key areas of indoor and outdoor high voltage electricity consumption. At present, the supervision measure is often to send safety supervisors to accompany the inspection. However, this supervision method depends on the safety awareness of personnel, and there are problems such as high labor cost and low efficiency. With the continuous development of computer technology, the detection of insulating glove wearing based on surveillance video has gradually become a research hotspot of this problem. Many scholars have carried out relevant research on this, and the current methods mainly include traditional detection methods and methods based on deep learning. Traditional methods usually use morphological

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 141–151, 2024.
https://doi.org/10.1007/978-981-99-7161-9_11

operations combined with color and shape features to detect insulated gloves. Mummadi et al. used the difference of glove shape to detect the area of the human hand and realized the detection of wearing insulation gloves, but they were easily affected by light [1]. Yu K et al. used edge detection algorithm to extract the contour of the hand and combined color and shape information to determine whether gloves were worn [2]. Since the traditional detection method is suitable for ideal scenes and easily affected by factors such as illumination, color difference and scale size, the accuracy of detection needs to be improved. With the development of deep learning technology, it also provides new ideas for the detection of insulating gloves wearing. Jin et al. proposed a detection model of insulating glove wearing based on convolutional neural network by improving the VGG-16 network, but there was a problem of missed detection [3]. Zhao et al. proposed an insulating glove wearing detection algorithm combined with Gamma transform by improving YOLOv3, which successfully improved the detection accuracy of insulating glove wearing under different illumination [4]. However, the above research methods have the problem of low detection accuracy in the case of incomplete target features under occlusion and small size targets. In view of the good accuracy and detection speed of YOLO series algorithms in object detection, based on YOLOX, this paper integrates SCAM attention mechanism into the feature extraction network to enhance the edge feature extraction ability, and replaces the last layer of the feature extraction network with the M-MHSA module to improve the global information of the model. Finally, a small object detection layer and a weighted bidirectional feature pyramid network are added to improve the feature fusion effect of small-scale objects [5]. Through comparative experiments, it is concluded that the detection effect of the proposed method is better than that of the common object detection algorithms such as YOLOX, which can effectively solve the detection problem of insulating gloves wearing in complex scenes.

2 Improved Target Detection Network

2.1 Network Structure

The improved object detection network proposed in this paper is mainly divided into three parts: backbone network, Neck network and prediction network. SCAM attention module is integrated into the backbone network to improve the extraction ability of target content features through its channel attention mechanism, and the spatial attention mechanism is used to improve the positioning ability of target location information. The M-MASH module is introduced at the end, and the multi-head attention mechanism of the transformer is combined to improve the ability of the model to extract global information. In the Neck network, BiFPN structure is used to replace the traditional PANet structure to speed up the fusion of multi-scale features, and finally sent to YoloHead for target prediction [6]. The overall structure is shown in Fig. 1 below.

The input image first passes through a Focus network structure, whose main role is to extract pixels from the high-resolution image and reconstruct them into the low-resolution image to obtain the corresponding feature layer. By stacking the channels, the width and height information is concentrated into the channel information to expand the receptive field and reduce the amount of calculation. After the Focus module, the image is extracted through four structures composed of Conv module and CSP Layer

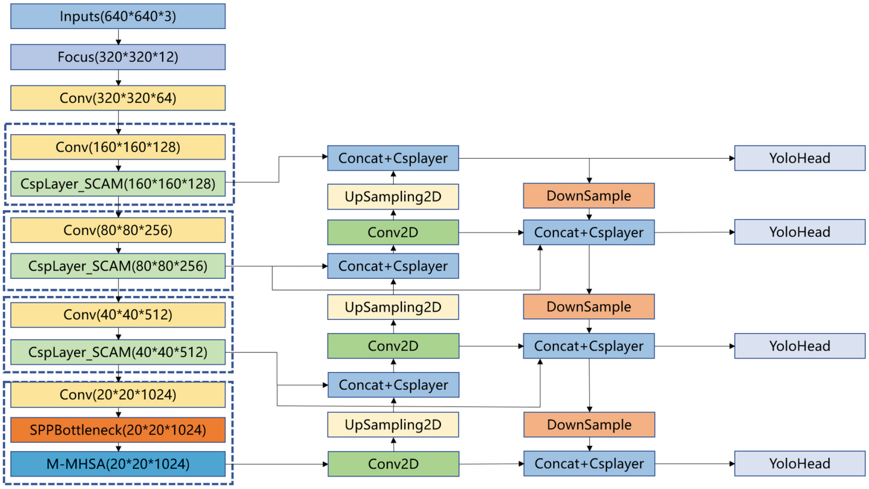


Fig. 1. Network structure diagram

module. In order to suppress the interference of general features in the process of feature extraction, the SCAM attention mechanism is introduced into the CSPLayer structure, which mainly includes the channel attention module and the spatial attention module[6]. Its specific structure is shown in Fig. 2 below.

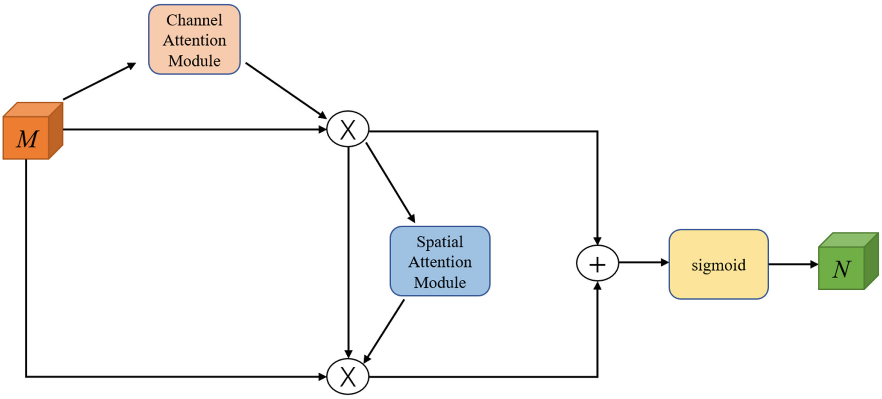


Fig. 2. Structure diagram of SCAM attention module

The input feature M first passes through the channel attention module, and the spatial dimension of the feature map is compressed by max pooling and average pooling, and obtains the corresponding max pooling features and average pooling features. The channel attention feature weights are generated through the multi-layer perceptron and multiplied with the input features to obtain the channel attention feature map, so as to improve the extraction ability of the target content features. Secondly, the channel attention feature map obtains the corresponding spatial attention weight through the spatial attention module, and obtains the spatial attention feature map by multiplying it with the channel attention feature map, so as to improve the positioning ability of target location information. Since the channel attention feature map has more semantic information than the original input feature M, which may make the attention area more concentrated and the receptive field smaller, it is easy to ignore the attention edge features. Therefore, the input feature M is multiplied with the spatial attention and added with the channel attention feature map, and the final output feature N is obtained by the sigmoid function [7]. In order to improve the model's ability to perceive global information and extract global features, while avoiding the loss of context information caused by prematurely using the transformer structure in the network to force the regression boundary, this paper replaces the last layer of the backbone network with the M-MHSA module, whose specific structure is shown in Fig. 3 below.

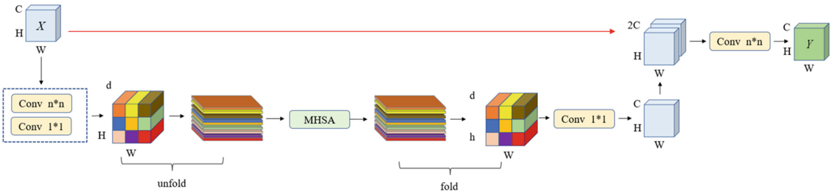


Fig. 3. Structure diagram of M-MHSA

For a feature map X with the input size of H × W × C, the local spatial information is encoded through the convolution operation with the convolution kernel size of 3 × 3, and then the tensor information is projected into the high-dimensional space through 1 × 1 convolution to obtain the feature map with the size of H × W × d. After the feature layer is expanded, multi-head self-attention mechanism is used for encoding [8]. The structure of the self-attention mechanism is shown in Fig. 4. The results of each self-attention mechanism can be calculated by Formula (1):

$$\text{head} = \text{softmax}\left(\frac{qk^T}{\sqrt{d_k}}\right)v \tag{1}$$

where q, k and v are the query vector, key vector and value vector of the self-attention mechanism respectively, and d_k is the dot product of the query vector and value vector. Since the size of the last feature layer of the feature extraction network of the algorithm in this paper is 20x20, four self attention mechanisms are used to form a multi head self attention mechanism for spatial information coding. Each self attention mechanism is used to calculate the relationship between different location pixels to improve the extraction ability of the global location feature information of the model [9]. The results calculated by the multi-head attention mechanism are re-adjusted into the feature map of H × W × d after folding operation, the feature map is projected into the low-dimensional space through 1 × 1 convolution, and the original feature map X is spliced to fuse the feature map with spatial position information and the original input feature map, so as to improve the overall global feature extraction ability. Finally, the number of channels

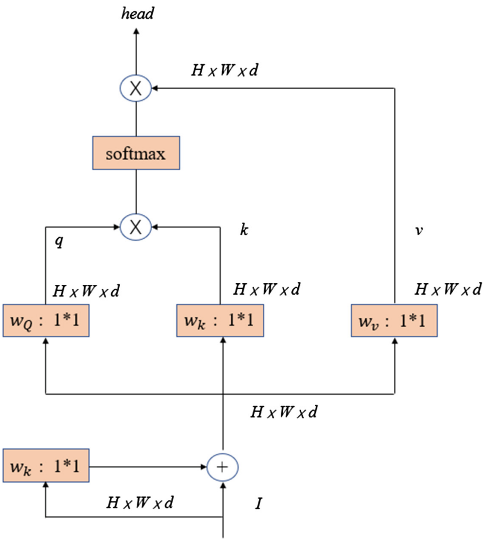


Fig. 4. Structure diagram of multi-head self-attention mechanism

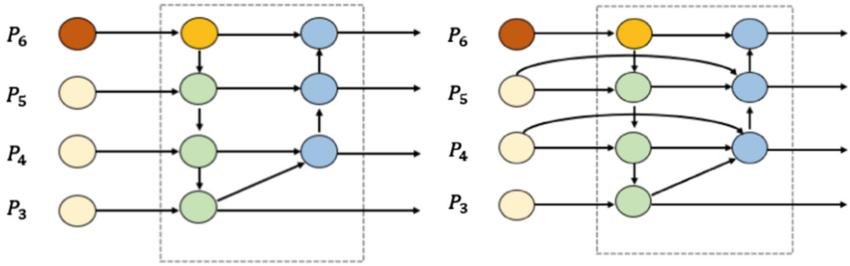
of the feature map is adjusted to be consistent with the input feature map by convolution operation for feature fusion at different scales.

The feature map obtained by the feature extraction network contains four different sizes of 160 × 160, 80 × 80, 40 × 40 and 20 × 20. The feature fusion between different sizes is carried out through the BiFPN structure of the Neck network, so the feature pyramid of the Neck network part is optimized below [10].

2.2 Improved Feature Pyramid Structure

The Neck network of the original YOLO series target detection model uses the combination of FPN and PANet to construct the feature pyramid network, the specific structure is shown in Fig. 5a. FPN transfers the strong semantic information of deep features to shallow features, and PANet transfers the strong location information of shallow features to deep features. Through the combination of FPN and PANet, the parameter aggregation of different size detection layers is realized, and finally the feature fusion between different levels is realized [11, 12]. The input of PANet is the feature information processed by FPN, but the original feature information extracted by backbone network is missing, which may lead to the problem of learning bias. Therefore, this paper uses BiFPN structure to improve the feature pyramid, which is shown in Fig. 5b.

Firstly, nodes with only one input end and one output end are screened out. If the input node and output node are in the same layer, the original feature layer of the corresponding backbone network is introduced to the PANet node for multi-scale feature fusion. At this time, the input of PANet is composed of the feature information processed by FPN and the original feature information. After the feature information of the original feature extraction network is involved in the calculation, the effect of feature fusion can be effectively improved, and the calculation amount of the model can be reduced



(a)PANet (b)BiFPN

Fig. 5. Pyramid structure with different features

by weight adjustment [13]. The prediction process mainly involves post-processing the feature maps of four different sizes. After 1 × 1 convolution, the loss is calculated and a feature vector including class probability, bounding box score and confidence is generated. The calculation of loss is mainly divided into three parts: classification loss, location loss and confidence loss. The total loss is the sum of the three types of loss, and the smaller the total loss value, the higher the detection performance of the model [6]. The confidence loss and classification loss are calculated based on the binary cross entropy loss function, which are used to calculate the probability of the real labeled target category in the model prediction rectangle box and the probability of the real labeled target category in the model prediction rectangle box. The localization loss is used to calculate the error between the predicted target box and the real target box, and IOU is often used as the index [14]. However, there are problems of low regression accuracy and missed detection of occluded targets, so the following will be improved from this aspect.

2.3 Optimization Loss Function

The traditional YOLO series models use IOU to calculate the coincidence between the predicted box and the true box and calculate the loss, and the calculation formula is shown in Formula (2):

$$IOU = \frac{A \cap B}{A \cup B} \tag{2}$$

For the occlusion phenomenon in the detection of insulated gloves, the border regression accuracy of IOU is low, and in the case of no intersection between the predicted box and the real box, the value of IOU is 0, which cannot reflect the distance between two boxes and cannot return the gradient. Therefore, DIOU is used as the loss function of prediction box in this paper for improvement [15]. The specific calculation formula is as follows:

$$DIOU = 1 - IOU + \frac{\rho(b, b_{gt})}{c^2} \tag{3}$$

where b and b_{gt} represent the center points of the predicted and true boxes, ρ represents the Euclidean distance between the two center points, and c represents the minimum diagonal distance of the bounding rectangle that can cover both the predicted and true boxes. The DIOU is obtained by calculating the distance ratio between the predicted box, the true box, and the minimum enclosing rectangular box [16]. Non-maximal suppression will set the prediction box whose DIOU is greater than the threshold to 0 when filtering unnecessary candidate boxes, which may cause the problem of missing targets in dense areas. Therefore, a more moderate calculation method is adopted in this paper, and the score of the prediction box will be given according to the size of the overlap area instead of directly setting 0 when calculating the score [17, 18]. The specific calculation formula is as follows:

$$S_i = \begin{cases} S_i & IoU(P,b_i)<Q \\ S_i(1-IoU(P,b_i)) & IoU(P,b_i)\geq Q \end{cases} \tag{4}$$

where S_i represents the score of the current predicted box, b_i is the current detected box, P is the detected box with the highest score, and Q is the threshold of the intersection over union ratio.

3 Experimental Results

3.1 Data Sets and Environment Analysis

The data set used in this paper consists of images taken in high voltage chambers and outdoor power distribution areas. There are a total of 3519 images, including two types of objects with and without insulated gloves. In order to avoid the phenomenon of overfitting during the network training, we adopted stretching, translation, rotation and other methods to enhance the data samples, and finally expanded the data set to 9726 pieces. The image annotation software LabelImg was used for annotation, and the training set, verification set and test set were divided in a ratio of 8:1:1, and the size of the input image was 640 × 640.

The operating system running the experiment is Ubuntu20.04, the CPU is intel-i9-12900 k, and the GPU is NVIDIA GeForce 3090. The training was performed with a learning rate of 0.0006, Batchsize of 32, epochs of 100, and adam as the optimizer.

3.2 Index of Evaluation

In order to accurately evaluate the detection effect of the model, this paper uses Precision, Recall, Average Precision (AP) and Mean Average Precision (mAP) as evaluation indicators to measure the performance of the model, and the specific calculation formula is shown in the following:

$$Precision = \frac{TP}{TP + FP} \tag{5}$$

$$Recall = \frac{TP}{TP + FN} \tag{6}$$

$$AP{=}\int_0^1 Precisiond(Recall) \tag{7}$$

$$mAP = \frac{1}{n}\sum_{i=1}^{n} AP_i \tag{8}$$

where, *TP* indicates that the model prediction is positive and the real annotation is positive, *FP* indicates that the model prediction is positive and the real annotation is negative, and *FN* indicates that the model prediction is negative and the real annotation is positive. The value of *AP* is used to evaluate the prediction effect of a certain type of target. Generally, the value of *Precision* is the value obtained by integrating *Recall* within the interval (0,1). *mAP* is the mean value of *AP* of multiple types of targets, where *n* is the number of categories and *i* is the current category number.

3.3 Contrast Experiment

3.3.1 Qualitative analysis

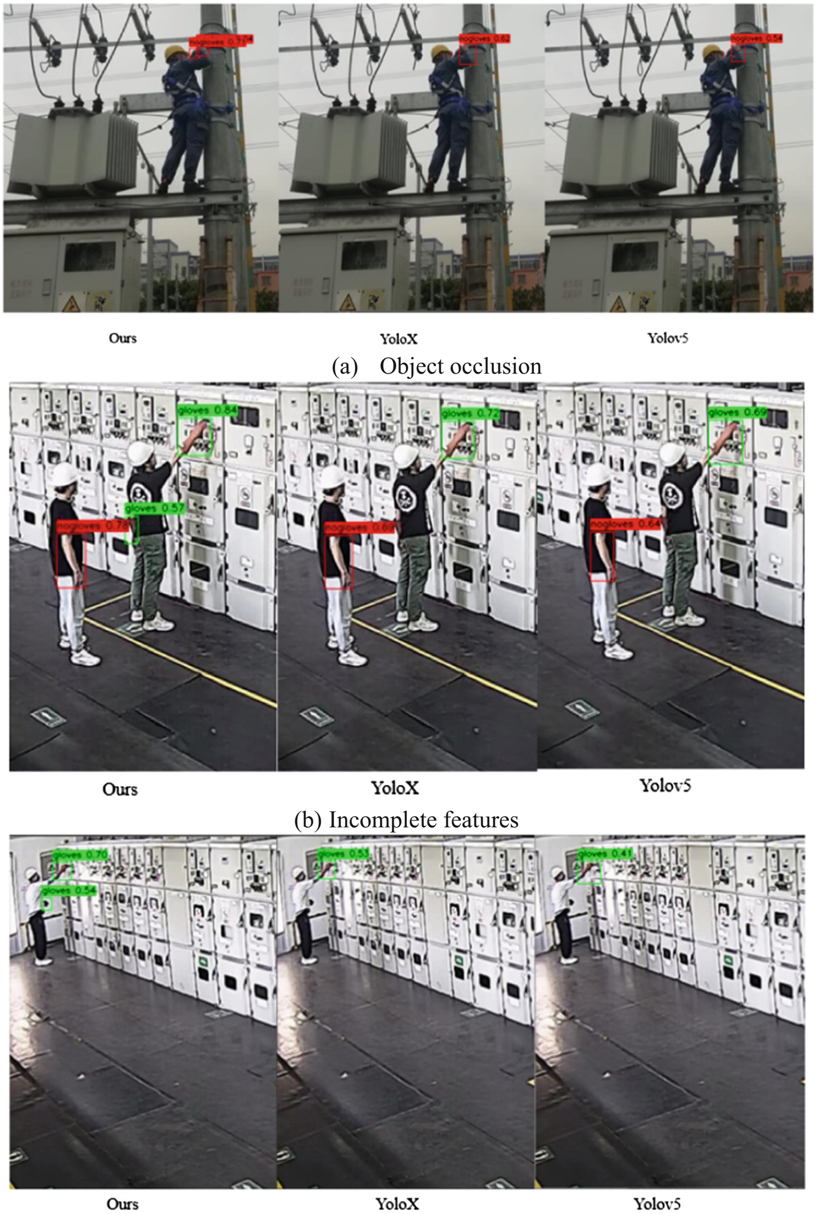
In order to verify the performance of the proposed algorithm, this paper chooses to compare with the current common YoloX and Yolov5 algorithms, and conducts comparative experiments in the case of object occlusion, incomplete features in the process of human activities and small-scale targets. The experiment uses 80% of the dataset built in this paper as the training set, 10% of the dataset and some public images as the test set. The operating system running the experiment is Ubuntu20.04, the CPU is intel-i9-12900k, the GPU is NVIDIA GeForce 3090, and the training epoch is 100. The specific effect is shown in Fig. 6 below. It can be seen from the figure that in the above circumstances, other algorithms all have the situation of missing targets, and the confidence is lower than that of the proposed algorithm. The detection speed of the proposed method in this paper can reach 32frame/s, which is still able to maintain a good detection speed compared with the 29frame/s of Yolov5 and the 38frame/s of YoloX, which is enough to prove the effectiveness of the proposed method.

3.3.2 Quantitative Analysis

In order to better prove the effectiveness of the method proposed in this paper, we choose the original YOLOX model as the benchmark, combine the multiple modules proposed in this paper and common object detection algorithms for comparative experiments, and use *mAP* as the evaluation index to measure the accuracy of insulating glove detection. The specific results are shown in Table 1. According to the results in the table, the *mAP* is improved after using the proposed module, and the *mAP* of the proposed final algorithm reaches 93.27%, which is better than the common object detection algorithms, which is enough to prove the feasibility of the proposed method in the detection task of insulating gloves in complex indoor and outdoor scenes.

4 Conclusion

In order to solve the problem of poor detection accuracy caused by the insulation glove wearing detection technology in complex scenes due to factors such as occlusion and small size targets, this paper integrated the SCAM attention mechanism module into



(a) Object occlusion

(b) Incomplete features

(c) Small-scale objectives

Fig. 6. The results of different algorithms are compared

the CSPLayer layer of feature extraction network to improve the model's ability to extract feature information and position information. The last convolutional layer of the feature extraction layer is replaced by the M-MHSA module, and the multi-head

Table 1. Model performance comparison table

Model	Precision (%)	Recall (%)	mAP (%)	FPS
YOLOv5s	79.13	74.27	76.33	29
YOLOX	81.21	78.17	86.91	38
YOLOX + SCAM	85.59	81.63	83.97	37
YOLOX + M-MHSA	83.01	80.74	82.35	36
YOLOX + SCAM + M-MHSA	89.37	85.32	87.12	34
YOLOX + SCAM + M-MHSA + BiFPN	92.27	89.41	91.37	33
Ours	94.78	90.56	93.27	32

attention mechanism is combined to improve the global information extraction ability of the model. Secondly, a small target detection layer is added. At the same time, BiFPN structure is used to fuse the feature information of the original feature layer during feature fusion and speed up multi-scale feature fusion. Finally, DIOU is used to improve the original algorithm to reduce the problem of target missing detection. The experimental results show that the proposed method can effectively solve the problem of insulating glove wearing detection in complex scenes, and the final *mAP* reaches 93.27%. In the future, we will consider further reducing the number of parameters of the model to improve the detection speed of the model.

Funding Statement. This paper was supported by the Natural Science Foundation of Beijing (4212001) and the Key Research and Transformation Project of Qinghai Province (2022-QY-205).

Conflicts of Interest. The authors declare no conflict of interest.

References

1. Mummadi, C. K., Philips Peter Leo, F., Deep Verma, K.: Real-time and embedded detection of hand gestures with an IMU-based glove. Informatics. MDPI J. **5**(2), 28–31(2018)
2. Yu, K., Liu, H., Li, T.: A protective equipment detection algorithm fused with apparel check in electricity construction. In: 2021 33rd Chinese Control and Decision Conference (CCDC), pp.3122–3127. IEEE (2021)
3. Jin, M., Chen, X., Lai, G., et al.: Glove detection system based on VGG-16 network. In: 2020 13th international symposium on computational intelligence and design (ISCID), pp.172–175. IEEE (2020)
4. Zhao, B., Lan, H., Niu, Z.: Detection and location of safety protective wear in power substation operation using wear-enhanced YOLOv3 algorithm, pp. 125540–125549. IEEE Access (2021)
5. Zhaosheng, Y., Tao, L., Tianle, Y.: Rapid detection of wheat ears in orthophotos from unmanned aerial vehicles in fields based on YOLOX. Front. Plant Sci. 851245–851245 (2022)
6. Cheng, X., Lu, T.: An improved YOLOv5s for protective gear detection. In: 2022 7th international conference on intelligent computing and signal processing (ICSP), pp. 661–665. IEEE (2022)

7. Woo, S., Park, J., Lee, J. Y.: Cbam: Convolutional block attention module. In: Proceedings of the European conference on computer vision (ECCV), pp. 3–19 (2018)
8. Panboonyuen, T., Thongbai, S., Wongweeranimit, W.: Object detection of road assets using transformer-based YOLOX with feature pyramid decoder on thai highway panorama. Inform J **13**(1), 5–9 (2022)
9. Yu, Y., Zhao, J.: Gong Q:Real-time underwater maritime object detection in side-scan sonar images based on transformer-YOLOv5. Remote Sensing J **13**(18), 3555–3559 (2021)
10. Tan, M., Pang, R., Le, Q. V.: Efficientdet: scalable and efficient object detection. In: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 10781–10790. IEEE (2020)
11. Gong, Y., Yu, X., Ding, Y.: Effective fusion factor in FPN for tiny object detection. In: Proceedings of the IEEE/CVF winter conference on applications of computer vision, pp. 1160–1168. IEEE (2020)
12. Wang, K., Liew, J. H., Zou, Y.: Panet: Few-shot image semantic segmentation with prototype alignment. In: Proceedings of the IEEE/CVF International Conference on Computer Vision, pp. 9197–9206. IEEE (2019)
13. Chen, J., Mai, H. S., Luo, L.: Effective feature fusion network in BIFPN for small object detection. In: 2021 IEEE International Conference on Image Processing (ICIP), pp. 699–703. IEEE (2021)
14. Zhou, D., Fang, J., Song, X.: Iou loss for 2d/3d object detection. In: 2019 International Conference on 3D Vision (3DV), pp. 85–94. IEEE (2019)
15. Zheng, Z., Wang, P., Liu, W.: Distance-IoU loss: Faster and better learning for bounding box regression. In: Proceedings of the AAAI conference on artificial intelligence. Journal **34**(07): 12993–13000 (2020)
16. Fang, J., Li, X.: Object detection related to irregular behaviors of substation personnel based on improved YOLOv4. Appl Sci J **12**(9): 4301–4305 (2022)
17. Huang, X., Ge, Z., Jie, Z.: Nms by representative region: Towards crowded pedestrian detection by proposal pairing. In: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 10750–10759. IEEE (2020)
18. Bodla, N., Singh, B., Chellappa, R.: Soft-NMS--improving object detection with one line of code. In: Proceedings of the IEEE international conference on computer vision, pp. 5561–5569. IEEE (2017)

Network Intrusion Detection Based on Hybrid Network Model and Federated Learning

Yuqing Kou[1,2](✉), Jieren Cheng[1,2], Yue Yang[1,3], Hao Wu[3], Yajing Li[1,2], and Victor S. Sheng[4]

[1] Hainan Blockchain Engineering Research Center, Hainan, China
1178575946@qq.com, cjr22@162.com
[2] School of Computer Science and Technology, Hainan University, Haikou 570228, China
[3] School of Cyberspace Security, Hainan University, Haikou 570228, China
[4] Department of Computer Science, Texas Tech University, Lubbock 79409, TX, USA

Abstract. Data is a valuable strategic resource for the development of modern society. However, with the increasingly complex network environment, privacy leaks and malicious attacks emerge in endlessly. For example, blockchain has also begun to become a new outlet for network black production, which poses a huge security threat to cryptocurrency. In this paper, we propose a hybrid network model (Cb Net), which uses Convolutional Neural Networks (CNN) and Bidirectional recurrent neural networks (BiGRU) to fully extract the space-time characteristics of network data traffic. Then, we propose an intrusion detection method (FLD), which introduces federated learning to collect traffic data from different network institutions, analyze network traffic and identify network attacks. We have fully evaluated the performance of the proposed model and method on the public dataset NSL-KDD. Experiments show that the proposed hybrid network model can achieve high detection accuracy, and the FLD method can effectively identify network attacks on the premise of ensuring the privacy of the local data of the users involved, and its performance is better than other methods.

Keywords: Federated learning · CNN · RNN · Network intrusion detection · NSL-KDD

1 Introduction

The vigorous development of the Internet has brought us great convenience as well as a great threat to network security. Network intrusion detection system (NIDS) is an important means of protection in the field of network security.

At present, deep learning technology is developing in full swing. Unlike traditional machine learning algorithms, which rely on manual design of features, deep learning uses hierarchical structures to unsupervised learn data to automatically extract features. However, the extensive application of artificial intelligence also

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 152–166, 2024.
https://doi.org/10.1007/978-981-99-7161-9_12

brings us new difficulties. On the one hand, deep learning requires a lot of tag data as the basis of training, and obtaining such tag data is a time-consuming and laborious task. On the other hand, the problem of data privacy disclosure is becoming more and more serious. Data from different sources may have different user privacy, so it is difficult to share data from different sources, resulting in data islands. Especially in network intrusion detection, a single network domain can generate very limited attack behavior tags in a certain time, which means it is difficult to prevent large-scale network intrusion in time. Network traffic may leak sensitive information and user data in the network domain. Therefore, it is not possible to directly aggregate data sets from multiple network domains. How to expand the number of training data and conduct model training on large-scale network data to achieve good model training effect under the premise of ensuring data privacy and security is an important problem to be solved in the field of network intrusion detection.In such an environment where data privacy is crucial, federated learning emerged as a collaborative ML paradigm [1]. As a new distributed machine learning technology, federated learning can effectively solve the "data island problem". We expect the federated learning to play a distributed advantage in the field of network intrusion: multiple participants can effectively expand network attack data, and encrypt and exchange information and model parameters while maintaining data independence, Under the premise of ensuring user privacy, improve the detection performance of the intrusion detection system in the complex network situation.

Our contributions are summarized as follows:

1. CBNet hybrid network model is proposed, which uses CNN layer to extract local spatial hierarchical features and BiGRU layer to extract long-distance dependent features. And customized focal loss is to decrease the weight of data types that are easy to classify, so that the model can focus more on data types that are difficult to classify in the training process, thus reducing the impact of data imbalance.
2. We propose a network intrusion detection method FLD based on federated learning mechanism, which can phone traffic data from different network institutions. In the FLD, the training data of each institution is saved locally, and only parameters are transferred during the training process. In this way, data privacy and security are protected and network traffic anomalies are detected.
3. We use the NSL-KDD dataset [2] to evaluate the performance of the proposed CBNet model and FLD method, simulate the real scenario of "data island", and compare and analyze the detection performance of the centralized learning and federated methods.

2 Related Work

Deep learning organizes "learning algorithms" hierarchically in the form of "artificial neural networks" that can learn and make intelligent decisions on their own. Convolutional neural networks (CNN) and cyclic neural networks (RNN) The popularity of deep learning has made depth shine. In recent years, researchers have used CNN and RNN to identify cyber attacks.

Khan et al. [3] used CNN to extract two-dimensional features. Kan et al. [4] proposed the network intrusion detection method of APSO-CNN, which innovatively uses adaptive particle swarm optimization to optimize the convolutional neural network. Experiments show that this method can effectively detect network intrusion attacks. Al Turaiki et al. [5] combined dimensionality reduction with features and used CNN to extract features. Yu et al. [6] proposed a hierarchical CNN method based on packet bytes, which automatically extracts features from Pcap files. Andresini et al. [7] proposed an intrusion detection model combining GAN and CNN. In this model, the traffic is mapped to a two-dimensional image representation, and a new network attack image is generated through the network generation mode. However, CNN is not effective in dealing with long-term data dependence. RNN has the ability to extract time characteristics from input network traffic data. Alkahtani and others [8] developed the IoT intrusion detection framework. CNN, Long LSTM and CNN-LSTM are used to classify traffic. Khan [9] uses LSTM to detect time features, and AE detects global features more effectively, learning key feature representation efficiently and automatically from a large number of unmarked original network traffic data. Jothi [10] and others proposed the world integrated LSTM intelligent intrusion detection system, which has high accuracy in anomaly detection of the Internet of Things. Yang et al. [11] proposed a short-term memory network intrusion detection model based on attention mechanism, which preserves the long-term dependence between data through short-term memory network. Kurochkin et al. [12] proposed a GRU based method to detect abnormal traffic in the software definition network, and Singh et al. [13] proposed a TL based stacked GRU model with generalization and memory capabilities.

As mentioned above, researchers mainly focus on improving the deep learning algorithm to improve the accuracy of the deep learning model, but ignore the data privacy in the process of model training. In 2016, Google formally proposed federated learning [13]. Federated learning has shown a very vigorous application prospect and has been applied in many fields. Such as recommendation system field, medical image analysis,automatic driving field and so on.Based on this, we aim to study the applicability of federated learning in network intrusion detection.

3 Hybrid Network Model Based on CNN and BiGRU

The proposed hybrid network model has a multi-layer structure, including input layer, preprocessing layer, 1D convolution layer, BiGRU layer, attention layer, output layer, etc. The model structure is shown in Fig. 1.

3.1 Input Layer

Since the input of the model only accepts digital data, the NSL-KDD dataset contains non digital data, such as protocols, states, and services. Therefore, it needs to be pretreated [15]. One-hot coding: Since each network traffic data in the NSL-KDD dataset we use has character characteristics such as “protocol type”, “service” and “flag”, we need to perform numerical operations on them. Normalization: Normalization is the re-scaling of data to a specific range to reduce redundancy and shorten the training time of the model. We used the minimum-maximum normalization method to linearly transform the original data, mapping to the range of [0, 1]. The formula is:

$$X_{[i]} = \frac{X_{[i]} - X_{min}}{X_{max} - X_{min}} \tag{1}$$

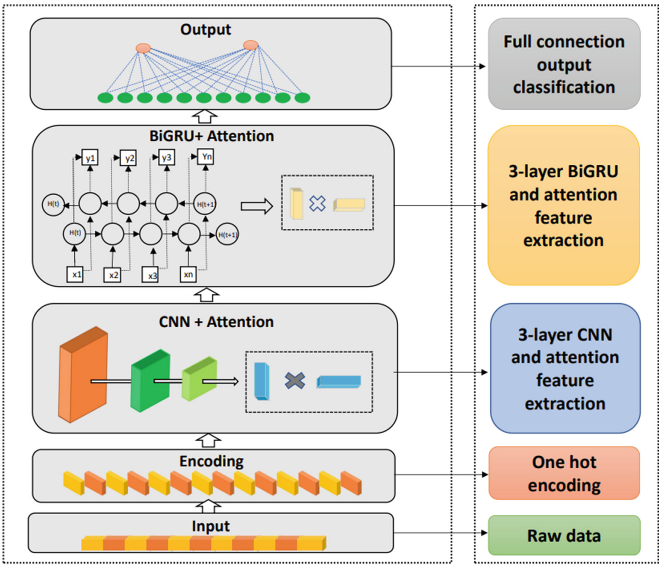

Output
BiGRU+ Attention
y1
y2
y3
Yn
H(t)
H(t+1)
x1
x2
x3
xn
CNN + Attention
Encoding
Input
Full connection output classification
3-layer BiGRU and attention feature extraction
3-layer CNN and attention feature extraction
One hot encoding
Raw data

Fig. 1. CBNet model diagram

3.2 CNN Layer

The one-dimensional data of network traffic time series input through the input layer first passes through the CNN layer, the main component of which is convolution. The feature mapping $f_m \in \mathcal{R}^{fd}$ is constructed by using the filter through the convolution operation, where f is a set of new features generated in the packet. f_m is the feature mapping obtained from the feature group.

$$hl_i^{fm} = \tanh(\omega^{fm} \chi_{i:i+f-1} + b) \tag{2}$$

Filter hl generation characteristic graph representation $hl = [hl_1, hl_2, \ldots, hl_{n-f=1}]$ where $hl \in \mathcal{R}^{n-f+1}$. In order to reduce training time and prevent over-fitting, we mapped the maximum pool operation for each feature $\overrightarrow{hl} = maxhl$. Finally, the new features generated are fed to the fully connected layer containing the softmax function to obtain the probability distribution of network traffic types. The mathematical formula of the fully connected layer is:

$$o_t = softmax = (\omega_{ho} hl + b_o) \tag{3}$$

3.3 BiGRU Layer

The model adopts BiGRU network, and we capture the time series in CNN by passing the newly constructed feature vector to GRUs.In order to capture the time-series pattern of the newly formed feature across time steps from the maximum pool operation in CNN, the newly constructed feature mapping vector is passed to the GRUs.

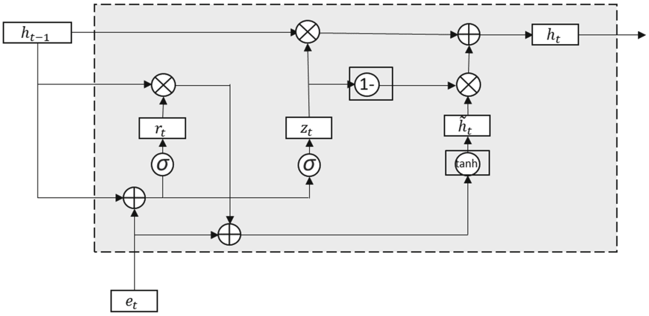


Fig. 2. GRU unit structure diagram

GRU network is a variant structure of RNN [16]. Compared with long-term short-term memory network LSTM, the structure is simpler and can reduce the time cost of model training. A single GRU unit is shown in Fig. 2. The state of each GRU unit is updated according to the calculation formula (4)–(7)

$$z_t = \sigma \left(W_z e_t + U_z h_t + b_z \right) \tag{4}$$

$$r_t = \sigma \left(W_r e_t + U_r h_{t-1} + b_r \right) \tag{5}$$

$$h'_t = tanh \left(W_h e_t + U_h \left(r_t * h_{t-1} \right) + b_h \right) \tag{6}$$

$$h_t = z_t * h_{t-1} + (1 - z_t) * \widetilde{h}_t \tag{7}$$

where h_t represents the output of GRU unit at the moment, and h'_t represents the candidate state. When r_t=0, $\widetilde{h}_t$ is independent of historical information h_{t-1} and only related to the current input e_t; when r_t=1, h_{t-1} is related to the current input and h_{t-1}. W, U, b and b are parameter matrices and vectors.

3.4 Attention Layer

Attention mechanism is introduced into 1DCNN network and BiLGRU network respectively. First, the hidden layer vector h_t obtained by convolution block or BiGRU is implicitly expressed as e_t through nonlinear transformation, and its expression is:

$$e_t = \ u \tan h\left(w_t h_t + b\right) \tag{8}$$

Then evaluate the importance of each flow at different time t. The normalized importance vector α_t is calculated by the softmax function, namely the attention weight. The fine-grained feature s_t can be obtained by the weighted sum of the coarse-grained feature α_t. According to the transformation of formula (9) and formula (10), the following is obtained:

$$\alpha_t = \frac{exp\left(e_t\right)}{\sum_{j=1}^{t} exp\left(e_j\right)} \tag{9}$$

$$s_t = \sum_{t=l}^{i} \alpha_t h_t \tag{10}$$

Finally, softmax classifier is used to predict the traffic type. The formula is:

$$y = \ softmax\left(W_h s + b_k\right) \tag{11}$$

where W_h and b represent classification weight and bias, and k is the number of types of network traffic.

3.5 Customized weight function focal loss

We use the sigmoid function as a binary classifier to distinguish normal traffic attack traffic.

$$sigmoid(h) = \frac{1}{1+e^{-h}} \tag{12}$$

For the loss function of dichotomy, binary cross entropy BCE is selected, and its expression is:

$$BCELoss = -y_i log y_i^{'} - \left(1-y_i\right) log\left(1-y_i^{'}\right) \tag{13}$$

where y_i indicates the real tag, and $y_i^{'}$ indicates the predicted tag value corresponding to the real tag. We use the softmax function as a multi-category classifier to distinguish attack traffic categories. For the unbalanced distribution of network intrusion samples, we used Focal loss [17] function to add modulation factor α and 1-α to reduce the loss weight of all samples in a easily classified category, and added modulation factor $(1-y_i^{'})^{\beta}$ and $y_i^{'}$ to reduce the loss weight of a single sample in a easily classified category.

$$binary\ Loss = -y_i\alpha(1-y_i^{'})^{\beta} log y_i^{'} - \left(1-y_i\right)(1-\alpha) log\left(1-y_i^{'}\right) \tag{14}$$

$$multi\ Loss = -\frac{1}{N}\sum_{1}^{N}\sum_{q\epsilon Q} y_{s,q} \underset{s}{\;} \alpha_q(1-y^{'}{}_{s,q})^{\beta} logy^{'}{}_{s,q} \tag{15}$$

where $y_{s,q}$ indicates the real tag, and $y^{'}{}_{s,q}$ indicates the predicted tag value corresponding to the real tag. The predefined weights of class q are denoted as α_q.

4 Intrusion Detection Method Based on Federated Learning

We assume that there are N distinct network institutions $\{M_1, M_2, \ldots, M_N\}$, respectively have their timing data $\{D_1, D_2 \ldots D_N\}$, and jointly train a machine learning model with its data. Traditional centralized way to collect data to the data center, and then to train the model and forecast, that is, the network data set into $D = \{D_1, D_2 \cup \ldots \cup D_N\}$ to train a model of a unified M_{sum}. Our proposed intrusion detection method FLD uses the federated learning paradigm to train and share the distributed cryptographic model to solve the data island problem in the real scenario of network intrusion. We use all the data of each network institution to train M_{fl}. In the process of model training, none of the network organizations will disclose their data to each other to ensure the security of the training process. We expect that the malicious traffic detection accuracy is close to or better than M_{sum} to prove the applicability of federated learning in network intrusion detection.The learning objectives of the central server is

$$arg\ min\ L = \sum_{i=1}^{n} l\left(y_i, f_s\left(x_i\right)\right) \quad (\omega, b) \tag{16}$$

where ω and b are the weights and bias to be learned by the central server, and (x_i, y_i) represents the global data, n is the size of the central server summary data set. The learning objectives of the network institution is

$$arg\ min\ L_j = \sum_{i=1}^{n^j} l\left(y_i^j, f_s\left(x_i^j\right)\right) \quad \left(\omega^j, y^j\right) \tag{17}$$

where ω^j represents the weight to be learned by the network mechanism; $\left(x_i^j, y_i^j\right)$ represents the time sequence data sequence of the jth network mechanism; n^j is he size of the network organization data set. After each round of training, the central server aggregates the weight of model parameters of each network organization. We used FedAvg algorithm to optimize the training process. Randomly select m network mechanisms for sampling, and average the gradient updates of these m network mechanisms to form a global update. Meanwhile, the current global model is used to replace the unsampled network mechanisms with the FedAvg algorithm [18]. network

$$f_s\left(\omega, b\right) = \frac{1}{M}\sum_{m=1}^{M} f\left(\omega^j, b^j\right) \tag{18}$$

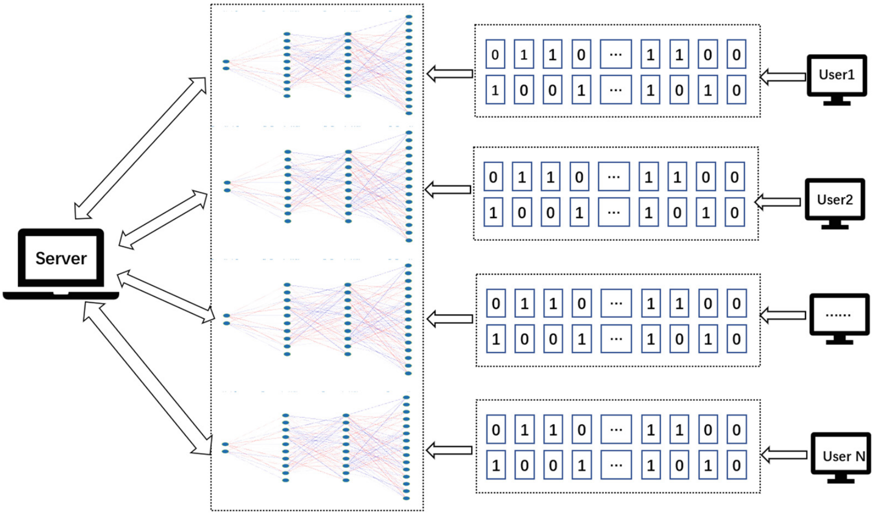


Fig. 3. Framework of the FLD method

The framework of the FLD method is shown in Fig. 3. It is divided into seven steps.

Step 1: The proposed hybrid network model CBNet is used as the cloud and each network institution model to identify traffic anomalies in network data, and CNN and BiGRU extract traffic sequence from the input network organization data. Step 2: Prospective network organizations download the model and do their homework. Step 3: The local data of the selected training node belong to the private state, and they are used locally to train the model. Step 4: Update the local model parameters and pass the model parameters to the central server. Step 5: After receiving updates from all network institutions, the central server aggregates model weights and creates a new update model. In this step we use the federated average algorithm to aggregate, weighting the parameters according to the local data set size. Step 6: The server returns parameters. At this time, the updated model parameters are sent back to the network institutions involved in the first round of training. Step 7: Each network organization continues to improve the model by replacing local parameters with updated global parameters.

5 Experiment and Evaluation

This section is divided into two parts: the implementation and evaluation process of the hybrid network model CBNet and the Federated Learning-based Intrusion detection Method (FLD). We used Keras with Tensorflow as the back end to build the model.In the future, we will take the blockchain environment as a further experimental verification environment.

5.1 Dataset

Public dataset NSL-KDD [19] is adopted as the experimental dataset,there are four attack types in the NSL-KDD: Dos, Probe, R2L, and U2R. Dataset information is shown in Table 1.

Table 1. Training set and test set information

	Training		Test	
Data category	Quantity	Proportion(%)	Quantity	Proportion(%)
Normal	67343	53.46	9711	43.08
Dos	45927	36.46	7458	33.08
Probe	11656	9.25	2421	10.74
R2L	995	0.79	2754	12.22
U2R	52	0.04	200	0.89

5.2 Evaluation Method

At present, the evaluation indexes in the field of network intrusion detection mainly include accuracy, precision, recall rate and F1-score. These indices can be calculated according to the four basic criteria of the confusion matrix: true positive (TP), false positive (FP), true negative (TN), and false negative (FN). Several indicators are calculated as follows:

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \tag{19}$$

$$P = \frac{TP}{TP + FP} \tag{20}$$

$$R = \frac{TP}{TP + FN} \tag{21}$$

$$F_1 - score = \frac{2 \times P \times R}{P + R} \tag{22}$$

5.3 Experimental Results and Discussion

Hybrid Network Model (CBNet) Performance Evaluation Figure 4 shows the confusion matrix of CB-Net, a hybrid network model with two categories. We calculated the accuracy, precision, recall rate and F1-score of the hybrid network model detection by the confusion matrix, and the values of the four evaluation criteria were all up to 98.5%. Experimental results show that this model has excellent performance for binary classification. Similary, the five

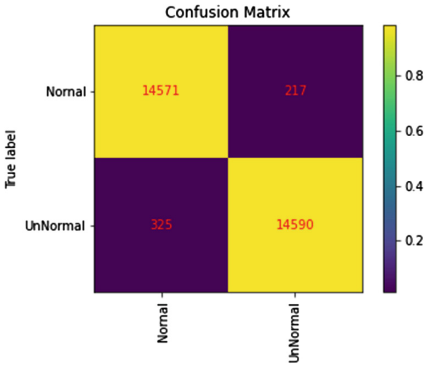


Fig. 4. Binary confusion matrix of CBNet

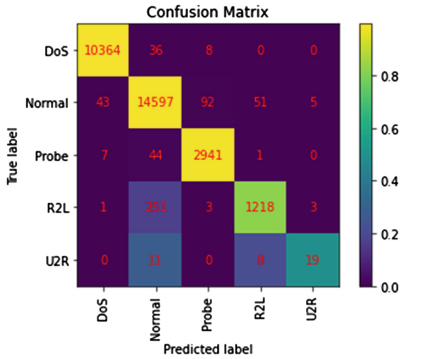


Fig. 5. Five classification confusion matrix of CBNet

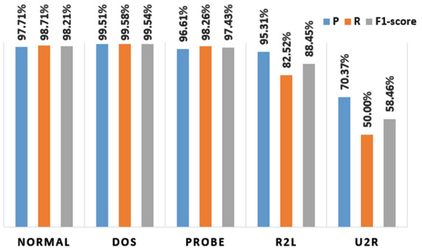


Fig. 6. Value of various data indicators

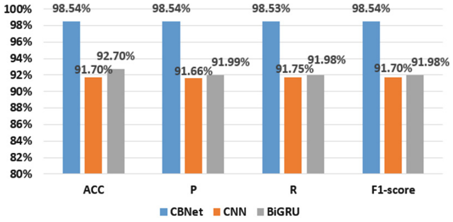


Fig. 7. Results of ablation experiment

categories confusion matrix of Fig. 5 shows the same excellent performance. The accuracy rate was 98.1%. Precision, recall rate and F1-score were 91.9, 85.81 and 88.42%, respectively.

In Fig. 6 , we show the accuracy, recall rate and F1-score of each category to analyze the detection effect of each data category. Despite the unbalance of class distribution in the data set, the proposed CBNet model still achieves attractive results, which proves the validity and robustness of the proposed model.

And we performed ablation experiments with CBNet model and neural network algorithm model (CNN, GRU). The comparison results are shown in In Fig. 7. Experiments show that the hybrid network model we adopted is superior to the single network model in terms of various indicators.

Performance Evaluation of Intrusion Detection Method FLD To simulate the situation of "data island", we randomly divide the data set into multiple parts to represent the local data owned by each user. This data processing method can ensure that each local user lives in a completely independent network environment, that is, the distribution of intrusion attack types is completely random and independent, and different users are subject to different

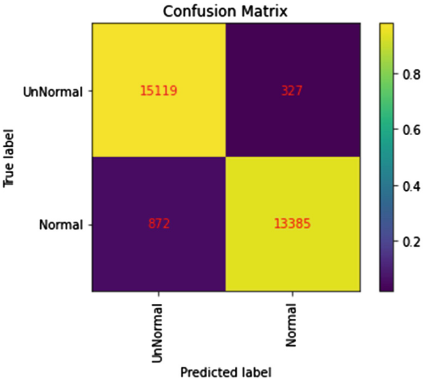


Fig. 8. Binary confusion matrix of FLD method

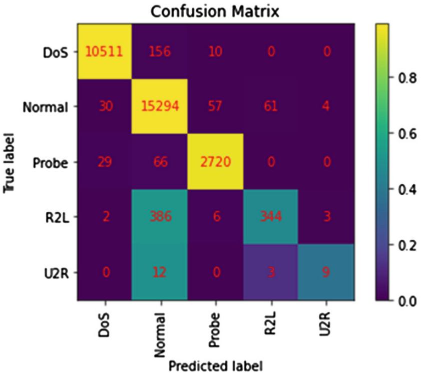


Fig. 9. Five class confusion matrix of FLD method

types of intrusion attacks and attacks, even some users may not have all types of intrusion attacks. If the dataset contains M pieces of data in total, and it is necessary to generate local data for N local users, then M/N pieces are directly and randomly extracted from the total dataset to form a user's local dataset.

Figures 8 and 9 show the confusion matrix obtained by the FLD method in the second and fifth classification experiments. After 20 epochs, most of the detection results basically hit the correct classification. In the second classification experiment, the accuracy rate, accuracy rate and F1 score value all reached more than 97%, which is only about 1% different from the centralized CBNet model. We believe that with the increase of epoch, the difference between the two will be smaller and smaller.

We compare the proposed CBNet model and FLD method with the classical work and recent work based on NSL-KDD dataset. The comparison information is shown in Tables 2 and 3. The detection accuracy of our CBNet model and FLD method is much higher than C4 5. Decision tree, random forest and other classical machine learning methods. Li et al. [20] used the improved Bat algorithm and random forest to detect malicious traffic. The generalization ability is not high, and the model performance trained by this method is not good enough compared with our model and method. Although Diro et al. [21] also used the deep learning method, the detection accuracy was less than 94% because they did not process high-dimensional data. Yang et al. [22] and Tian et al. [23] used deep confidence networks and did not explicitly deal with time related learning of observed variables, so the accuracy of traffic classification is not as high as our models and methods. shan Kumar et al. [24] used genetic algorithm to improve the neural network to detect traffic, but it only optimized the weight of the neural network. Our hybrid network model CBNet is an extension of NN, which can extract more effective feature information. From the experimental data, the accuracy and F1 value of CBNet model and FLD method are higher than this method.

Table 2. Comparison of secondary classification results

	Comparison of secondary classification results			
	ACC	P	R	F(%)
C4.5 decision tree	74.6	/	/	/
Random forest	74	/	/	/
Random tree	72.8	/	/	/
SVM	74	/	/	/
Tian et al. [23]	97.2	94.6	98.5	96.5
shan Kumar et al. [24]	95.5	97.5	89.4	93.3
CBNet	98.5	98.5	98.5	98.5
FLD (N = 10)	97.5	97.1	97.2	97.1

Table 3. Comparison of five classification results

	Comparison of five classification results			
	ACC	P	R	F(%)
Li et al. [20]	93.96	/	/	/
Diro et al. [21]	92.77	/	/	/
Yang et al. [22]	84.98	/	/	/
Tian et al. [23]	96.06	87	71.8	76.2
shan Kumar et al. [24]	95.6	90.5	65.2	69.4
CBNet	98.1	91.9	85.81	88.42
FLD (N = 10)	97.22	86.8	75.6	78

We use the FLD intrusion detection method to compare it with the hybrid network model (CBNet) that each user only uses its local dataset for training. We set the number of local users to N = 10, 50, 100, that is, 1/10 dataset, 1/50 dataset and 1/100 dataset are used respectively. Only the local dataset is used to train a group of users of the mixed model. Since each user generates its own model, the performance of each client is averaged to compare the results. Figure 10 shows the comparison of accuracy indicators of FLD method and CBNet model under different data set sizes. It can be clearly seen that under the same data scale, the FLD method has a higher accuracy rate for identifying abnormal traffic, and the difference is more and more obvious as the data scale decreases.

We use the F1 score value, the harmonic value of accuracy and recall, to draw a comparison chart between FLD method and CBNet model under different data scales, as shown in Fig. 11. Similar to the rule of accuracy, under the same data size, the F1 score value of FLD method is higher, and the difference will become more obvious as the data set size decreases. This shows that the FLD method with federal learning mechanism has better performance.

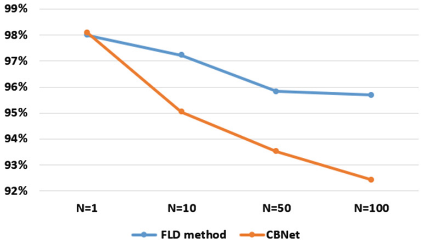


Fig. 10. Comparison of accuracy under different data set sizes

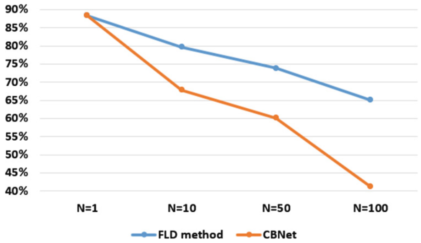


Fig. 11. Comparison of F1-score under different dataset sizes

As mentioned earlier, our FLD method has better detection performance than CBNet only when the data sets are of the same size. In order to find out the specific reason for the large difference in detection accuracy between the two, we further compared the specific F1 score values of each data type between the two. When N = 10, F1 score values of various data types are shown in Fig. 12. The results of Probe and Probe are basically the same, while the F1-score values of the other four data types of CBNet model centralized learning are lower than those of FLD method, and the comparison is obvious in small sample U2R and R2L.

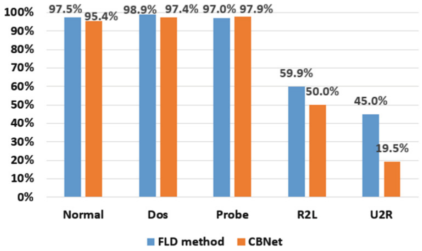


Fig. 12. F1-score value of various data when N = 10

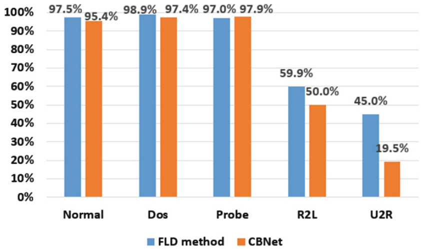


Fig. 13. F1-score value of various data when N = 50

As the size of the dataset decreases, when N = 50, the F1 score values of various data types are shown in Fig. 13. Our comparison results show that the F1 score of each data type using FLD method is significantly lower than CBNet centralized learning, and the F1 score of small samples U2L and U2R are more than twice as high.The reason is that in the case of random data grouping, as the data size decreases, the number of small samples R2L and U2R owned by some users is extremely low or even zero, which makes it extremely difficult for such users to detect such attacks. And with the reduction of the data size, the detection difficulty of small samples becomes more and more difficult.

6 Conclusion

In this paper, a hybrid network model CBNet is proposed, and the experimental results verify its excellent intrusion detection performance. In particular, we further propose a network intrusion detection method FLD based on federated learning, and the experiment proves that our FLD method can break the "data island" problem faced by current network institutions, and is feasible in the real network intrusion scenario. In the future, we will use real network traffic data such as the internal server traffic of the State Grid to further experiment.And we will conduct cross chain anomaly detection in the blockchain environment.

Acknowledgment. This work was supported by Hainan Provincial Natural Science Foundation of China(Grant No. 620MS021, 621QN211), the Key Research and Development Program of Hainan Province (Grant No. ZDYF2021GXJS003, ZDYF2020040), the Major science and technology project of Hainan Province (Grant No. ZDKJ2020012), National Natural Science Foundation of China (NSFC) (Grant No. 62162022, 62162024), Science and Technology Development Center of the Ministry of Education Industry-university-Research Innovation Fund (2021JQR017), Innovative research project for Graduate students in Hainan Province (Grant No.Qhyb2022-93).

References

1. Qiang, Y.: Federal learning: the last mile of ai. CAAI Trans. Intell. Syst. **15**(1), 183–186 (2020)
2. Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A.A: A detailed analysis of the kdd cup 99 data set. In: IEEE International Conference on Computational Intelligence for Security Defense Applications (2009)
3. Khan, M.A., Karim, M.R., Kim, Y.: A scalable and hybrid intrusion detection system based on the convolutional-lstm network. Symmetry **11**(4) (2019)
4. Kan, X., Fan, Y., Fang, Z., Cao, L., Li, X.: A novel iot network intrusion detection approach based on adaptive particle swarm optimization convolutional neural network. Inf. Sci. (2021)
5. Al-Turaiki, I., Altwaijry, N.: A convolutional neural network for improved anomaly-based network intrusion detection. Big Data **9**(3), 233–252 (2021)
6. Yu, L., Dong, J., Chen, L., Li, M., Xu, B., Li, Z., Qiao, L., Liu, L., Zhao, B., Zhang, C.: PBCNN: packet bytes-based convolutional neural network for network intrusion detection. Comput. Netw. **194**, 108117 (2021). [Online]. Available: https://doi.org/10.1016/j.comnet.2021.108117
7. Andresini, G., Appice, A., Rose, L.D., Malerba, D.: GAN augmentation to deal with imbalance in imaging-based intrusion detection. Future Gener. Comput. Syst. **123**, 108–127 (2021). [Online]. Available: https://doi.org/10.1016/j.future.2021.04.017
8. Alkahtani, H., Aldhyani, T.H.H.: Intrusion detection system to advance internet of things infrastructure-based deep learning algorithms. Complex 5 579 851:1–5 579 851:18 (2021). [Online]. Available: https://doi.org/10.1155/2021/5579851
9. Khan, M.A., Kim, Y.: Deep learning-based hybrid intelligent intrusion detection system. Comput. Mater. Continua **7**, 17 (2021)

10. Jothi, B., Pushpalatha, M.: Wils-trs—a novel optimized deep learning based intrusion detection framework for iot networks. In: Personal and Ubiquitous Computing, pp. 1–17
11. Yang, S., Tan, M., Xia, S., Liu, F.: A method of intrusion detection based on attention-lstm neural network. In: ICMLT 2020: 2020 5th International Conference on Machine Learning Technologies (2020)
12. Kurochkin, I.I., Volkov, S.S.: Using gru based deep neural network for intrusion detection in software-defined networks. IOP Conf. Ser. Mater. Sci. Eng. **927**(1), 012035 (2020)
13. Singh, N.B., Singh, M.M., Sarkar, A., Mandal, J.K.: A novel wide deep transfer learning stacked gru framework for network intrusion detection. J. Inf. Secur. Appl. 61 (2021)
14. Cheng, K., Fan, T., Jin, Y., Liu, Y., Yang, Q.: Secureboost: a lossless federated learning framework. Intell. Syst. IEEE (99), 1 (2021)
15. Paulauskas, N., Auskalnis, J.: Analysis of data pre-processing influence on intrusion detection using nsl-kdd dataset. In: Electrical, Electronic Information Sciences, pp. 1–5 (2017)
16. Salem, F.M.: Gated RNN: The Gated Recurrent Unit (GRU) RNN. Springer International Publishing, pp. 85–100 (2022). https://doi.org/10.1007/978-3-030-89929-5_5
17. Lin, T.Y., Goyal, P., Girshick, R., He, K., Dollar, P.: Focal loss for dense object detection. IEEE (2), (2020)
18. Karimireddy, S.P., Kale, S., Mohri, M., Reddi, S.J., Stich, S.U., Suresh, A.T.: Scaffold: stochastic controlled averaging for federated learning (2019)
19. Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A.A: A detailed analysis of the kdd cup 99 data set. In: IEEE International Conference on Computational Intelligence for Security Defense Applications (2009)
20. Li, J., Zhao, Z., Li, R., Zhang, H.: Ai-based two-stage intrusion detection for software defined iot networks. IEEE Internet Things J. 6(2), 2093–2102 (2019). [Online]. Available: https://doi.org/10.1109/JIOT.2018.2883344
21. Diro, A.A., Chilamkurti, N.K.: Distributed attack detection scheme using deep learning approach for internet of things. Future Gener. Comput. Syst. **82**, 761–768 (2018). [Online]. Available: https://doi.org/10.1016/j.future.2017.08.043
22. Yang, Y., Zheng, K., Wu, C., Niu, X., Yang, Y.: Building an effective intrusion detection system using the modified density peak clustering algorithm and deep belief networks. Appl. Sci. 9(2) (2019)
23. Tian, Q., Han, D., Li, K., Liu, X., Duan, L., Castiglione, A.: An intrusion detection approach based on improved deep belief network. Appl. Intell. **50**(10), 3162–3178 (2020). [Online]. Available: https://doi.org/10.1007/s10489-020-01694-4
24. Kumar, G.: An improved ensemble approach for effective intrusion detection. J. Supercomput. **76**(1), 275–291 (2020). [Online]. Available: https://doi.org/10.1007/s11227-019-03035-w

A Blockchain-Based Encrypted Data Retrieval Scheme for Smart Grid

Hong Zhao[1], Hongzhong Ma[1], Yong Yang[1], Di Wang[1], Siyi Chen[2], and Qiao Zhang[3](✉)

[1] State Grid Gansu Electric Power Research Institute, Lanzhou 730070, China
[2] Department of Electrical Engineering and Information Technologies, University of Naples Federico II, 80125 Naples, Italy
[3] Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
zq65536@163.com

Abstract. With the popularization of smart grid, the power industry has gradually attracted people's attention. Among them, grid data is an important data that contains personal privacy. Once these data are stolen by attackers, it may be inferred from the private information of grid users, such as work schedule, income. In order to protect the private data in smart grid, this paper proposes a blockchain-based data retrieval scheme for smart grid. Firstly, private data is symmetrically encrypted and then uploaded to a cloud service. For the purpose of retrieve encrypted data on cloud services, we use searchable encryption combined with inverted index technology. Data users holding retrieval tokens can directly retrieve ciphertext data from cloud services. Secondly, to ensure the transparency and traceability of data access, we propose to take the alliance chain composed of several sub-institutions under the same power system organization as the network basis. And all the privacy data access records will be recorded on the chain for the convenience of later access traceability. Finally, we simulated our scheme in a realistic environment. The safety analysis and simulation experiment prove that our scheme is safe and feasible.

Keywords: Smart grid data · Searchable encryption · Blockchain · Inverted index

1 Introduction

With the improvement of people's living standard, the demand for electricity is rising rapidly and the grid is becoming an indispensable part of people's daily life [1]. The constant development of science and technology in recent years also makes the grid evolve from traditional Grids into Smart Grids (SG), which are represented by intelligent and information conversion. The overall architecture of smart grid can be roughly divided into the following layers as shown in Fig. 1: physical layer, sensor/actuator layer, network layer, application layer [2]. Taking smart meters (SMs) as an example, as a typical device

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 167–178, 2024.
https://doi.org/10.1007/978-981-99-7161-9_13

in smart grid, it brings convenience to users' lives by monitoring their electricity consumption in real time and allowing them to view their power consumption. However, the interconnectivity of these devices and the security of the upper layer applications raises concerns about the security of electricity data. Because the leakage of users' electricity consumption data through monitoring SMs or upper layer application vulnerabilities can reveal personal information such as user behavior and wealth [3]. This paper focuses on the security above the data sensors layer, i.e., the application slayer.

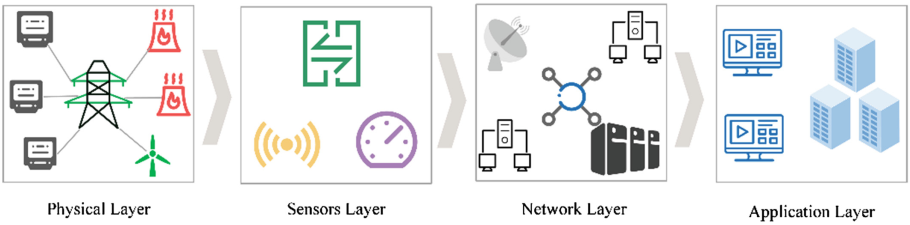


Fig. 1. Grid framework

In reality, the grid company involves many production business departments and joints, and there are a large number of independent systems within the grid companies. On the one hand, there are data inconsistencies between these systems, forming a data silo effect. On the other hand, the security performance of a single server cannot meet the higher level of security requirements. If these servers are attacked, there is a great possibility of privacy data leakage. To address these problems, Wang et al. [4] proposed an identity-based data aggregation protocol for the smart grid. In their scheme, they use identity-based encryption and signature schemes to protect the confidentiality and integrity of grid data. Kumar et al. [5] propose an elliptic curve-based signature scheme to protect the integrity of data in smart grid. In parallel with grid data content protection, the scale of grid data is also rising rapidly. For example, in a provincial grid in China, almost 1 Tb of data is generated one day [6]. Such a large amount of data is certainly difficult to solve with traditional computers. Cloud computing services are considered to be low-cost, efficient, and always online, hence more and more researchers are outsourcing private data in the smart grid to cloud services for processing. Searchable encryption started from the scheme proposed by Song et al. in 2005 in reference [7]. The data owner first selects suitable keywords for his/her data to generate an encrypted index, and the data user can use the retrieval trapdoor containing the keywords to search. If the trapdoor and the encrypted index can match, the corresponding encrypted data is returned. Eltayieb and others [8] outsource encrypted grid data to cloud services for storage. To solve the problem that a large number of encrypted data cannot be quickly retrieved, they introduce searchable encryption technology. Data users with retrieval traps can quickly search for the data they want from cloud services, and this process will not disclose any user's privacy. Wen et al. [9] proposed a searchable encryption scheme with dual tokens to solve the problem that data in smart grid should be kept secret while security audit is required. And this solution supports range query in the ciphertext. Wang et al. [10] believe that the existing searchable encryption scheme with a single keyword is not suitable for a large amount of power grid data. They propose a multi-keyword searchable encryption scheme under smart grid, which is proved to be secure under DBDH assumption. Although the existing scheme can solve the problem of ciphertext retrieval when the power grid data is outsourced to the cloud service, the retrieval process still needs to facilitate all the encrypted indexes. Even with the support of the cloud service with powerful computing power, the retrieval efficiency is still hardly satisfactory.

Although the above scheme realizes the outsourcing of smart grid data to cloud services and realizes the ciphertext retrieval on cloud services. However, their scheme does not take into account the non-repudiation of encrypted data access operations. As an emerging technology, blockchain has attracted wide attention because of its distributed, immutable, open, transparent, and other characteristics [11]. Smart contract is a piece of code deployed on the blockchain [12], and its execution does not require the participation of a third party. Therefore, the execution result of smart contract is considered to be trusted, and since every node in the blockchain contains the hash value of the previous node, the result of contract execution is also considered to be immutable. As early as 2018, Dong et al. [13] proposed that the increasingly complex grid environment needed a secure and powerful network facility. Blockchain, as distributed data, could provide a network basis for grid data management and smart meters data aggregation. Applying blockchain to smart grid data protection protects the integrity of the data while making any manipulation of the data non-repudiation. Subsequently, reference [14] uses the alliance chain Fabric to enable data transactions on the smart grid. In the same year, Wang et al. [15] proposed an anonymous authentication and key negotiation protocol in the edge computing scenario in the power grid environment, which can ensure the identity security of smart meters in the smart grid environment when they access the edge gateway. Smart contracts in their scheme are responsible for managing the key materials table. Since then, Khattak et al. [16] have used blockchain and smart contract technology to exchange data on the smart grid. They believe that the electricity price should be calculated in real-time according to the real-time demand of consumers (electricity demanders, generally power users). The blockchain represented by the alliance chain Fabric can protect the non-repudiation in the process of data exchange, and the existence of smart contracts can make the execution of transactions without the involvement of third parties.

Based on the above literatures, we note that blockchain can effectively record the operation records of data in smart grid data management, ensuring the integrity and non-repudiation of data. At the same time, the existing searchable encryption schemes need to retrieve all encrypted indexes from cloud services in full text, which is not the optimal scheme in the huge scale of power grid data. To solve the above problems, this paper proposes a blockchain-based encrypted data retrieval scheme for smart grid. Our main contributions are as follows:

1. Our scheme uses multi-keyword searchable encryption technology to retrieve ciphertext from the cloud server. Meanwhile, in order to improve the retrieval efficiency, we combine inverted index into searchable encryption to support fast ciphertext retrieval on the cloud service.
2. To ensure the untamperability of power grid data and non-repudiation of power grid data access, we use alliance chain technology to build alliance chain within multiple

grid institutions. Only nodes in the alliance chain can access private data, and all access will be recorded on the blockchain.

3. Security analysis proves that our scheme is safe under the DBDH assumption. In addition, we carry out simulation experiments based on the actual environment, and the results show that our scheme is feasible.

The rest of the article is arranged as follows: The second section is about advanced knowledge. The third section gives a brief description of our scheme. The main details are in Section 4, and Section 5 is security analysis and performance analysis. We summarize our scheme in Section 6.

2 Preliminaries

2.1 Bilinear Pairing

For two cyclic groups G_a and G_b with prime order p. Suppose that $e : G_a \times G_a \rightarrow G_b$ is a general map, we call e as a bilinear map if e satisfies the following three properties.

(1) Bilinearity: $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ for all $g_1, g_2 \in G_a$ and $a, b \in Z_p$.
(2) Non-degeneracy: There exits $g_1, g_2 \in G_a$ such that $e(g_1, g_2) \neq 1$, where 1 is the unit of G_b.
(3) Computability: For all $g_1, g_2 \in G_a$, $e(g_1, g_2)$ can be calculated quickly in a polynomial time.

2.2 Inverted Index

Search index, a common search tool, is a mapping relationship that allows us to quickly find the location of the content we need. The data structure at the core of large-scale search engines is the inverted index, which is essentially a collection of sorted integer sequences called inverted lists [17]. The inverted index consists of a dictionary (Location) and inverted files (Inverted Files). Here we take the example of the encrypted set of files in the grid and the corresponding set of keywords. First, we create a traditional index structure as shown in Fig. 2, where each encrypted file corresponds to several keywords. If we need to find the encrypted file corresponding to a certain keyword, we need to iterate through all the encrypted files. When the number of encrypted files is much larger than the size of the keywords space, it is no longer appropriate to apply the traditional indexing architecture.

On the contrary, if we build the index according to the inverted indexing method, we have the structure as in Table 1, and the mapping relationship becomes keywords to encrypted files. In this structure, not only the fast search of a single keyword, but also the joint search of multiple keywords is supported. For example, to find encrypted files containing both keywords kw_1 and kw_2.

2.3 Decision Bilinear Diffie-Hellman (DBDH) Assumption

Let G and G_T be two cyclic groups with prime order p, and e is a bilinear map. Randomly select $x, y, z \in Z_p$ and $T \in G_T$, denote $X = g^x, Y = g^y, Z = g^z$. It is difficult to determine whether T is equal to $e(g, g)^{xyz}$ in any probabilistic polynomial-time.

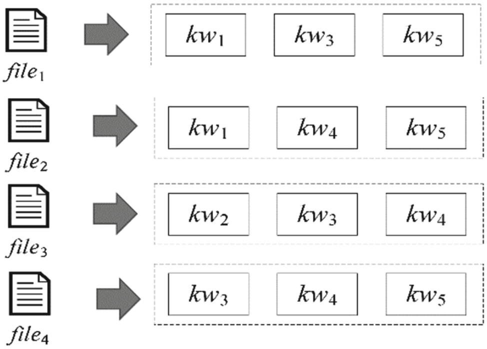


Fig. 2. Keywords corresponding to the encrypted file

Table 1. Invert the index file list

Keywords	Encrypted files
kw_1	$file_1, file_2$
kw_2	$file_2$
kw_3	$file_1, file_3, file_4$
kw_4	$file_2, file_3, file_4$
kw_5	$file_1, file_2, file_5$

3 System Overview

3.1 System Model

In this subsection, we first introduce our blockchain-based encrypted data retrieval scheme for smart grid. Our scheme contains four participants: alliance chain (blockchain), smart grid data centers(data center), cloud services(cloud), and data users. Their specific responsibilities and functions are shown below.

Blockchain: The alliance chain is played by all grid company nodes within the same organization, for example, all grid companies within the same province. It acts as the trusted database of the current system and is the central node of the system. It is responsible for recording all of the user's retrieval operations and communicating with the cloud service via the blockchain prognosticator.

Data Centers: Data center refers to the internal servers of the grid. After symmetrically encrypting private data and generating message summaries, the SMs uploads it to the upstream data center. Note that data centers are not responsible for storing data, they are also responsible for collecting a certain amount of data and then interacting with the blockchain for data upload. This is because there are a huge number of data collectors and if they interact directly with the blockchain, it will put a burden on the blockchain network.

Cloud Server: Cloud services can be provided by third parties or built in-house by grid companies. In our system, the cloud service is considered to be always online and has unlimited computing and storage capacity. In particular, it is important to note that in our scheme, the cloud service is not a trusted entity. It is partially trusted in terms of security.

Data users: The data users of the system can be staff members within the grid or regulators, etc. They can submit retrieval tasks to the blockchain under the condition that they hold retrieval tokens to quickly retrieve encrypted data from cloud services (Fig. 3).

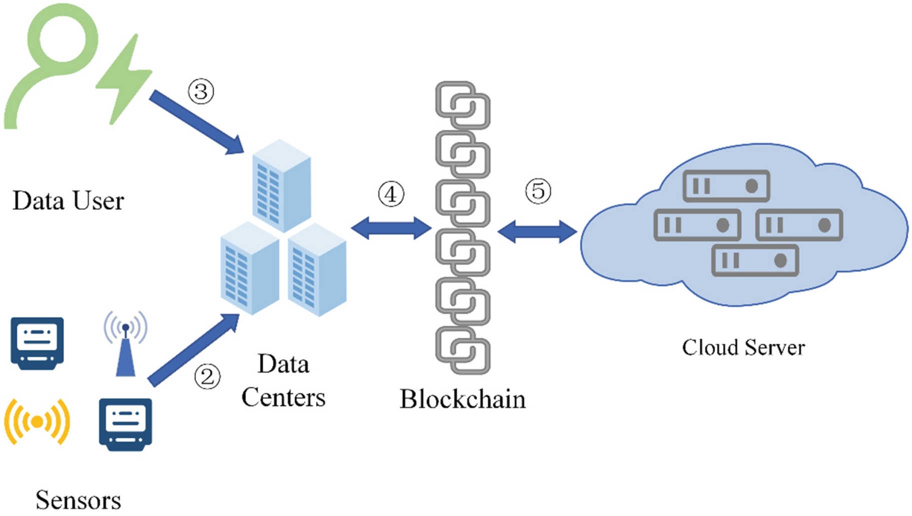


Fig. 3. System architecture

3.2 The Procedure of the System

The main processes in our system are as follows:

Step 1: System initialization. This process is mainly performed by a trusted third-party authorization authority (AA). In this phase, the AA initializes the keyword space, generates the system master key, and is responsible for generating public-private key pairs for the users. All public keys will be placed in the system open space for all users to query, while the private keys will be kept by the users themselves. It is noted that all key exchanges will be performed on a trusted channel.

Step 2: File collection. The private data collected from the data collector (SMs) is not uploaded directly to the cloud service; it needs to be uploaded to the corresponding upstream data center first.

Step 3: Build Index. This process will be executed by the data center server. The data center executes searchable encryption to generate the corresponding encrypted index and submits the encrypted index to the blockchain, and the smart contract executes the file upload operation.

Step 4: File upload. After the smart contract receives the encrypted file and index, it needs to communicate with the blockchain prophecy machine and cloud service because the contract does not interact with the outside world directly. At the same time, this upload operation will be uploaded to the blockchain as a deposit certificate.

Step 5: File search. If data users need to use the data, they need to apply for a retrieval trapdoor from the corresponding data center, then they submit the retrieval trapdoor to the blockchain. And with the help of the blockchain prognosticator, the search request is sent to the cloud service for execution. All the operation records are also recorded on the blockchain.

4 Construction of Proposed Scheme

Our blockchain-based multi-keyword fast retrieval scheme for grid data is composed of the following algorithms.

SysInit(1^{λ}): The trusted third-party authorization authority runs this algorithm, and λ is a secure parameter. Denote G_1 and G_2 are two groups with a large prime order p, and g is the generator of G_1. Suppose $e : e(G_1, G_1) = G_2$ is a bilinear map, and $H : \{0, 1\}^* \to G_1$ is a secure hash function. AA generates a random number $x \in Z_p^*$ and keeps x as the master key of system. It publishes $parms = \langle G_1, G_2, p, g, g \cdot x, e, H \rangle$ as the global system parameters.

KeyGen$(params)$: After system initialization, AA performs the following steps to generate the public-private key pairs $\langle SK_d, PK_d \rangle$ for each data center node in grid. It chooses a random number $s_d \in Z_p^*$ and then calculates $Y_d = s_d \cdot g$ to get $SK_d = s_d$ and $PK_d = Y_d$. Then AA uses the same way to get the key pairs $\langle SK_c, PK_c \rangle$ of CS, where $SK_c = s_c$, $PK_c = s_c \cdot g$. Finally, AA exposes the public key PK as the public system parameter, and then the private key SK is sent to the corresponding user through a secret channel.

BuildIndex$(params, Fd, W, PK_c, PK_d)$: After the data center receives a sufficient number of encrypted file sets Fd and the corresponding keyword sets W from data collectors such as smart meters. For each file $file_i \in Fd$ corresponding to the list of keywords $kw_{ij} \in W$, it computes $I_1 = e\big(SK_d \cdot H\big(kw_{ij}\big), g \cdot x\big) \cdot e\big(g \cdot r_j, SK_d \cdot PK_c\big)$. Then, the data center generates j random numbers $r_j \in Z_p^*$ and computes $I_2 = \big\{g \cdot r_j\big\}$. After generating indexes for all encrypted files, the data center creates the inverted index file (IIF) for the batch of files as shown in Table 2.

Next, the data center executes Algorithm 1 and performs the obfuscation operation of the encrypted file to get the final IIF. Finally, the data center submits the encrypted file to the blockchain for recording and uploads it to the cloud service.

Algorithm 1: ***Inverted Index File Confusion***

```
Input: all inverted index files: iifs
Output: obfuscated inverted index files
```

(*continued*)

(*continued*)

Algorithm 1: ***Inverted Index File Confusion***

```
let max_size = **max**(iifs)
**for** iif in iifs
    let gen_size = max_size – size(iif)
    generate gen_size random files random_files
    iif.add(random_files)
**end for**
**return** iifs
```

TrapdoorGen$(params, kw, MK, SK_d)$: If other data centers in the system or employees within the grid want to perform a search, then they first need to request a retrieval trapdoor Td from the data owner. It first submits the set of keywords kw wants to search, and then DU generates r_k for $kw_k \in kw$. Next DU calculates $T_1 = e(PK_d, x \cdot H(kw_k)) \cdot e(g \cdot r_k, x \cdot PK_c)$ and $T_2 = g \cdot r_k$. Finally, the trapdoor $Td = \{T_1, T_2\}$ is returned to the data user.

Search$(IIF, Td, params, SK_c)$: When the cloud service receives a search request submitted by the blockchain prophecy machine and the corresponding retrieval token Td, it executes Eq. 1 for all IIFs. If the retrieval criteria are met, it returns the corresponding encrypted file list. Meanwhile, the search results will be recorded on the blockchain.

$$\frac{I_{1,i}}{e\left(I_{2,i}, PK_d\right) \cdot SK_c} = \frac{T_{1,j}}{e\left(T_{2,j}, g \cdot x\right) \cdot SK_c} \tag{1}$$

5 Analysis of Our Scheme

5.1 Correctness Analysis

The cloud service performs the retrieval step of Eq. 1 and the left-hand side is calculated as follows:

$$\begin{aligned} & \frac{I_{1,i}}{e\left(I_{2,i}, PK_d\right) \cdot SK_c} \\ & = \frac{e\left(SK_d \cdot H\left(kw_{ij}\right), g \cdot x\right) \cdot e\left(g \cdot r_j, SK_d \cdot PK_c\right)}{e\left(I_{2,i}, PK_d\right) \cdot SK_c} \\ & = \frac{e\left(s_d \cdot H\left(kw_{ij}\right), g \cdot x\right) \cdot e\left(g \cdot r_j, s_d \cdot g \cdot s_c\right)}{e\left(g \cdot r_j, s_d \cdot g\right) \cdot s_c} \\ & = e\left(s_d \cdot H\left(kw_{ij}\right), g \cdot x\right) \end{aligned} \tag{2}$$

Table 2. Inverted index file

kw	I_1	I_2	Encrypted files
kw_1	$I_{1,1\ldots}$	$I_{2,1\ldots}$	$file_1, file_3, file_4, file_5$
kw_2	$I_{1,2\ldots}$	$I_{2,2\ldots}$	$file_2, file_4, file_6$
kw_3	$I_{1,3\ldots}$	$I_{2,3\ldots}$	$file_1, file_2, file_3$
kw_4	$I_{1,4\ldots}$	$I_{2,4\ldots}$	$file_5, file_6$
kw_5	$I_{1,5\ldots}$	$I_{2,5\ldots}$	$file_3$

Meanwhile, the right-hand side of the equation for Eq. 1 is calculated as follows:

$$\begin{aligned} &\frac{T_{1,j}}{e\left(T_{2,j}, g \cdot x\right) \cdot SK_c} \\ &= \frac{e(PK_d \cdot H(kw_k), x) \cdot e(g \cdot r_k, x \cdot PK_c)}{e\left(I_{2,i}, PK_d\right) \cdot SK_c} \\ &= \frac{e(s_d \cdot g \cdot H(kw_k), x) \cdot e(g \cdot r_k, x \cdot g \cdot s_c)}{e(g \cdot r_k, g \cdot x) \cdot s_c} \\ &= e(s_d \cdot g \cdot H(kw_k), x) \end{aligned} \tag{3}$$

After the calculation, if the left side is equal to the right side, the keywords match. The cloud service will remove the confusing files and return them to the data consumer.

5.2 Security Analysis

5.2.1 Confidentiality, Integrity, and Non-Repudiation

Firstly, in our scheme, after data collectors such as smart meters collect the grid user data, they first perform symmetric encryption as well as hash calculation on it. The message digest is then uploaded to the data center as an attachment to the encrypted file for subsequent searchable encryption operations. After data users get ciphertext data, they can use the symmetric key obtained by the implementation to decrypt and verify whether the data content has been tampered with. This can effectively protect the confidentiality and integrity of private data. In addition, we also incorporate blockchain in the scheme, where all privacy data access operations are recorded on the blockchain. If an organization has retrieved the data, it can be traced back to the malicious data user through the blockchain's traceability mechanism.

5.2.2 Provable Security

Our scheme can be proved to be secure under the DBDH assumption. Nayak et al. [18] proposed a data outsourcing storage scheme based on searchable encryption and inverted index. In their scheme, the public key of the data user is included in the encrypted index. In other words, it means that the accessibility of the encrypted index is restricted at the stage of generating the encrypted index. In the smart grid scenario, this scheme of specifying data users is difficult to achieve data sharing. Therefore, we have redesigned the key of the scheme and introduced blockchain as the network infrastructure. Nayak et al. have performed a detailed security proof in their scheme reference [18], hence the security proof is not the main part of our discussion.

5.3 Performance Analysis

To verify the feasibility of our system, we simulated a ciphertext retrieval scenario in a computer software environment with 100 files and 100 keyword spaces. The computer operating system is Windows 10-64bit, hardware is i5-12490f 3.0GHz CPU, 32 GB Mem. We use version 2.0.0 version of JPBC library [19], which is a wrapper for PBC library [20] by Java and supports bilinear pair operation. For system security, our scheme is based on the elliptic curve as $y^2 = x^3 + x$.

Our simulation experiments are divided into control group and experimental group, each encrypted file corresponds to five keywords, and the number of keywords contained in the retrieval trap gate is also five. Specifically, the control group followed the traditional searchable encryption scheme, which iterated through all the encrypted files. The experimental group, by contrast, searched according to an inverted index of five encrypted files. The BuildIndex and TokenGen parts of the two experiments are the same, and the specific time consumption is shown in Fig. 4. We can observe that the time consumption of this part increases linearly with the size of the encrypted file, and the time complexity of the two parts is approximately equal, which is also in line with our expectation for the calculation formula. In terms of retrieval time, it can be seen from Fig. 5 that our scheme is more efficient in retrieving a large number of encrypted files in the scenario. The main reason for the difference is that we use an inverted index file to build an inverted index file for a group of five encrypted files, which is also in line with the role of the data center in our scheme.

6 Conclusion

In this paper, we propose a blockchain-based encrypted data retrieval scheme for smart grid that effectively solves the problem of retrieving large-scale encrypted data under smart grid. By using searchable encryption with inverted indexing, the data center collects a sufficient number of encrypted files and message digests, and then generates inverted index files and obfuscates them. It is then uploaded to the cloud service where data users can submit keyword requests to the data center for retrieval trapdoors. The retrieval trapdoor can be submitted to the cloud service for ciphertext retrieval, and all access operations in between are recorded on the blockchain.

Compared with the existing scheme, the main innovation of our scheme is the use of inverted index technology. In the smart grid scenario where the number of encrypted files is much larger than the ciphertext space, our scheme can effectively save the ciphertext retrieval time and avoid traversing all encrypted files. However, the optimization of inverted index files on the cloud service has not been carefully considered, and will be our focus in the future.

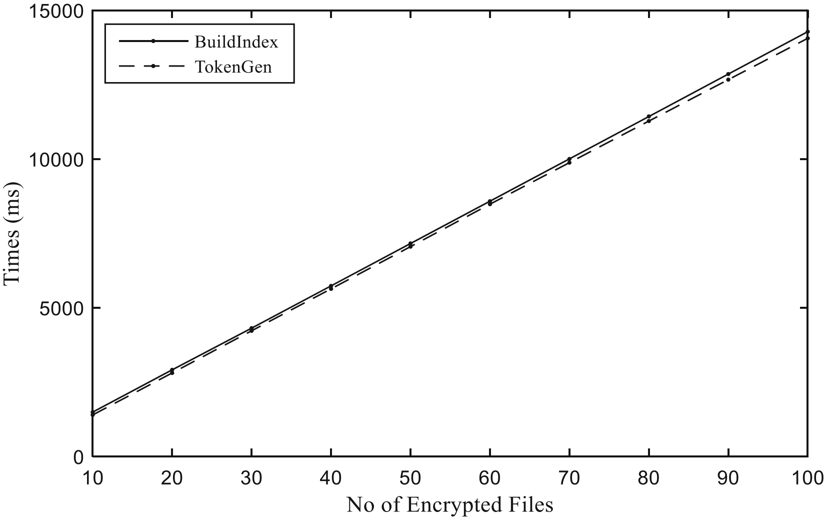


Fig. 4. BuildIndex and TokenGen time

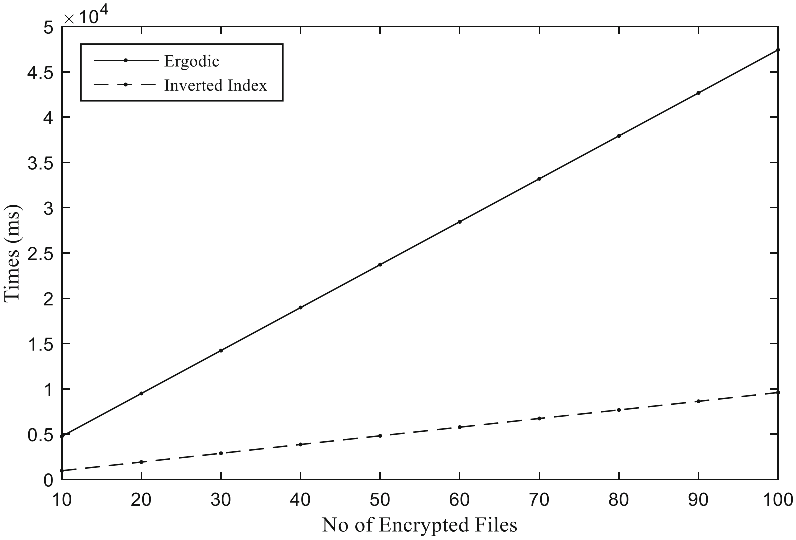


Fig. 5. Retrieval time

Acknowledgments. This work was supported by the NSFC (GrantNos.72293583, 62271070,61962009), and the Project (GrantNo.JCKY2021208B036).

References

1. Iqbal, J., et al.: A generic internet of things architecture for controlling electrical energy consumption in smart homes. Sustain. Cities Soc. **43**, 443–450 (2018)
2. Nguyen, T., Wang, S., Alhazmi, M., Nazemi, M., Estebsari, A., Dehghanian, P.: Electric power grid resilience to cyber adversaries: State of the art. IEEE Access **8**, 87592–87608 (2020)
3. Pham, C.T., Månsson, D.: A study on realistic energy storage systems for the privacy of smart meter readings of residential users. IEEE Access **7**, 150262–150270 (2019)
4. Wang, Z.: An identity-based data aggregation protocol for the smart grid. IEEE Trans. Industr. Inf. **13**(5), 2428–2435 (2017)
5. Kumar, A., Abhishek, K., Shah, K., Namasudra, S., Kadry, S.: A novel elliptic curve cryptography-based system for smart grid communication. Int. J. Web Grid Serv. **17**(4), 321–342 (2021)
6. Giri, J., Sun, D., Avila-Rosales, R.: Wanted: A more intelligent grid. IEEE Power Energ. Mag. **7**(2), 34–40 (2009)
7. Song, D. X., Wagner, D., Perrig, A.: Practical techniques for searches on encrypted data. In: Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000, pp. 44–55. IEEE (2000)
8. Eltayieb, N., Elhabob, R., Hassan, A., Li, F.: An efficient attribute-based online/offline searchable encryption and its application in cloud-based reliable smart grid. J. Syst. Architect. **98**, 165–172 (2019)
9. Wen, M., Lu, R., Zhang, K., Lei, J., Liang, X., Shen, X.: PaRQ: A privacy-preserving range query scheme over encrypted metering data for smart grid. IEEE Trans. Emerg. Top. Comput. **1**(1), 178–191 (2013)
10. Wang, D., Wu, P., Li, B., Du, H., Luo, M.: Multi-keyword searchable encryption for smart grid edge computing. Electr. Power Syst. Res. **212**, 108223 (2022)
11. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: "An overview of blockchain technology: Architecture, consensus, and future trends." In: 2017 IEEE International Congress on Big Data (BigData congress), Honolulu, HI, USA, pp. 557–564 (2017)
12. Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., Wang, F.Y.: "An overview of smart contract: architecture, applications, and future trends." In: 2018 IEEE Intelligent Vehicles Symposium (IV), Changshu, JiangSu, China, pp. 108–113 (2018)
13. Dong, Z., Luo, F., Liang, G.: Blockchain: A secure, decentralized, trusted cyber infrastructure solution for future energy systems. J. Mod. Power Syst. Clean Energy **6**(5), 958–967 (2018)
14. Pathak, R., Gupta, N., Khetarpal, P., Jain, S.: BIJLI: A hyperledger-based blockchain-powered application for decentralized power management and electricity distribution. In: Applications of Computing, Automation and Wireless Systems in Electrical Engineering, pp. 363–372. Springer, Singapore (2019)
15. Wang, J., Wu, L., Choo, K.K.R., He, D.: Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure. IEEE Trans. Industr. Inf. **16**(3), 1984–1992 (2019)
16. Khattak, H.A., Tehreem, K., Almogren, A., Ameer, Z., Din, I.U., Adnan, M.: Dynamic pricing in industrial internet of things: Blockchain application for energy management in smart cities. J. Inf. Secur. Appl. **55**, 102615 (2020)
17. Pibiri, G.E., Venturini, R.: Techniques for inverted index compression. ACM Comput. Surv. (CSUR) **53**(6), 1–36 (2020)
18. Nayak, S.K., Tripathy, S.: SEPS: Efficient public-key based secure search over outsourced data. J. Inf. Secur. Appl. **61**, 102932 (2021)
19. Caro De, A., Iovino, V.: "jPBC: Java pairing based cryptography." In: 2011 IEEE Symposium on Computers and Communications, pp. 850–855 (2011)
20. Lynn, B.: URL: https://crypto.stanford.edu/pbc, (2013)

Design and Implementation of Distributed Architecture for Test Data Analysis Platform

Weidong Qian[1,1](✉), Yanling Yao[2], Da Lin[1], Yuan Xu[1], Haihong Wu[3], and Haijian Shao[4]

[1] China Ship Scientific Research Center, Wuxi 214082, Jiangsu, China
qianwd@cssrc.com.cn
[2] China Gas Turbine Establishment, Chengdu 610500, China
[3] CSSC Orient Wuxi Software Technology Co., Ltd, Wuxi, China
[4] University of Nevada, Las Vegas, United States

Abstract. According to the existing business characteristics of the test data analysis platform, a distributed architecture scheme suitable for aviation, aerospace, shipbuilding and other industries is designed, and a unified description specification for test data is established to solve the problems of data format diversity and data volume under the two scenarios of non-real-time data and real-time data. The platform adopts a hierarchical design idea, and has a detailed design of the platform architecture and business functions. It realizes a high-performance and highly available test data analysis platform, provides rich analysis and drawing functions and data visualization capabilities, and has good scalability.

Keywords: Test data · Unified description specification · Data analysis platform · Data visualization

1 Introduction

Aeroengine is a pneumatic and thermal propulsion machine working on the flight platform, and is the "heart" of the aircraft [1, 2]. Its performance directly affects the flight safety of the aircraft [3]. Therefore, in the process of aeroengine model development, it is necessary to pass research test [4–6], pre-flight performance test [7], type approval test [8], acceptance test [9, 10] and other quality verification tests before type approval acceptance. Each test of aeroengine takes a long time, and the whole test will last for 4−5 years. Sometimes, according to the actual application of the engine, engine modification and troubleshooting tests may be carried out to optimize the relevant functions of the engine or solve the engine failure that occur during the use of the engine. In the longtime test process, a large amount of test data will be generated [11], and the analysis and processing of these test data is an important task in the process of aeroengine model development [12–14].

As the working conditions of the aeroengine are very harsh, and the aeroengine is in the working conditions of high temperature, high pressure and high speed rotation [15], the steady working conditions from the idle state to the take-off state require data

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 179–188, 2024.
https://doi.org/10.1007/978-981-99-7161-9_14

acquisition and recording after the engine is stable. During the test, it is necessary to confirm, judge and store the validity of the real-time collected data. It involves many types of parameters and a large amount of data, which brings difficulties to the analysis and management of test data. The main problems are as follows:

(1) The test parameters are relatively complex, including pressure, temperature, thrust, fuel flow, speed, humidity, area, engine intake interface, air mass flow, engine inlet total pressure, engine inlet total temperature, etc. [16];
(2) There are many data sources and data types, including real-time data, non-real-time data, etc. [17];
(3) Lack of unified description specification for test data, and data processing methods cannot be used universally [18].

In view of the above situation, this paper adopts distributed architecture technology to build a data analysis platform to unify and standardize the test data information. It opens up the interaction of all links and businesses in the data analysis business process, realizes a standard and unified data analysis process, and solves the problem that there are too few experimental data analysis tools and the analysis process is not standardized.

2 Platform Distributed Architecture Design

The data analysis platform adopts a distributed architecture to meet the CAP theory of distributed systems [19–21]. The analysis tool runs on different servers and stores the data in the database after running. The specific architecture is shown in the Fig. 1.

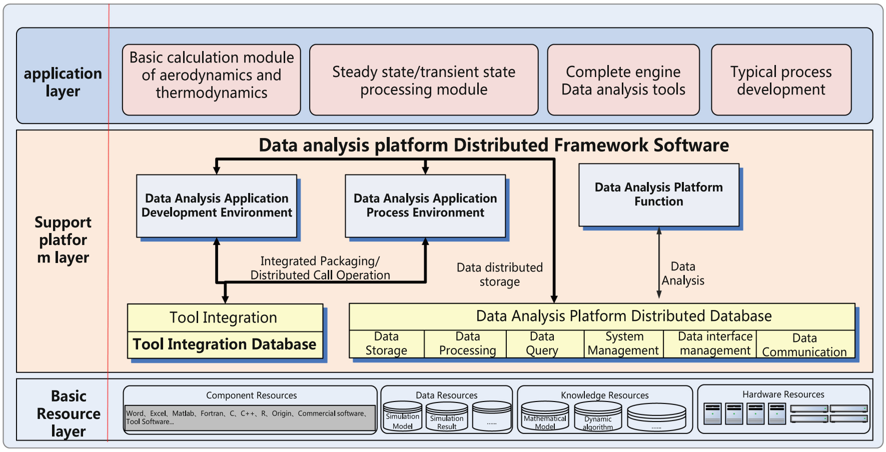

application layer
Basic calculation module of aerodynamics and thermodynamics
Steady state/transient state processing module
Complete engine Data analysis tools
Typical process development
Support platfor m layer
Data analysis platform Distributed Framework Software
Data Analysis Application Development Environment
Data Analysis Application Process Environment
Data Analysis Platform Function
Integrated Packaging/ Distributed Call Operation
Data distributed storage
Data Analysis
Tool Integration
Tool Integration Database
Data Analysis Platform Distributed Database
Data Storage
Data Processing
Data Query
System Management
Data interface management
Data Communication
Basic Resource layer
Component Resources
Word、Excel、Matlab、Fortran、C、C++、R、Origin、Commercial software、Tool Software...
Data Resources
Simulation Model
Simulation Result
......
Knowledge Resources
Mathematical Model
Dynamic algorithm
......
Hardware Resources

Fig. 1. Architecture design of test data analysis platform.

3 Test Data Analysis Platform

3.1 Real-time Data Acquisition Interface

In accordance with the test data processing requirements, the platform analyzes the existing structure of the altitude simulation test bench. Based on TCP/IP transmission protocol, it customizes the special interface for real-time data. The data sends binary data packets at the frequency of 50 frames per second, and obtains the required data through data packet analysis for real-time data processing. The corresponding data processing process is shown in Fig. 2.

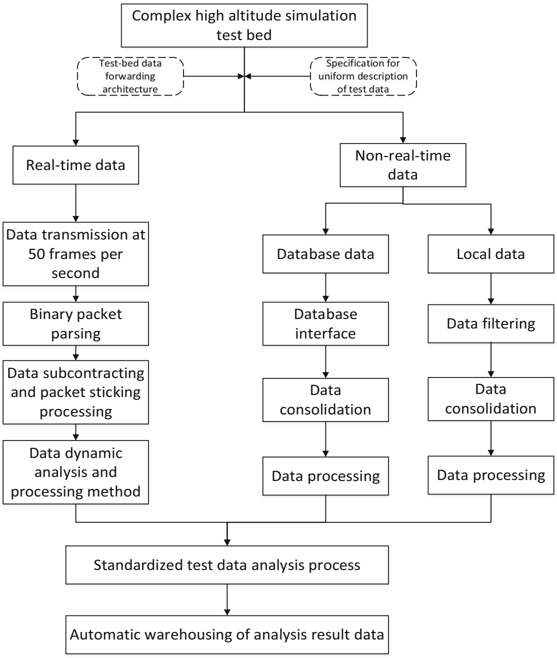

Complex high altitude simulation test bed
Test-bed data forwarding architecture
Specification for uniform description of test data
Real-time data
Non-real-time data
Data transmission at 50 frames per second
Binary packet parsing
Data subcontracting and packet sticking processing
Data dynamic analysis and processing method
Database data
Database interface
Data consolidation
Data processing
Local data
Data filtering
Data consolidation
Data processing
Standardized test data analysis process
Automatic warehousing of analysis result data

Fig. 2. Real-time data acquisition and processing method.

The detailed steps are as follows:

(1) Binary data transmission, acquisition and analysis: define the parsing rules of binary data packets, complete packet header data parsing, and obtain test data description information such as data packet type, length, channel number, etc.

(2) Data packetization and sticky packet handling: As the binary packets sent each time are limited in length, the interface needs to be able to divide and paste binary packets according to the packet length information. That is to say, when the primary information sent is too large to generate a packet, you can paste the packet to get a complete packet, and when the primary information sent is too small to generate a packet, you can subcontract the packet.

(3) Dynamic data analysis and processing method: During real-time data acquisition, the data needs to be recorded locally only when the specific judgment conditions are met. Such judgment conditions are different due to different types of tests and cannot be cured. Therefore, it is necessary to customize a special data dynamic analysis and processing method module. The module loads a dynamic link library in real time with the program startup to perform conditional judgments. A function interface is agreed upon in the link library, in which the user can obtain and process the test data of the specified channel in the last second (Fig. 3).

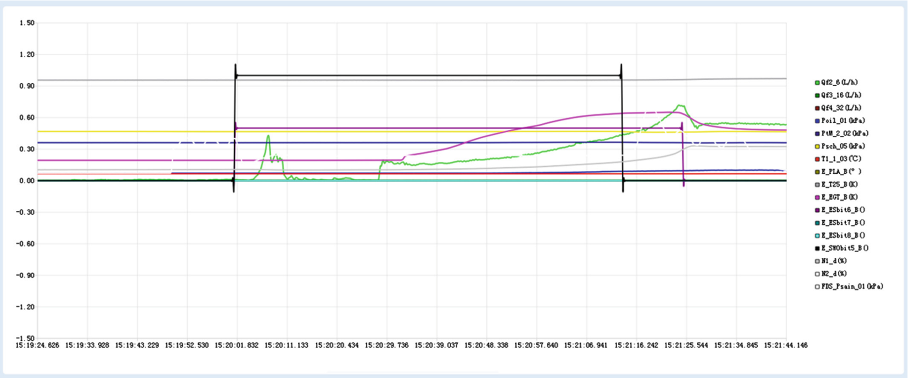


Fig. 3. Human computer interface for real-time data acquisition.

3.2 Data Analysis Toolset

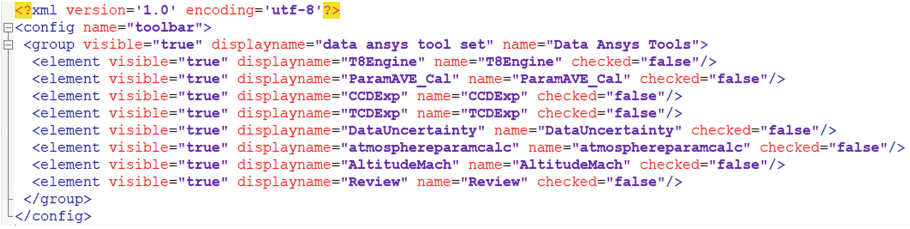
In order to ensure that the standardized processing meets the requirements of rapid analysis and processing, more than ten self-developed small data analysis tool sets with different development environments and programming languages are deeply standardized and integrated. The tool set includes data validation, data uncertainty analysis, non-standard atmospheric performance parameter analysis, performance parameter analysis under uneven intake conditions, engine performance degradation analysis, Reynolds number impact analysis, bypass ratio evaluation, sensitivity analysis, multi-point measurement parameter evaluation, etc. The platform unifies the tool set interface specification to form reusable components, realize standardized modification and management of tool sets, and support subsequent tool set extension.

At the same time, the tool set database is established to manage the tool set, which is convenient for users to call. The existing data analysis tools can be integrated. Most of the existing tools are executable programs and have their own independent interactive interfaces. The software needs to be able to conduct configurable integration and call.

By default, an ansystools folder is added under the directory where the platform starts BAT. Users can add existing tools to this folder directory. The tool directory contains all the dependent files required for program operation by default, and ensure that the startup

EXE has the same name as the tool folder. A png image file with the same name as the tool folder needs to be prepared under the tool directory.

The platform provides a special configuration file to configure the integration tool information, including name, display name, visibility and other information. The specific configuration design is shown in the following Fig. 4.



```
<?xml version='1.0' encoding='utf-8'?>
<config name="toolbar">
 <group visible="true" displayname="data ansys tool set" name="Data Ansys Tools">
  <element visible="true" displayname="T8Engine" name="T8Engine" checked="false"/>
  <element visible="true" displayname="ParamAVE_Cal" name="ParamAVE_Cal" checked="false"/>
  <element visible="true" displayname="CCDExp" name="CCDExp" checked="false"/>
  <element visible="true" displayname="TCDExp" name="TCDExp" checked="false"/>
  <element visible="true" displayname="DataUncertainty" name="DataUncertainty" checked="false"/>
  <element visible="true" displayname="atmosphereparamcalc" name="atmosphereparamcalc" checked="false"/>
  <element visible="true" displayname="AltitudeMach" name="AltitudeMach" checked="false"/>
  <element visible="true" displayname="Review" name="Review" checked="false"/>
 </group>
</config>
```

Fig. 4. Content Profile.

The data analysis tool set interface is shown in the following Fig. 5.

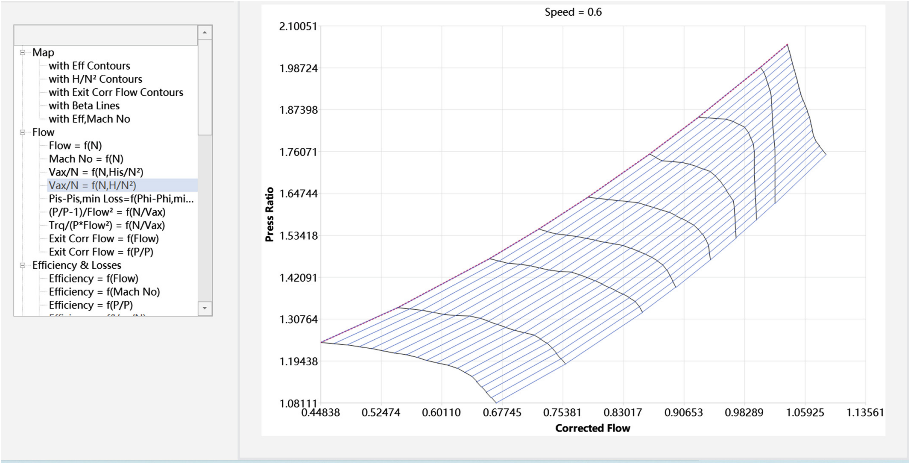


Fig. 5. Unified management and application of toolsets.

3.3 Automatic Analysis Process of Test Data

The platform has developed a data analysis application development environment. Users establish business processes according to specific business requirements to achieve process templating. Through visual workflow and data flow design, a series of process templates are formed. Through unified driving engine, the scheduling of business control processes and automatic data flow are completed. Two typical data automatic analysis processes are built here, which are steady state data processing process and transient state data processing process. The steady state process includes four data tools, which are steady state pretreatment, bad point elimination, air flow calculation, and reasoning calculation. The transient state process includes four data tools, which are data pretreatment, initial value judgment, process calculation, and result output.As shown in Figs. 6 and 7.

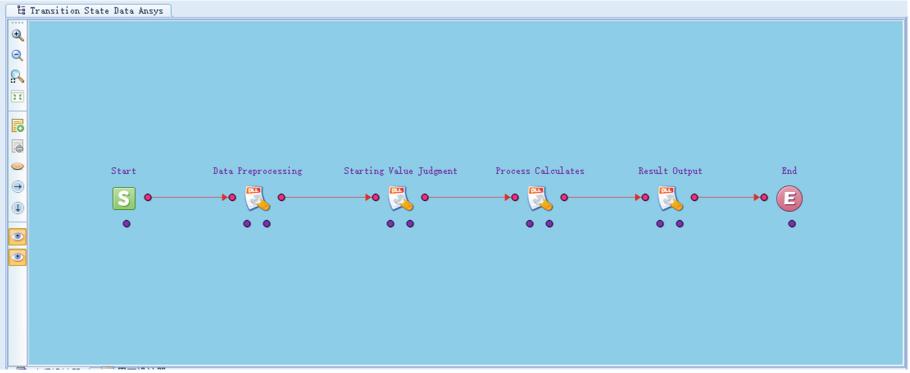


Fig. 6. Analysis and processing flow of transition state data.

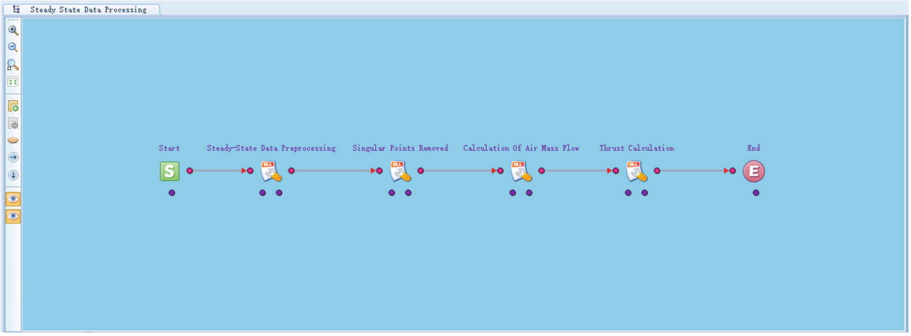

Steady State Data Processing
Start
Steady-State Data Preprocessing
Singular Points Removed
Calculation Of Air Mass Flow
Thrust Calculation
End
S
E

Fig. 7. Analysis and processing flow of steady state data.

3.4 Visualization of Test Data Analysis and Result Management

The platform has completed the fairing module of high-altitude platform test data, including new speed line, setting grid, modifying data, auxiliary grid line definition, reference point definition, flow characteristic fairing, efficiency characteristic fairing, modifying surge point, characteristic checking, data output, etc.

The platform provides a variety of data presentation methods to show data, including tables, curves, charts, etc., to enhance the effect of data visualization. It can draw two-dimensional graphs for data tables, including linear graph, scatter plot, vertical line graph, tooth graph, vertical ladder graph, horizontal ladder graph, double Y-axis graph, waterfall graph, zoom graph, horizontal histogram, stack bar graph, area graph, pie graph, etc. It can also customize a variety of data presentation methods according to the characteristics of the industry, so as to help designers view image data more intuitively and effectively (Fig. 8).

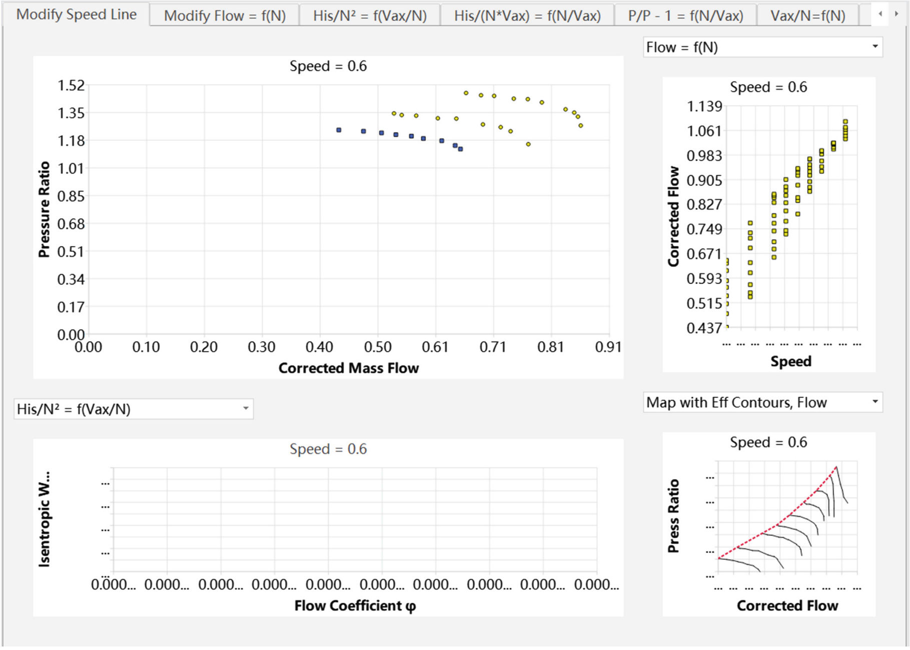


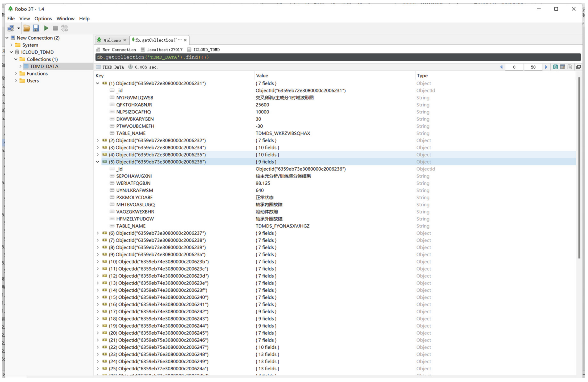
Fig. 8. Visualization of test data results.

The storage method provided by the platform for test data is a combination of structured and unstructured methods. The data records that can be parsed and processed to form database tables are called structured data; Pictures, sounds, videos and other files that do not need to be decomposed are collectively referred to as unstructured files.

Analyze and process the excel file in the compressed package according to the low frequency test data and dynamic test data analysis results provided by the user.

In this module, users can store low-frequency test data and dynamic test data analysis results. For standard format compressed package files, they can import data, analyze the contents of excel files in the compressed package, and generate structural and unstructured data related to low-frequency test data and dynamic test data analysis results, which are then stored in relational database Oracle and NoSQL database Mongodb.

By parsing the excel file, the data in excel is converted into relational data and non-relational data. The relational data is mainly the basic information of the test data, the metadata information of the dynamic data, etc., while the non-relational data is the data with corresponding identification information after processing, which is stored in the non-relational database MongoDB to facilitate subsequent queries and other operations (Fig. 9).



```
db.getCollection('TDMD_DATA').find({})
```

```
Key                                            Value                                    Type
(1) ObjectId("6359eb72e3080000c2006231")       { 7 fields }                             Object
    _id                                        ObjectId("6359eb72e3080000c2006231")     ObjectId
    NYJFGVMLQWSB                               交叉稀疏/主成分1时域波形图                   String
    QFKTGHXABNJR                               25600                                    String
    NLPSIZOCAFHQ                               10000                                    String
    DXWVBKARYGEN                               30                                       String
    PTWVOUBCMEFH                               -30                                      String
    TABLE_NAME                                 TDMDS_WKRZVIBSQHAX                       String
(2) ObjectId("6359eb72e3080000c2006232")       { 7 fields }                             Object
(3) ObjectId("6359eb72e3080000c2006234")       { 10 fields }                            Object
(4) ObjectId("6359eb72e3080000c2006235")       { 10 fields }                            Object
(5) ObjectId("6359eb73e3080000c2006236")       { 9 fields }                             Object
    _id                                        ObjectId("6359eb73e3080000c2006236")     ObjectId
    SEPOHAWJGXNI                               核主元分析/训练集分类结果                    String
    WERIATFQGBJN                               98.125                                   String
    UYNJLKRAFWSM                               640                                      String
    PXKMOLYCDABE                               正常状态                                  String
    MHTBVOASLUGQ                               轴承内圈故障                               String
    VAOZGKWEXBHR                               滚动体故障                                 String
    HFMZELYPUDGW                               轴承外圈故障                               String
    TABLE_NAME                                 TDMDS_FYQNASXVJHGZ                       String
(6) ObjectId("6359eb73e3080000c2006237")       { 9 fields }                             Object
(7) ObjectId("6359eb73e3080000c2006238")       { 7 fields }                             Object
(8) ObjectId("6359eb73e3080000c2006239")       { 7 fields }                             Object
(9) ObjectId("6359eb74e3080000c200623a")       { 7 fields }                             Object
(10) ObjectId("6359eb74e3080000c200623b")      { 7 fields }                             Object
(11) ObjectId("6359eb74e3080000c200623c")      { 7 fields }                             Object
(12) ObjectId("6359eb74e3080000c200623d")      { 7 fields }                             Object
(13) ObjectId("6359eb74e3080000c200623e")      { 7 fields }                             Object
(14) ObjectId("6359eb74e3080000c200623f")      { 7 fields }                             Object
(15) ObjectId("6359eb74e3080000c2006240")      { 7 fields }                             Object
(16) ObjectId("6359eb74e3080000c2006241")      { 7 fields }                             Object
(17) ObjectId("6359eb74e3080000c2006242")      { 9 fields }                             Object
(18) ObjectId("6359eb74e3080000c2006243")      { 9 fields }                             Object
(19) ObjectId("6359eb74e3080000c2006244")      { 9 fields }                             Object
(20) ObjectId("6359eb74e3080000c2006245")      { 7 fields }                             Object
(21) ObjectId("6359eb75e3080000c2006246")      { 7 fields }                             Object
(22) ObjectId("6359eb75e3080000c2006247")      { 10 fields }                            Object
(23) ObjectId("6359eb76e3080000c2006248")      { 13 fields }                            Object
(24) ObjectId("6359eb76e3080000c2006249")      { 13 fields }                            Object
(25) ObjectId("6359eb77e3080000c200624a")      { 13 fields }                            Object
```

Fig. 9. Non-relational data storage.

After importing the compressed package, the Excel test data file in the compressed package will be automatically parsed and parsed in the new interface. Realize the automatic data import function, including the import and modification of single image data according to the corresponding requirements, and the batch import of multiple image data in the same format. After the analysis and processing, the data in the specified format will be output according to the user's needs. According to the actual use and format setting, the data will be output in the form of interface and report. The report data file format includes txt, dat, etc., for the use of report preparation, data processing, calculation and evaluation.

This module provides the import and export of various international and domestic standard data formats, including TXT, DAT, etc. The system can configure different import schemes for image data in different formats, such as the delimiter of each line of data, ignoring the number of starting lines, and whether to simplify the space at the end of the line. One configuration can be used for multiple image data files. After the data is imported successfully, it will be displayed in the form of a table in the software (Fig. 10).

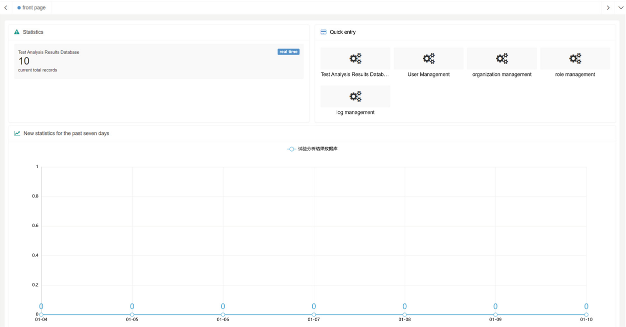
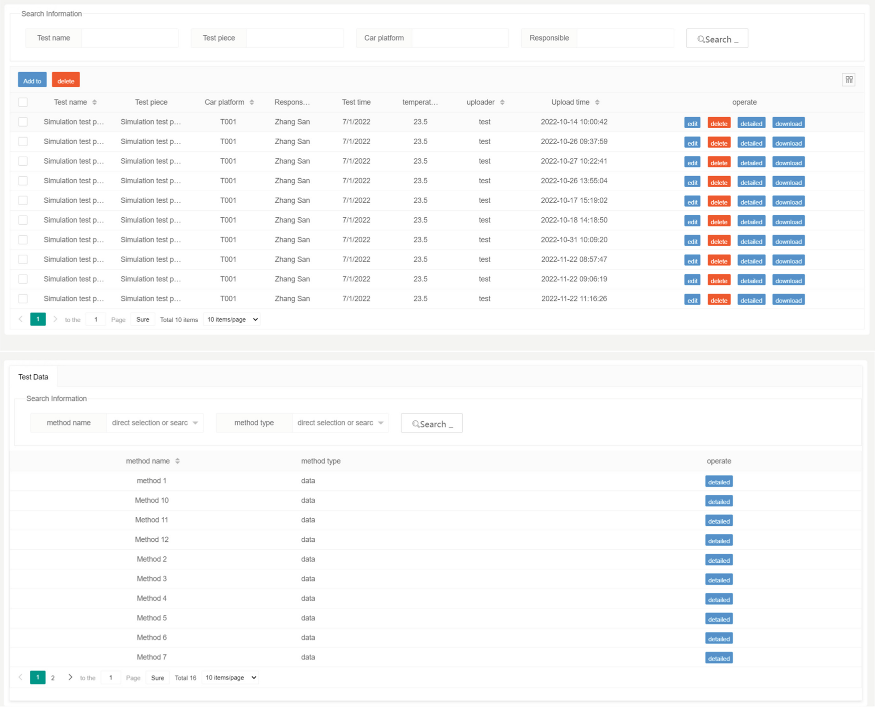


Fig. 10. Test data import.

The platform dynamically parses the imported low-frequency test data and dynamic test data analysis results, and generates different query conditions. The query method is fuzzy query. The query method first differentiates the query according to the user query content, and manages the test data to facilitate subsequent data analysis (Fig. 11).



	Test name	Test piece	Car platform	Respons…	Test time	temperat…	uploader	Upload time	operate
□	Simulation test p…	Simulation test p…	T001	Zhang San	7/1/2022	23.5	test	2022-10-14 10:00:42	edit delete detailed download
□	Simulation test p…	Simulation test p…	T001	Zhang San	7/1/2022	23.5	test	2022-10-26 09:37:59	edit delete detailed download
□	Simulation test p…	Simulation test p…	T001	Zhang San	7/1/2022	23.5	test	2022-10-27 10:22:41	edit delete detailed download
□	Simulation test p…	Simulation test p…	T001	Zhang San	7/1/2022	23.5	test	2022-10-26 13:55:04	edit delete detailed download
□	Simulation test p…	Simulation test p…	T001	Zhang San	7/1/2022	23.5	test	2022-10-17 15:19:02	edit delete detailed download
□	Simulation test p…	Simulation test p…	T001	Zhang San	7/1/2022	23.5	test	2022-10-18 14:18:50	edit delete detailed download
□	Simulation test p…	Simulation test p…	T001	Zhang San	7/1/2022	23.5	test	2022-10-31 10:09:20	edit delete detailed download
□	Simulation test p…	Simulation test p…	T001	Zhang San	7/1/2022	23.5	test	2022-11-22 08:57:47	edit delete detailed download
□	Simulation test p…	Simulation test p…	T001	Zhang San	7/1/2022	23.5	test	2022-11-22 09:06:19	edit delete detailed download
□	Simulation test p…	Simulation test p…	T001	Zhang San	7/1/2022	23.5	test	2022-11-22 11:16:26	edit delete detailed download

< 1 > to the 1 Page Sure Total 10 items 10 items/page

method name	method type	operate
method 1	data	detailed
Method 10	data	detailed
Method 11	data	detailed
Method 12	data	detailed
Method 2	data	detailed
Method 3	data	detailed
Method 4	data	detailed
Method 5	data	detailed
Method 6	data	detailed
Method 7	data	detailed

< 1 2 > to the 1 Page Sure Total 16 10 items/page

Fig. 11. Test data management

4 Concluding Remarks

This paper proposes a set of distributed architecture scheme suitable for aviation, aerospace, shipbuilding and other industries, and implements a high-performance, highly available test data analysis platform. It was deployed and implemented in the laboratory of Mianyang Gas Turbine Research Institute in Sichuan, China, and initially formed a complex high-altitude simulation test bed test data analysis business system, realizing effective processing and rapid analysis of real-time and non-real-time data. At present, a general test data analysis expert system is formed by integrating conventional mathematical analysis, data validation, uncertainty evaluation, test performance analysis and other task tool sets under the unified platform interface. It solves the current problems of too few test data analysis tools and nonstandard analysis process, and improves the test data analysis ability and efficiency.

References

1. Yang, P.: Research status and prospects of materials for Aero-engines in China. J. Phys: Conf. Ser. (2021). https://doi.org/10.1088/1742-6596/1802/2/022049
2. Qiu, L.: Strength and stiffness analysis of a test module for aero-engines under complex load conditions. Beijing University of Chemical Technology, Master (2020)
3. Hu, B., Xu, Y., Liu, Z et al.: Design of a massive test data playback system for an aeroengine. Aeronaut. Comput. Technol. **49**(04), 119–122 (2019)
4. Luan, X., Gao, Y., Zhang, Z et al.: Experimental and numerical study on stress distribution characteristics of traveling wave resonance of high-speed bevel gear in Aero-engine. Appl. Sci. **13**(3), 1814 (2023)
5. Seyed-Ehsan, M.-H., Kamran, B.: Nonlinear effects of bolted flange connections in aeroengine casing assemblies. Mech. Syst. Signal Process. **166**(10), 108433 (2022)
6. Huanxian, B., Huang, X., Zhang, X.: An overview of testing methods for aeroengine fan noise. Prog. Aerosp. Sci. (2021). https://doi.org/10.1016/j.paerosci.2021.100722
7. Gong, W., Liu, G., Wang, J et al.: Aerodynamic and thermodynamic analysis of an aero-engine pre-swirl system based on structure design and performance improvement. Aerosp. Sci. Technol. (2022). https://doi.org/10.1016/j.ast.2022.107466.
8. Xue, H., Chang, H., Liu, X.: Technical research on the ground water ingestion test equipment of a certain type of Aeroengine. Mech. Eng. (01), 64–65+71 (2019)
9. Feng, W.: A review of reliability testing of aero-engine components. Popul. Stand. **04**, 165–167 (2021)
10. Gong, Q et al.: Model reliability engineering manual. National Defense Industry Press, Peking (2004)
11. Zhang, D., Chen, Z., Ding, T.: Application about data acquisition system in aero engine test management. Intern. Combust. Engine & Parts **06**, 164–166 (2022)
12. Peng, L: Design of Aeroengine test data analysis platform based on LabVIEW. Comput. Program. Ski. Maint. (03), 118–120+144 (2019)
13. Li, Y., Li, J., Qi, Y.: Discussion on aeroengine test and data management technology. Public Commun. Sci. & Technol. **11**(21), 91–92 (2019)
14. Wen, W., Chen, Z., Cao, Y et al.: Design of data management system in Aeroengine test. Aeroengine **47**(03), 97–102 (2021)
15. Liu, X., Liu, K.: Composition and development of aeroengine test technology. Autom. & Instrum. **01**, 1–6 (2022)
16. Bo, Z.: Research on aeroengine test and data management technology. Electron. Test **12**, 78–79 (2017)
17. Yuankun, G.: Research on key technologies of aeroengine product development process integration. Northwestern Polytechnical University, Doctor (2006)
18. Wang, S., Shi, L.: Research on key technologies of aeroengine data sharing. Mech. Sci. Technol. **37**(08), 1306–1312 (2018)
19. Wang, R., Jianjun, W., Hou, J.: Distributed real time computing engine–Storm research. China Sci. Technol. Inf. **06**, 68–69 (2015)
20. Chen, M.: CAP Theory of distributed system design. Comput. Educ. **15**, 109–112 (2015)
21. Sun, X., Zhang, W.: The dynamic data privacy protection strategy based on the CAP theory. Int. J. Interdiscip. Telecommu Netw. (IJITN) **7**(1), 44–56 (2015)

An Intelligent Optimization Algorithm Based on Adaptive Change Mechanism

Yanling Yao[1](✉), Feng Wu[1], Da Lin[2], Weidong Qian[2], Haihong Wu[3], and Haijian Shao[4]

[1] China Gas Turbine Establishment, Chengdu 610500, China
aeccyaoyanling@126.com
[2] China Ship Scientific Research Center, Jiangsu, Wuxi 214082, China
[3] CSSC Orient Wuxi Software Technology Co., Ltd, Wuxi, China
[4] University of Nevada, Las Vegas, USA

Abstract. Aiming at the urgent need and existing bottleneck of model parameter optimization in data enrichment in engine design and application, the problem of large dispersion of data enrichment results caused by the uncertainty of data input was carried out. A self-optimization algorithm with the goal of minimizing global deviation was developed in the uncertainty interval by combining multiple input parameters, and the multi-objective problem was converted into a single objective problem by adding weights, The adaptive weight change mechanism is introduced to balance the optimization intensity of each objective. In the end, the algorithm gets only one solution, which eliminates the difficulty of engineers' selection of solutions and greatly improves the efficiency of optimization.

Keywords: Rich data · Optimization of model parameters · Adaptive change mechanism · Self-optimization algorithm

1 Introduction

In the domestic engine test, there are more or less insufficient interpretation of the exposure problems in the test, positioning analysis is not in place. Part of the reason is due to the complex structure of the aero-engine, the high degree of system integration, the harsh service environment, and changeable working conditions, at the same time, there are restrictions such as limited online testing conditions and difficult to guarantee the amount of diagnostic information [1]. Some other factors come from the lack of summary of the common laws between domestic and foreign models [5], and insufficient understanding of the strengths and weaknesses of various models of engines. If these information belonging to different engines can be summarized and refined, it can provide a lot of experience for model design test [6]. To carry out the above work, we need a large number of accurate data that can be used for explicit direct comparison as support, so data enrichment technology came into being.

Unlike the traditional gradient based optimization algorithm, which uses a single initial point, the intelligent optimization algorithm is based on the data enrichment algorithm and optimization algorithm [2]. Starting from the original data directly measured

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 189–199, 2024.
https://doi.org/10.1007/978-981-99-7161-9_15

in the experiment, the full view of the aeroengine is obtained through reasonable constraints and extrapolation. The population based on multiple initial points is used as the initial population, and the bionic random operator is used to generate new solutions. Evaluate the above solutions by calling black-box or white-box optimization objective function [3], select a certain amount of excellent solutions as the next generation parent population according to the corresponding objective function value, and search for the optimal solution through multiple iterations [4]. By mastering these more comprehensive data, we can more clearly grasp the performance matching of the main engine components and the changes under various test conditions, so as to better interpret and evaluate the test results.

The establishment of intelligent optimization algorithm based on adaptive change mechanism can enrich the existing test data, and there is an overall understanding of the parameter change pattern during the enrichment process, which is of practical significance for the optimization of key parameters of various parts of the engine.

2 Multi-objective Optimization Algorithm

Based on the original genetic algorithm, an adaptive weight change mechanism is proposed to automatically adapt the evaluation function to a specific optimization problem by different weights without prior knowledge between different objectives for different working conditions. For super multi-objective optimization problems, common multi-objective optimization algorithms, such as NSGA-II, NSGA-III, MOEA/D, have many problems in solving super multi-objective problems [7]. The research on such super multi-objective problems in evolutionary computing is still immature. Therefore, we transform the multi-objective problems into a single-objective problem by summing up the multi-objectives by weights. Further, in order to solve the problem that the single-objective optimization algorithm cannot balance multiple objectives, we add a weight adaptive mechanism to the original single-objective algorithm to guide the setting of weights by the final error during the evolutionary process, i.e., the final result error is fed back to the optimization process to form a closed loop.

Converting the multi-case multi-objective problem into a single-objective problem with average working error, which greatly reduces the difficulty of optimization and the generalization ability of the model itself. In practical application, there are a lot of problems with multiple operating conditions and multiple objectives. The common solution is to optimize the evaluation function of the worst operating condition, however, in the actual operation of this program, it was found that using the worst condition as the direction of optimization would reduce the error of other working conditions while increasing the error of other working conditions. After analyzing the reasons, it is believed that this is because only optimizing the worst working condition can not ensure that the error of other working conditions can be effectively reduced. Therefore, we finally convert the multi-case problem into a single-case problem by taking the average value of each working condition, which can ensure that the different optimization environments of all working conditions are considered and provide more guidance for the direction of optimization.

2.1 Establishment of Optimization Model

In this study, the data enrichment process is modeled as a data generation model error minimization problem, i.e., a model parameter optimization problem, as follows:

$$\min\left|100\cdot\sum_{i=1}^{M}\alpha_i\left|\frac{f_i\prime}{f_i}-1\right|\right| \tag{1}$$

where, M denotes the number of optimization targets. α_i is the weight coefficient of each objective, i.e., it indicates the difficulty of optimizing different objectives (which can be artificially specified by a priori knowledge or dynamically adjusted during the optimization process).f_i denotes the true value of the target under the training number.f_i' refers to the approximation values of the different objectives calculated after obtaining the optimization parameters.

The difficulty in solving this problem arises from the multi-case scenario requirements and the black box model. First of all, in terms of problem modeling, there is a contradiction in the performance of the generated model under the same set of parameters for different operating conditions, i.e., optimizing the model error in one operating condition leads to an increase in the error in other operating conditions, so that it is impossible to obtain a solution applicable to all operating conditions. The contradiction between the above operating conditions increases the difficulty of problem solving. Secondly, the data generation model is black-box, that is, the internal structure is unknown. Due to the lack of corresponding a priori knowledge, there is no definite expression for the optimization objective function, so it cannot be solved by gradient-based optimization methods, and only non-gradient evolutionary algorithms can be used to solve it.

In addition, since there are multiple objectives of the output of this problem, traditional multi-objective evolutionary algorithms do not have good generalizability in solving this super-multi-objective optimization (many-objective) and do not have any a priori knowledge between the output objectives. At the same time, the output of the multi-objective algorithm is the Pareto non dominated solution set, that is, no solution in this solution set is better than the other solution on all objectives, and it is difficult to determine the final solution. The output of multiple solutions makes it more difficult for engineers to select the final solution, especially when it is difficult to select a superior solution without prior knowledge and preference. In this regard, in this study, the multi-objective is converted into a single-objective problem by summing the weights in combination with a specific problem, and the adaptive change mechanism of the weights is introduced to balance the optimization strength of each objective so that the algorithm finally obtains a unique solution, eliminating the difficult part of the engineer's selection of the solution.

2.2 Optimization Algorithm Termination Condition

In order to combine the optimized global information and local information, we use the simplified Kalman filter to calculate the mutual control ratio s_t, and decide whether to terminate the optimization according to s_t. For the convenience of introduction, we introduce the termination optimization algorithm by taking the calculation of s_t in the t-th optimization as an example.

First, calculate the prior estimate $\hat{s}_t^-$ of s_t. To simplify the calculation, let A = 1 and B = 0. This means that we consider that each generation of the optimization maintains a certain advantage over the previous generation, namely:

$$\hat{s}_t^- = \hat{s}_{t-1} \tag{2}$$

At the same time, the process of updating and calculating the covariance matrix is simplified.

$$P_t^- = P_{t-1} \tag{3}$$

$$z_t = s_t \tag{4}$$

The above two equations respectively indicate that the error of mutual control ratio of each iteration is the same and the s_t calculated by the formula each time contains local information.

Thus, the information gain can be expressed as:

$$K_t = \frac{P_t^-}{P_t^- + R} \tag{5}$$

Meanwhile, the posterior estimate of the mutual control ratio is:

$$\hat{s}_t = \hat{s}_t^- + K_t\left(z_t - \hat{s}_t^-\right) \tag{6}$$

The posterior estimation of the mutual control ratio of each generation contains the global and local information of the optimization, which is used as the termination criterion of the optimization algorithm. In addition, the minimum threshold of mutual control ratio $\hat{s}_{\min}$ shall be specified in advance. When Eq. (7) (Table 1):

$$\hat{s}_t < \hat{s}_{\min} \tag{7}$$

When established, the optimization is terminated.

Table 1. Termination optimization algorithm steps.

Serial number	Terminate the optimization algorithm process
1	Initialize $t = 0$, $\hat{s}_0 = 1$
2	Set R
3	Set the maximum number of iterations $t_{\max}$
4	Set minimum mutual control ratio $\hat{s}_{\min}$

(*continued*)

Table 1. (*continued*)

Serial number	Terminate the optimization algorithm process
5	while $\hat{s}_t \geq \hat{s}_{\min}$ and $t < t_{\max}$ do:
6	Execute an iterative process of evolutionary algorithm
7	$t = t + 1$
8	Calculate the prior estimate of the mutual control ratio, $\hat{s}_t^-$, Using Eq. (2)
9	Calculate the measured value of the mutual control ratio, z_t, Using Eqs. (3) and (4)
10	Obtain a posteriori estimates of the mutual control ratio, $\hat{s}_t$, Using Eqs. (6) and (7)
11	End while (End cycle)

3 Data Enrichment Algorithm

3.1 Algorithmic Logic

The aero-engine data enrichment software is suitable for engines of various configurations, supporting configuration selection and independent expansion of subsequent algorithms. The software analyzes the aero-engine data measured by the test, and the user customizes the split of the test data, defining the data as: reference points, training points and validation points. The user can modify key parameters of the algorithm such as optimization times, population number, iteration termination parameters, etc. through the interface.

The data enrichment algorithm enriches the test data by inputting the engine test data, and outputs key information at different sections of the aeroengine, such as pressure ratio, flow rate, efficiency, etc. [8]. The algorithm execution logic is shown in Fig. 1.

3.2 Algorithm Input and Output

(1) Input

The data rich input parameters are some engine test parameters.

p2_od denotes Inlet pressure. t2_od denotes Inlet temperature. Pamb_od denotes Environmental pressure. p3tar_od denotes Culvert pressure.

(2) Output

The test data is enriched through the data enrichment algorithm, and the output results are the key parameters of each section of the engine. See the following table for detailed output data (Table 2).

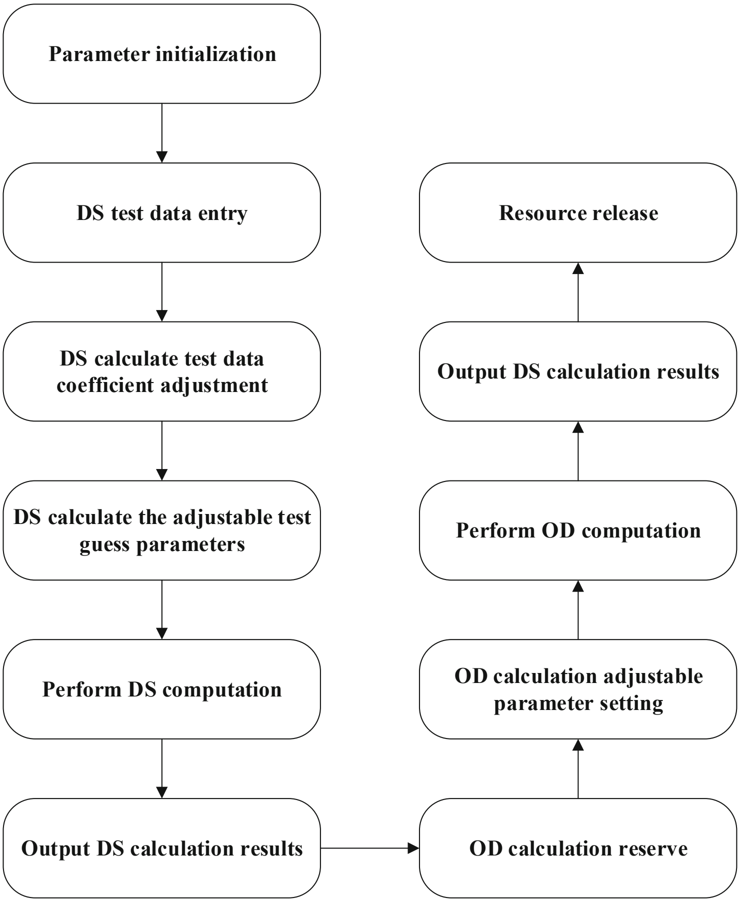

Parameter initialization
DS test data entry
DS calculate test data coefficient adjustment
DS calculate the adjustable test guess parameters
Perform DS computation
Output DS calculation results
OD calculation reserve
OD calculation adjustable parameter setting
Perform OD computation
Output DS calculation results
Resource release

Fig. 1. Data-rich algorithm operation logic.

The results of the data enrichment process are dynamically displayed, and the values of each point are viewed, as shown in Fig. 2.

Table 2. Key output parameters of data enrichment.

Key output parameters			
odo_W2	Converted flow	odo_WF	Combustion chamber outlet temperature
odo_P3	Compressor pressure ratio	odo_T3	Compressor efficiency
odo_P13	External culvert pressure ratio of fan	odo_T21	Fan intrinsic efficiency
odo_P44	High pressure turbine efficiency	odo_P5	Low pressure turbine efficiency
odo_T16	Heat transfer coefficient of internal and external culverts	odo_FN	Nozzle thrust coefficient
odo_T5	Design culvert ratio	odo_P21	Internal pressure ratio of fan
odo_T13	Fan external efficiency	odo_P16	External culvert pressure ratio
odo_A8	Nozzle flow coefficient		

4 Intelligent Optimization Algorithm Software

4.1 Algorithm Configuration

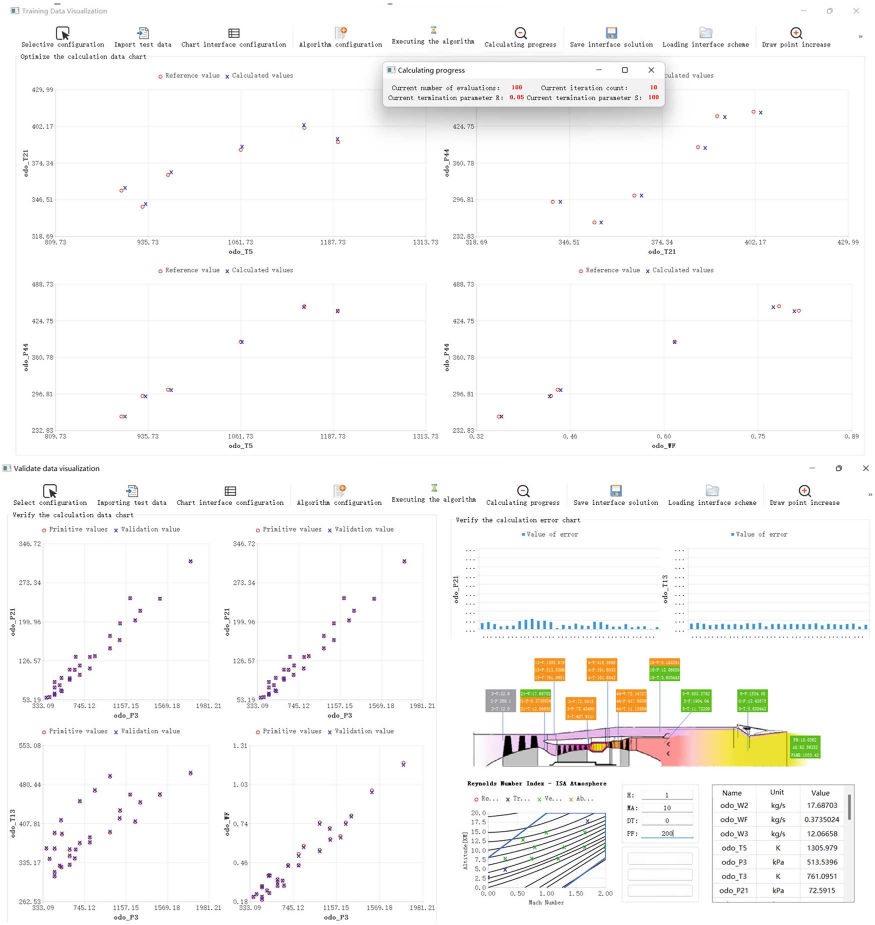
The user can click the configuration selection button on the interface to select the required configuration in the pop-up window of algorithm configuration selection. In addition, this software supports the user to independently expand the engine configuration in the future, and the engine algorithm configuration expansion can be completed by supplementing the document in the specified format under the background corresponding directory (Fig. 3).

4.2 Interface Scheme Design

After the user selects the test file that requires rich data, the software automatically parses the file, and users can customize the test data into reference points, training points and verification points according to the data display interface. After classification, click OK, and the background will classify and write the data to different files to provide input files for subsequent data optimization and enrichment (Fig. 4).

4.3 Test Point Display

Test point display. After the user imports the test data, click the test point display button to pop up the test point pop-up drawing, which consists of the formula curve base map and data points (Fig. 5).



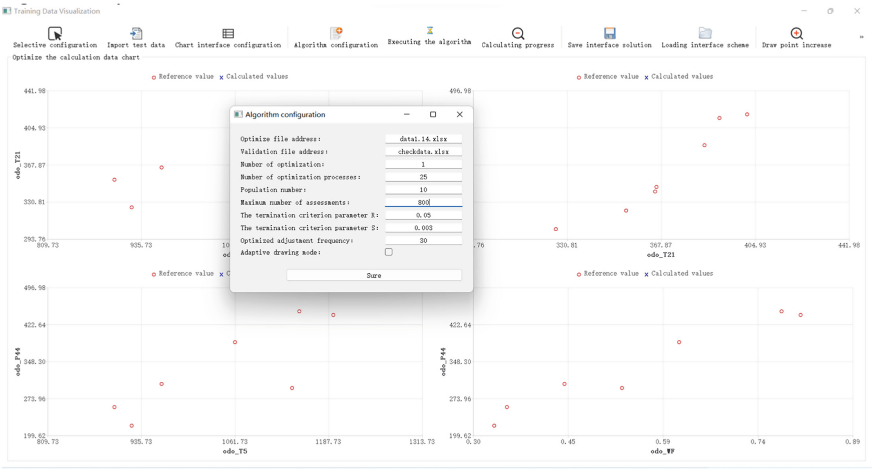
Calculating progress

Current number of evaluations: 100 Current iteration count: 10
Current termination parameter R: 0.05 Current termination parameter S: 100

H: 1
MA: 10
DT: 0
PF: 200

Name	Unit	Value
odo_W2	kg/s	17.68703
odo_WF	kg/s	0.3735024
odo_W3	kg/s	12.06658
odo_T5	K	1305.979
odo_P3	kPa	513.5396
odo_T3	K	761.0951
odo_P21	kPa	72.5915

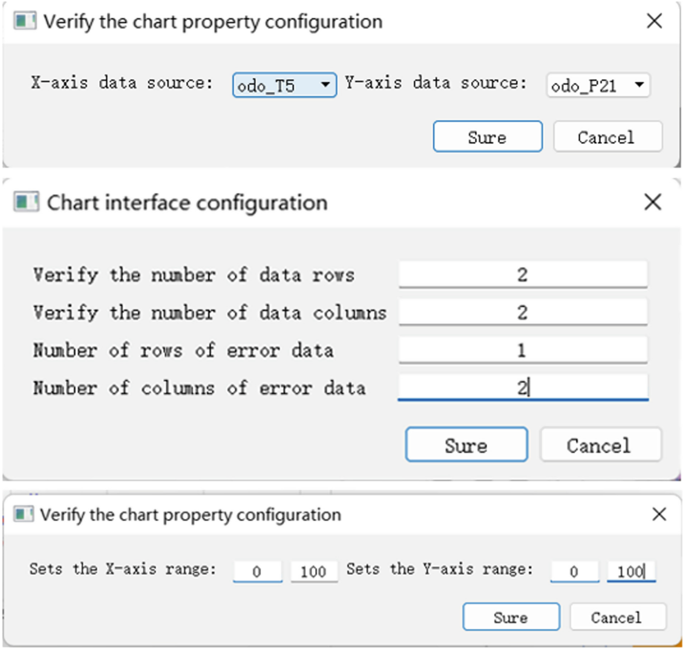
Fig. 2. Data enrichment results output.



Algorithm configuration

Optimize file address: data1.14.xlsx
Validation file address: checkdata.xlsx
Number of optimization: 1
Number of optimization processes: 25
Population number: 10
Maximum number of assessments: 800
The termination criterion parameter R: 0.05
The termination criterion parameter S: 0.003
Optimized adjustment frequency: 30
Adaptive drawing mode: □

Fig. 3. Algorithm configuration.



Verify the chart property configuration

X-axis data source: odo_T5 Y-axis data source: odo_P21

Chart interface configuration

Verify the number of data rows 2
Verify the number of data columns 2
Number of rows of error data 1
Number of columns of error data 2

Verify the chart property configuration

Sets the X-axis range: 0 100 Sets the Y-axis range: 0 100

Fig. 4. Interface scheme configuration.

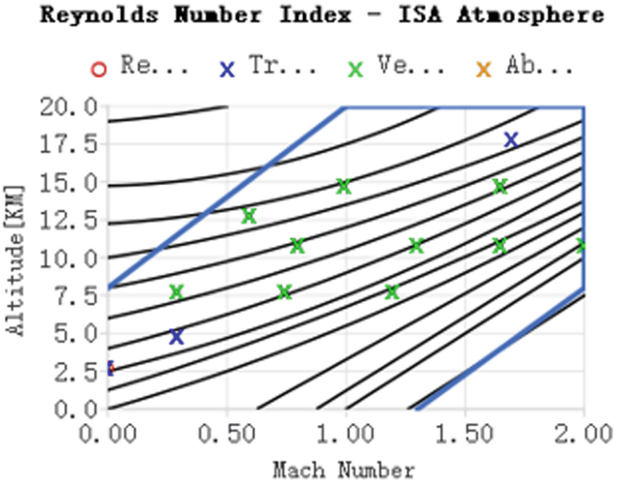


Fig. 5. Test point display.

5 Conclusion

By modeling the real problem as a multi-objective optimization problem under multiple operating conditions, the internal parameters of the model can be well back-calibrated. Aiming at the urgent need and existing bottleneck of model parameter optimization in data enrichment in engine design and application, as well as the problem of large scattering of data enrichment results due to the self-induced uncertainty of data input. A self-optimization algorithm with the objective of minimizing global deviation is carried out by combining multiple input parameters in an uncertain interval. The multi-objective problem is converted into a single objective problem by summing weights, and an adaptive change mechanism of weights is introduced to balance the optimization intensity of each objective. The final algorithm can get the unique solution, which saves the engineers the difficulty of selecting the solution and greatly improves the efficiency of optimization. From the optimization results, it can be seen that the intelligent optimization algorithm based on the adaptive change mechanism has a good application prospect.

References

1. Jia, L., Xu, D., Dakun, S et al.: Response and stabilization of a two-stage axial flow compressor restricted by rotating inlet distortion. Chin. J. Aeronaut., **34**(09), 72–82 (2021)
2. Fanyu, L., Li Jun, X., Dong, et al.: Influence of SPS casing treatment on axial flow compressor subjected to radial pressure distortion. Chin. J. Aeronaut. **30**(02), 685–697 (2017)
3. Sakata, Y. and Ohta, Y.: Coexisting state of surge and rotating stall in a two-stage axial flow compressor using a double-phase-locked averaging technique. J. Therm. Sci., **26**(01), 38–46 (2017)
4. Simon.: Evolutionary optimization algorithms: a bionic and population-based approach to computer intelligence. Tsinghua University Press (2018)

5. Jing, L., Boyao, Z., Dayi, Z., et al.: Current status and prospect of fault diagnosis for aero gas turbine engines. J. Aeronaut. **43**(8), 626565 (2022)
6. Leppmann, H.: Study on the influence of tip clearance on the matching of multistage axial compressor. Tsinghua University (2015)
7. Baojie, L., Chuanhai, Z., Guangfeng, A., et al.: Using tandem blades to break loading limit of highly loaded axial compressors. Chin. J. Aeronaut. **35**(04), 165–175 (2022)
8. Limin, G., Xudong, F., Xuan, C., et al.: Discussion on design method of compressor transition section. J. Aeronaut. **34**(05), 1057–1063 (2013)

AcLGB: A Lightweight DDoS Attack Detection Method

Fantao Zeng[1,2], Jieren Cheng[1,2](✉), Zhuyun Cao[1], Yue Yang[1,2],
and Victor S. Sheng[3]

[1] School of Computer Science and Technology, Hainan University, Haikou 570228, China
cjr22@163.com

[2] Hainan Blockchain Technology Engineering Research Center, Haikou 570228, China

[3] Department of Computer Science, Texas Tech University, TX 79409, USA

Abstract. With the development of Internet technology, distributed denial of service(DDoS) attack has always been a hot and difficult point in network security.Protecting network infrastructure and information security is also becoming more and more important.However, cyber security is an arms race, as attacks develop and network traffic surges, intelligent solutions face the challenge of detecting sensitive changes in traffic characteristics.In this paper, we propose a lightweight Adaptive Clustering-based LightGBM(AcLGB) detection method.This is a new DDoS traffic classification method and an effective lightweight detection method.We introduce a new clustering technique to learn the clustering centers that can be used to extend the characteristics of a given dataset.It solves the challenge of difficult detection when traffic characteristics change sensitively.The model separates the samples of different categories in the best way, and outperforms the current detection method with 99.98% detection accuracy. In the CIC-DDoS2019 data set, the detection time of 802s is better than other detection methods.

Keywords: Network security · DDoS attack · LightGBM · Clustering

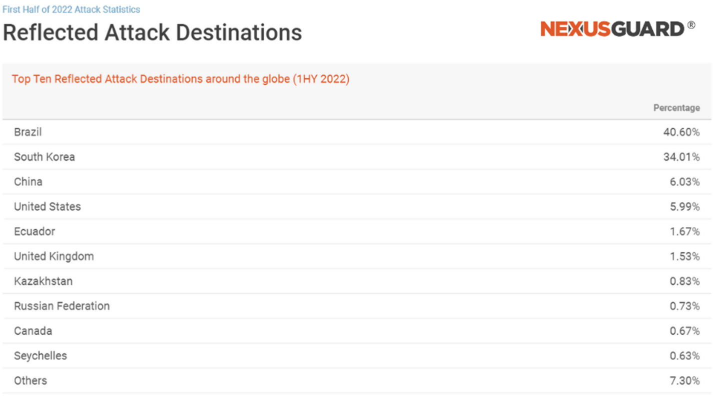
1 Background Introduction

1.1 Background

A distributed denial of service (DDoS) attack involves flooding a target server with traffic, rendering it inoperable. It is different from other attack types. The main purpose of DDoS attacks is not to steal private data, but to degrade the performance of the target server. DDoS attacks are distributed denial-of-service attacks. Multiple clients attack a target server at the same time, rapidly depleting the resources of the target server. Botnets of malware-infected client computers are also a form of DDoS attack.

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 200–212, 2024.
https://doi.org/10.1007/978-981-99-7161-9_16

The most recent massive DDoS attack was a massive attack on GitHub in 2018, which lasted 20 min. GitHub has its own internal security mechanism that blocks attacks when attacked, and it was one of the largest DDoS attacks in the world. In 2022, Google Cloud Armor customers suffered a distributed denial of service (DDoS) attack based on the HTTPS protocol that reached 46 million requests (RPS) per second, the largest attack of its kind ever recorded. In just two minutes, the attack escalated from 100,000RPS to a record 46 million RPS, nearly 80 percent higher than the previous high, and Cloudflare eased an HTTPS DDoS of 26 million RPS in June. The attack began at 09:45 am Pacific time on June 1, initially targeting the victim's HTTP/S load balancer at a rate of 10,000RPS. Within eight minutes, the attack intensified to 100,000RPS, and Google's CloudArmorProtection was activated by generating alerts and signatures based on certain data extracted from traffic analysis. Two minutes later, the attack peaked at 46 million requests per second. Fortunately, the customer had already deployed Cloud Armor's recommendation rules, and the hack did not have the desired effect.From this, we can see that DDoS attacks are not far away from us, and let's look at the consequences of DDoS attacks.


NEXUSGUARD®

First Half of 2022 Attack Statistics

Reflected Attack Destinations

Top Ten Reflected Attack Destinations around the globe (1HY 2022)

	Percentage
Brazil	40.60%
South Korea	34.01%
China	6.03%
United States	5.99%
Ecuador	1.67%
United Kingdom	1.53%
Kazakhstan	0.83%
Russian Federation	0.73%
Canada	0.67%
Seychelles	0.63%
Others	7.30%

Fig. 1. Top ten reflected attack destinations around the globe(1HY 2022)

According to NexusGuard [1] statistics on DDoS attacks in 2022, the total number of attacks and average attack size increased by 75.60 percent and 55.97 percent, respectively, in the first half of 2022 compared to the second half of 2021. Compared to the second half of 2021, the maximum attack size was reduced by 66.82%, and the maximum attack size was 232.00 Gbps. Compared to the same month in five years, March had the fewest number of attacks, while June had the highest number of attacks, the highest number of attacks, and the highest number of attacks. While the number of attacks increased from April 2022 to June 2022, the number of attacks declined during the same period in 2021. Figure 1 shows this.

We summarize the data of DDoS attacks in the following sections.

a. Type of attack media: In the first half of 2022, UDP attack and HTTPS flood were the two attack types, contributing 39.58% and 15.94% respectively, while TCP ACK attack ranked the third with 6.48%.
b. Attacks by category: Volume (direct flood) attacks accounted for 67.93% of total attacks recorded in the first half of 2022, with HoH increasing 48.22% and down 15.06% year-on-year.
c. Protocol attacks: UDP and TCP attacks were the two main attack types in the first half of 2022, accounting for 61.27 and 30.57% respectively.
d. Attack duration: 69.27% of attacks lasted less than 90 min, and the remaining attacks lasted more than 90 min. 17.15% of the attacks lasted more than 1200 min.

From the above data, we can find that the target of DDoS attacks is not only to affect the target website, but also to affect the normal operation of services. The cost of DDoS attacks is relatively low, but large-scale DDoS attacks have a huge impact on services. Because attackers often change the nature of attacks, such sensitive characteristics make it difficult to detect DDoS attacks, and therefore difficult to detect and mitigate the impact of attacks.

1.2 Main Contribution

Despite rapid advances in AI-based DDoS detection methods [11], existing solutions are still very sensitive to small changes in the various characteristics of network traffic. Specifically, because these techniques learn from the characteristics of a single sample, training them on carefully designed features, inadvertently mislabeled samples, or small subsets of unbalanced data sets negatively affects their ability to generalize, thus making it very difficult to detect new DDoS attacks.

Main contribution: We introduce a new clustering technique to learn clustering centers that can be used to extend the characteristics of a given data set.Based on the clustering results, we use the normalization method of softmax to process the data set, which is convenient for lightGBM classifier to conduct classification training. The statistical features and clustering features are joined together, and then LightGBM algorithm is applied to classify the generated new data set.Finally, in order to prove the effectiveness of our solution, we evaluated the effectiveness of the AcLGB algorithm on the network traffic data set of CIC-DDoS2019 [2], and it reached the accuracy of 99.98979% in the detection accuracy. In terms of detection time, 802s is better than the conventional classification model.

2 Related Work

We briefly describe other test methods that are directly related to our test method and highlight their shortcomings.

2.1 DDoS Attack Detection Based On Deep Learning

Most deep learning-based detection methods attempt to match observed network flow with previously learned patterns. Despite increasing adoption rates, they produce unacceptably high false positive rates with relatively little improvement in detection performance. This greatly limits their applicability in real life. Autoencoders (AE) can learn potential representations of features and reduce their dimensions to minimize memory consumption [3–5], which drives their use for abnormal traffic detection. Tan et al. [6] applied convolutional neural networks (CNN) to learn the spatial representation of packets, and then used image classification methods to identify malware traffic. Wang et al. [7] combined CNN with long short-term memory (LSTM) structures to learn the spatial and temporal correlations between features. As effective as these techniques are, they completely ignore the time-based statistical characteristics that can be inferred from the semantic relationships in packets and packet payloads. Min et al. [8] used these ignored attributes and applied natural language processing techniques to process the packet payload. This improves detection performance, but it still has several important weaknesses, including ignoring data set imbalances and showing very high processing times when working with large data sets.

2.2 DDoS Attack Detection Based On Machine Learning

Machine learning refers to the analysis of large amounts of data by machines and the automatic learning of rules and patterns in the data, so as to achieve automatic decision-making and control. In the field of DDoS attack detection, many scholars carry out researches. Dong et al. [9] proposed the improved KNN (K-Neighbors), which mainly focuses on adding a weight to the predicted samples. The weight can make the samples that are closer to the predicted samples contribute more to the model, and the algorithm can perform better in some specific distributions. Due to the defects of KNN itself, its efficiency in processing large samples will be insufficient. Li et al. [10] proposed a method of feature dimension reduction, which extracted 19-dimensional features from high-dimensional network traffic and classified network traffic by combining clustering and support vector machine (SVM) algorithm. In the field of machine learning, feature selection is often decided by humans. Once the feature selection is insufficient, the training effect will be poor.

3 System Architecture

A lightweight AcLGB detection method based on LightGBM.

We propose a lightweight DDoS attack detection method based on LightGBM, which can maximize the detection efficiency of the model and reduce the detection time. At the same time, multi-core cluster balancing detection performance is introduced to ensure that the detection accuracy is not lost. It not only reduces the false alarm rate, but also improves the detection efficiency.

Feature extractor module: converts raw network packets into headers and statistical feature vectors.

Adaptive clustering module: low dimensional embedding of network flow features is constructed, and abstract attributes shared by a group of samples belonging to the same traffic type are calculated.

Classification module: statistical features and clustering features are connected together, and then LihgtGBM algorithm is applied to classify the generated new data set.

In the following sections, we describe in detail the specific operations of each module and its related role in detecting DDoS attacks.

3.1 Feature Extractor Module

By processing the data features of the original data set, AcLGB extracts more representative representation information from it to represent the data, which is embodied in: deleting null and 0 values; Remove useless features including "Flow ID", "Source IP", "Unnamed: 0", etc. By reducing useless features and reducing the training pressure of classifiers, the performance of clustering modules and classifiers can be effectively improved, and the training reasoning time of AcLGB can be greatly reduced.

3.2 Adaptive Clustering Module

Although the training speed of LightGBM is very fast and the memory usage is very small, it is sensitive to the interference effect of noisy data. We need to organize the data input effectively to reduce the impact of data on the classification module. We propose a new model, AcLGB, which is based on a clustering algorithm that generates clustering centers to be used as extensions of the input features to be clustered. Because our adaptive clustering method is designed to be end-to-end differentiable, the training is performed on small batches by which the network learns the low-dimensional representation of the input and computes the corresponding kernel center. This operation is performed online iteratively, with the probability that the last layer of the kernel network produces each sample among inputs belonging to all possible classes.

The clustering algorithm is to learn the similarity content of the data set to group similar samples together. Through this process, the data is effectively organized. By proposing multiple kernel clustering networks, each network may learn one of the required classification clusters, and we use encoders to reduce the original network traffic dimension to any required dimension. As shown in the Fig. 2, we can use the encoder to reduce the dimensionality of the input features to the desired feature dimension.

Let Kc be the set of features obtained from the cluster center of a given class C. For any two samples i, j ∈ C.

$$\text{distance }\ (\chi_i \cup K_c, \chi_j \cup K_c) \leq \text{ distance }\ (\chi_i, \chi_j) \tag{1}$$

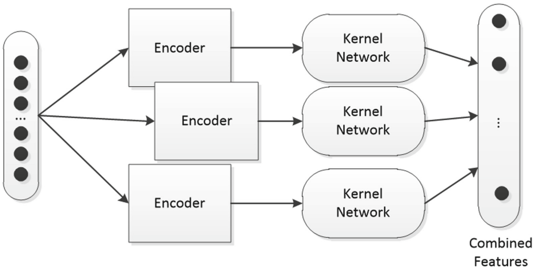


Fig. 2. Multiple kernel clustering process

Let i and j be n-dimensional real-valued vectors:

$$\chi_i = \{x_{i1}, x_{i2}, \ldots, x_{in}\} \in \mathbb{R}^n \quad \chi_j = \{x_{j1}, x_{j2}, \ldots, x_{jn}\} \in \mathbb{R}^n \tag{2}$$

When Xit and Xjt correspond to each feature of the sample data, t belongs to [0, n], assuming that xi and xj are both C-class data, it is clear that we can obtain the CTH cluster center Kc:

$$K_c = \{k_{c1}, k_{c2}, \ldots, k_{cm}\} \in \mathbb{R}^m \tag{3}$$

Finally we obtain the aggregated features:

$$\chi_i' = \{x_{i1}, x_{i2}, \ldots, x_{in}, k_{c1}, k_{c2}, \ldots, k_{cm}\} \in \mathbb{R}^{n+m} \tag{4}$$

$$\chi_j' = \{x_{j1}, x_{j2}, \ldots, x_{jn}, k_{c1}, k_{c2}, \ldots, k_{cm}\} \in \mathbb{R}^{n+m} \tag{5}$$

An intuitive way for us to calculate the clustering effect is to compare the similarity between the original and aggregated feature vectors, namely Q1 and Q2,

$$Q_1 = \text{distance}\left(\chi_i, \chi_j\right) \text{ and } Q_2 = \text{ distance } \left(\chi_i', \chi_j'\right)$$

$$Q_1 = \frac{1}{n} \sum_{\alpha=1}^{n} \left(x_{i\alpha} - x_{j\alpha}\right)^2 \tag{6}$$

$$Q_2 = \frac{1}{n+m} \left(\sum_{\alpha=1}^{n} \left(x_{i\alpha} - x_{j\alpha}\right)^2 + \sum_{\alpha=1}^{m} \left(k_{c\alpha} - k_{c\alpha}\right)^2 \right) \tag{7}$$

$$Q_2 = \frac{1}{n+m} \sum_{\alpha=1}^{n} \left(x_{i\alpha} - x_{j\alpha}\right)^2 \tag{8}$$

$$Q_1 - Q_2 = \frac{m}{n+m} \cdot Q_1 \Rightarrow Q_2 = \beta \cdot Q_1 \tag{9}$$

3.3 Classification Module

Finally, AcLGB uses classification module to process the combined extraction features and clustering center of each sample, and outputs the inferred traffic class to which the flow belongs. The training classification is carried out by LightGBM. 70% of the data set is taken as the training set and 30% is taken as the verification set to judge and classify the input data. LightGBM is a classification algorithm based on decision tree. First, it is a decision tree algorithm based on Histogram. It discretized continuous floating point feature values into k integers, constructs histogram with width of k, and performs statistics in the histogram according to discretized values as indexes. Then, according to the discrete value of the histogram, the optimal segmentation point is found by traversing. LightGBM conducts difference acceleration based on Histogram algorithm. Secondly, LightGBM adopts a growth strategy based on the leaf-wise algorithm with depth limitation. This strategy finds the Leaf with the largest splitting gain from all current leaves each time, and then splits, and so on. On this basis, the maximum depth limit is added to prevent overfitting on the basis of ensuring high efficiency.

Compared with traditional XGBoost, LightGBM has the advantages of faster speed and smaller memory, so we choose this classification algorithm as the design of our classification module.

3.4 AcLGB Detection Procedure

Lightgbm-based lightweight attack detection method mainly uses LightGBM's lightweight detection model to improve the overall detection speed and ensure the memory overhead, and reduces the impact of noise data in the data set on the training process through multi-core clustering to ensure the overall robustness. As shown in the Fig. 3, the specific process is as follows:

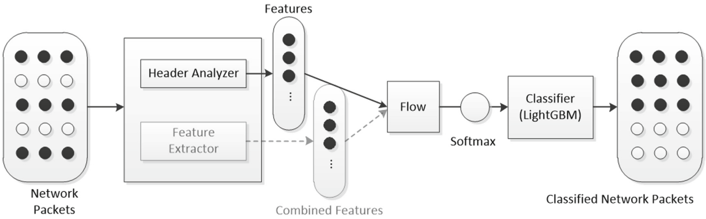


Fig. 3. AcLGB detection procedure

Step 1 AcLGB processes very large volumes of traffic by processing the raw network packet stream into a feature-based bidirectional stream representation.

Step 2 AcLGB is based on the clustering method. We extract a series of features from the original data packet and extend these features using the learned clustering center.

Step 3 AcLGB uses softmax normalization method to process the input training data.

Step 4 AcLGB uses LightGBM classifier to detect DDoS attacks.

4 Specific Experiments

In this section, we introduce the specific process of the experiment.

4.1 Dataset

We evaluate the performance of our method on CIC-DDoS2019 dataset. CIC-DDoS2019 contains benign, up-to-date common DDoS attacks that resemble real real-world data. It also includes the results of network traffic analysis. Using CICFlowMeter-V3, streams are marked according to timestamp, source and destination ip, source and destination port, protocol, and attack. It is collected by the Canadian Network Security Laboratory on January 12, 2019 and March 11, 2019. The total data set is 28.9GB. The data set contains a variety of DDoS attack classification labels. Make an experimental comparison. Finally, we split the preprocessed dataset into a training set and a test set with a ratio of 70 and 30%.

4.2 Preprocessing

Through Fig. 4, we can see that there are many data features that are useless for our model training, so we remove null and zero values; Remove useless features, including “Flow ID”, “Source IP”, “Unnamed: 0”, etc. By reducing useless features and reducing the training pressure of the classifier, the performance of the clustering module and classifier can be effectively improved, and we greatly reduce the training inference time of AcLGB.

4.3 Experimental Parameter Selection

We implemented AcLGB in Python 3.7 using PyTorch [16] and LightGBM libraries. For the AcLGB algorithm, we adopted a set of fully connected NN encoders with 3 hidden layers containing 500, 200 and 50 neurons, respectively. The number of neurons in the output layer is equal to the required dimension of the kernel, which we set to 10 in our experiments with e^{-4} as the training learning rate. We use the classification algorithm of LightGBM as our classifier, and the parameters of LightGBM are shown in Table 1.

Next we evaluate the results of the overall DDoS attack detection, where AcLGB extrapolates meaningful low-dimensional representations from headers and statistical features extracted from raw network traffic data. Using these automatically learned features, we determine different cluster centers and use them to expand the title and statistical properties. With these additional features, we expect our classifier to be more accurate and to easily distinguish even the most

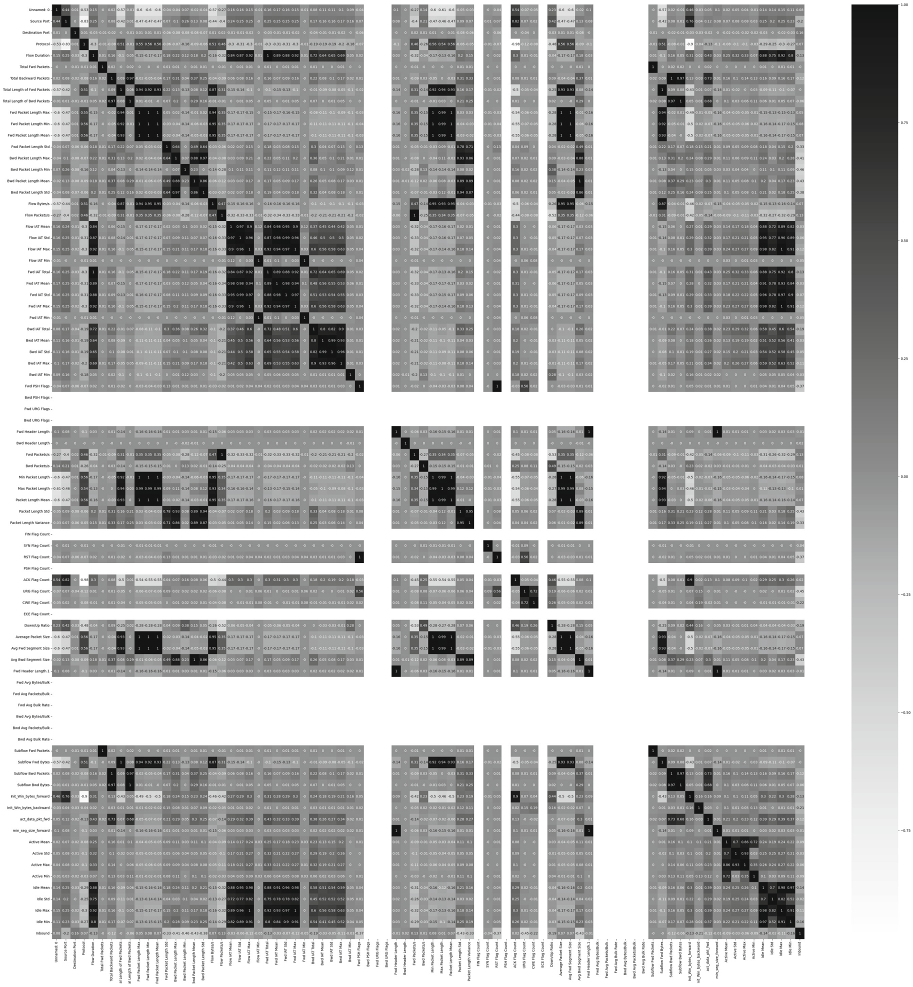
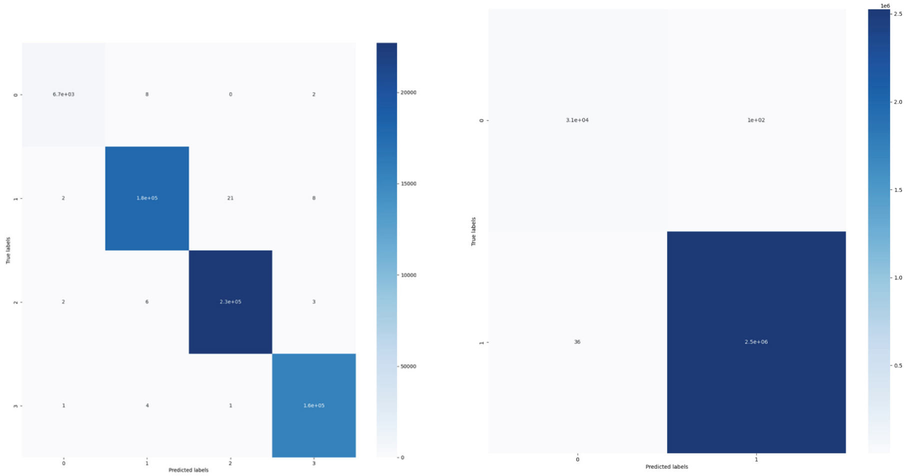


Fig. 4. Feature correlation graph

Table 1. Hyperparameter selection of LightGBM

Parameters	Default values	Meaning
boosting_type	gbdt	Set the promotion type
num_leaves	31	Number of leaf nodes
learning_rate	0.1	Learning rate
feature_fraction	0.9	Feature selection ratio
begging_fraction	0.7	Sample sampling ratio
begging_freq	5	Iterative execution cycle

similar patterns. To verify our hypothesis, we perform multi-label classification on the above CIC-DDoS2019 real dataset, as shown in Fig. 5a. Therein we distinguish between benign and malicious traffic and identify the type of each traffic separately. And do the binary classification experiment without using multiple kernel clustering to process the data, as shown in Fig. 5b.



(a) 4 Classification results

(b) 2 Classification results

Fig. 5. Confusion matrix results

Table 2. Confusion matrix in classification task

	Actual positive	Actual negative
Predicted positive	TP	FP
Predicted negative	FN	TN

4.4 Evaluation Metrics

To measure the performance of our AcLGB, we use the held out testing set to compute confusion matrices, based on which we calculate the number of True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) inferences. The details are given in Table 2. With these, we derive a number of metrics that allow us to assess the quality of the classification results of AcLGB and those produced by the benchmarks considered, namely:

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN} \tag{10}$$

$$\text{Precision} = \frac{TP}{TP + FP} \tag{11}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{12}$$

$$\text{FAR} = \frac{FP}{FP + TN} \tag{13}$$

$$\mathbf{F_1 score} = 2 \cdot \frac{\text{Precision*Recall}}{\text{Precision+Recall}} \tag{14}$$

In the CIC-DDoS2019 real dataset, we also calculated the accuracy, precision, recall, F1 score of AcLGB, which is similar to a two-stage classification process, where the first stage corresponds to classifying DDoS traffic by clustering. The second stage corrects misclassified samples by a further LightGBM classifier. Finally, we compare the experimental performance of different methods on CIC-DDoS2019 dataset in Table 3, We can find that our method has a detection accuracy of 99.98%, a Recall value of 99.71% and a F1 score of 99.55%, which is much higher than other detection methods.

Table 3. Performance comparison of different methods on CIC-DDoS2019 dataset

Thesis	Methods	Accuracy	Precision	Recall	F1 score	Training time
De Assis MOV [12]	CNN+LSTM	96.34	95.71	95.49	95.60	1077
Javaid A [13]	Regression	95.59	95.41	95.95	95.53	1245
Sadaf K [14]	Isolasion Forest	91.49	90.28	90.74	90.51	1377
Wei Y [15]	AE+MLP	97.76	97.74	97.63	97.68	1127
AE-XGBoost	AE+XGBoost	98.92	98.96	98.94	98.95	1745
Our	AcLGB	99.98	99.38	99.71	99.55	802

5 Conclusion and Prospect

Based on LightGBM, this paper proposes a lightweight DDoS attack detection method AcLGB, which can maximize the detection efficiency of the model and reduce the detection time. At the same time, multi-core clustering is introduced to balance the detection performance and ensure that the detection accuracy is not lost. It not only reduces the false positive rate, but also improves the detection efficiency. We verify the effectiveness of our method through experiments on

CIC-DDoS2019 dataset, which can be deployed on devices with limited computing resources. At present, the abnormal flow of this data set is much higher than the normal flow. In the future, the data set with more balanced distribution can be found to verify the method.

This work was supported by National Natural Science Foundation of China (NSFC) (Grant No. 62162022, 62162024), the Key Research and Development Program of Hainan Province (Grant No. ZDYF2020040, ZDYF2021GXJS003),the Major science and technology project of Hainan Province (Grant No. ZDKJ2020012), Hainan Provincial Natural Science Foundation of China (Grant No. 620MS021, 621QN211), Science and Technology Development Center of the Ministry of Education Industry-university-Research Innovation Fund(2021JQR017), Innovative research project for Graduate students in Hainan Province (Grant No. Qhyb2022-93). Supported by the Key Laboratory of PK System Technologies Research of Hainan.

References

1. "NexusGuard" [online] Available: https://www.netscout.com/
2. "CIC-DDoS2019" [online] Available: https://www.unb.ca/cic/datasets/ddos-2019.html
3. Yu, Y., Long, J., Cai, Z.: Session-based network intrusion detection using a deep learning architecture. In: International Conference on Modeling Decisions for Artificial Intelligence, pp. 144–155 (2017)
4. Yu, Y., Long, J., Cai, Z.: Network intrusion detection through stacking dilated convolutional autoencoders. In: Security and Communication Networks, pp. 1–10 (2017)
5. Yousefi-Azar, M., Varadharajan, V., Hamey, L., Tupakula, U.: Autoencoder-based feature learning for cyber security applications. In: IEEE International Joint Conference on Neural Networks, pp. 3854–3861 (2017)
6. Tan, Z., Jamdagni, A., He, X., Nanda, P., Liu, R., Hu, J.: Detection of denial-of-service attacks based on computer vision techniques. IEEE Trans. Comput. **64**(9), 2519–2533 (2014)
7. Wang, W., Sheng, Y., Wang, J., Zeng, X., Ye, X., Huang, Y., et al.: HAST-IDS: Learning Hierarchical Spatial-Temporal Features using Deep Neural Networks to Improve Intrusion Detection (2017)
8. Min, E., Long, J., Liu, Q., Cui, J., Chen, W.: TR-IDS: anomaly-based intrusion detection through text-convolutional neural network and random forest. In: Security and Communication Networks, pp. 1–9 (2018)
9. Dong, S., Sarem, M.: DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks. **8**, 5039–5048 (2018)
10. Li, Y., Xia, J., Zhang, S., et al.: An efficient intrusion detection system based on support vector machines and gradually feature removal method. Expert Syst. Appl. **39**(1), 424–430 (2012)
11. Cui, J., Zhang, Y., Cai, Z., Liu, A., Li, Y.: Secure-display path for security-sensitive applications on mobile. Comput. Mater. Continua **55**(1), 17–35 (2018)
12. de Assis, M.V.O., Carvalho, L.F., Rodrigues, J.J.P.C., et al.: Near real-time security system applied to SDN environments in IoT networks using convolutional neural network. Comput. Electr. Eng. **86**, 106738 (2020)

13. Javaid, A., Niyaz, Q., Sun, W., et al.: A deep learning approach for network intrusion detection system. Eai Endorsed Trans. Secur. Saf. **3**(9), 2 (2016)
14. Sadaf, K., Sultana, J.: Intrusion detection based on autoencoder and isolation Forest in fog computing. **8**, 167059–167068 (2020)
15. Wei, Y., Jang-Jaccard, J., Sabrina, F., et al.: AE-MLP: a hybrid deep learning approach for DDoS detection and classification. IEEE **9**, 146810–146821 (2021)
16. "PyTorch", [online] Available: https://pytorch.org/

Prediction of Passenger Flow During Peak Hours Based on Deep Learning

Yajing Li[1](✉), Jieren Cheng[1,2], Yuqing Kou[1], Dongwan Xia[1],
and Victor S. Sheng[3]

[1] School of Computer Science and Technology, Hainan University, Haikou 570228, China
2469120165@qq.com

[2] Hainan Blockchain Technology Engineering Research Center, Haikou 570228, China

[3] Department of Computer Science, Texas Tech University, Lubbock, TX 79409, USA

Abstract. In many deep learning tasks, feature extraction and fusion in multivariate time series is an indispensable part of passenger flow prediction. Because there is also a certain correlation between passenger flow time series, it is very meaningful to successfully capture the time characteristics of the series and the dependencies between each series. Therefore, this study combined Residual Network (ResNet) and Attention Gated Recurrent Unit (Attention GRU) to build a ResGRU model for predicting subway passenger flow data during peak hours. This study has improved ResNet and attention GRU, then designed the ResGRU model architecture. Among them, the subway network topology is constructed by graphs, ResNet is used to capture the hidden spatial features between data, attention GRU captures the deep temporal features between data. This study not only considered passenger flow data, but also added subway network topology data, even weather and air pollution index data. Finally, three time solts of 10, 15 and 30 min were used to forecast the peak passenger flow on the public dataset. The ResGRU model was compared with the single model, the combined model and an ablation experiment. The experimental results demonstrate the high robustness and superiority of the model.

Keywords: Deep learning · Residual network · Gated Recurrent unit · Prediction passenger flow

1 Introduction

The transportation system is one of the most important constructions in a modern city, which is maintaining the normal travel of different groups of people. In the development of intelligent transportation system (ITS), through the consumption record of transportation toll system, traffic video monitoring and the detection of the positioning system of smartphones, those can monitor the

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 213–228, 2024.
https://doi.org/10.1007/978-981-99-7161-9_17

dynamic changes of traffic in real time. That helps the traffic management department formulate scientific and reasonable management strategies to avoid sudden traffic problems [1]. As an integral part of ITS, traffic flow forecasting comprehensively considers historical traffic state data and other factors what may affect traffic state. It can timely notice potential traffic changes for a period of time in the future, which will improve the stability of the traffic system [2]. Traffic flow is predicted based on the traffic pattern in the past period of time, the various traffic factors in the same period of time have an impact on the future traffic volume [3].

At present, the subway is becoming the preferred way of people's daily travel. During the peak hours of weekdays, serious congestion often occurs at subway stations. Compared with other traffic passenger flows, the subway passenger flow is more cyclical, the passenger flow in the morning and evening peak periods shows a certain pattern. In order to relieve traffic pressure, in the meantime speeding up subway route design and urban network planning, research on subway passenger flow forecasting during peak periods is worthy of attention. Accurate and timely passenger flow forecasting methods will support plan individual routes in advance and reduce commuting stress, even avoid accidents such as stampedes. In previous work, traffic flow prediction involves multiple modes of travel, but they don't take into account external factors for instance traffic routes, weather conditions, air quality, and holidays.

With the development of machine learning, a number of machine learning models and hybrid prediction models have emerged for passenger flow forecasting, such as back-propagation neural network (BPNN), random forest learning and support vector machine (SVM) models. However, these methods only make predictions based on the passenger flow time series data, without considering the topology of the transportation network. Their improved prediction accuracy is also limited.

Deep neural networks have achieved remarkable results in the field of traffic flow forecasting. Short-term and long-term forecasting of traffic flow in traffic applications have attracted more researchers, most of whom focus on constructing new models for forecasting. Because of the multi-dimensional traffic data information which involves a variety of dynamic data in some emergencies, the traffic time series data prediction problem is more challenging than the prediction problems in other application fields. Although many deep learning models have been proposed in this field, a majority of the models are constructed based on specific datasets, the generalization ability of the models is weak. When using new datasets for prediction research, the model prediction performance degrades. Moreover, the deep learning model still has some defects, for instance the inability to reflect the advanced prediction performance when the raw data is small, the inexplicability of the model itself.

Under this premise, this study combines ResNet and Attention GRU to construct a "ResGRU" model, so that make short-term prediction of subway passenger flow during peak hours. The model not only considers the dynamic temporal and spatial characteristics between subway stations, but also adds a weather index to more comprehensively predict the subway passenger flow law in the short term. It can be seen from the ablation experiments of the ResGRU model, although the prediction results are not much different, the model prediction accuracy is improved after adding the subway network topology and weather and air pollution indices. The rest of this paper is described as follows. In Sect. 2, the existing work related to traffic flow prediction is depicted. In Sect. 3, the design architecture of ResNet, Attention GRU and ResGRU models are introduced. In Sect. 4, the experimental dataset and related evaluation metrics are discussed, comparative experiments are carried out on the model to prove the effectiveness of the model. Finally, it is concluded in Sect. 5.

2 Related Work

After decades of research, the development of the field of traffic flow prediction is now in the fourth generation of deep neural networks (the application of graph convolutional networks) . However, it is still the third generation of technology (the fusion of CNN and RNN) is extensively used [4]. Among the classical statistical models, the ARIMA model is relatively widely used in the field of traffic forecasting. Jie et al. [5] employed ARIMA and various external covariates to predict the daily passenger flow of the Taipei Metro. In [6], the ARIMA model is used to detect the stationarity of the data set, in which the data with large fluctuations are subjected to differential processing. Run et al. [7] coupled with ARIMA and gray prediction model, then selected the data of each subway entrance in a city to predict subway passenger flow. However, the classical statistical models also have certain shortcomings. The nonlinear characteristics of the data are ignored, more importantly the model must manipulate relatively stable data.

In deep learning, CNN can capture the dynamic dependencies of spatial regions of traffic and passenger flow data, RNN is more sensitive to perceive the temporal information features of traffic and passenger flow data. The continuous improvement of deep learning algorithms has led to significant improvements in traffic flow prediction performance. Bai et al. [8] pointed out that learning node-specific patterns is crucial for understanding related time series data. In [9] adopting online learning (OL) technology, the advantages of transport and online learning in traffic flow forecasting are clarified. In [10], a set of heuristic indicators was proposed. Provide traffic managers with a more informative decision-making process through the integration of index information. Shen et al. [11] pointed out that most of the existing works use time series analysis to study urban rail transit passenger forecasting. Fafoutellis et al. [12] combined extended recurrent neural network(RNN) and long short-term memory network (LSTM) for traffic prediction, they used network-wide data for traffic condition prediction, but did not meditate the high dimensionality of the data. Zhao et al. [13] introduced a memory time series network to solve the urban traffic forecasting problem, while the forecasting effect was not ideal when dealing with complex data features. Shih et al. [14] deal with related time series through filters and an improved attention mechanism, though the model will lose some data features in long-term prediction. Based on long-range Transformers, Grigsby et al. [15] recover the relations required to achieve competitive performance in prediction tasks, yet the model performance gains are not high. Zhao et al. [16] combined a graph evolution network and a bidirectional long-short-term memory network with an attention mechanism. Although complex topological spatial features and dynamic temporal features were extracted from temporal and spatial traffic data, the model prediction performance was unstable.

Nowdays, in the field of road traffic prediction, researchers have also begun to apply residual neural networks, such as taxi flow [17], traffic flow [18,19] and traffic state [20] prediction. As far as current research is concerned, the application of ResNet in traffic passenger flow prediction is relatively less, prediction performance has not been better achieved. Long short-term memory networks have achieved some results in time series prediction. Gated recurrent units (GRU) and LSTM both contain gating mechanisms, while GRU uses hidden states to transmit information. It is generally faster to train than LSTM.GRU has already carried out relevant experiments in power anomaly forecasting [21], wind power forecasting [22] and stock forecasting [23], but the research in the field of traffic passenger flow forecasting is still comparatively lacking. Liu et al. [24] effectively learned dynamic spatiotemporal features via ConvLSTM units. Wu et al. [25] captured both temporal and spatial dependencies in traffic flow data, what gets by extracting external knowledge such as relationships between variables and variable attributes. In [26] established a new multi-step traffic prediction model that dynamically captures the spatial correlation of traffic data. While these models can capture traffic data spatial dependencies, they do not take into account for other traffic external factors, for instance weather conditions, air quality, or traffic accidents. When bad weather or poor air quality occur, people may adjust their travel patterns even postpone their trips. Therefore, these external factors are also crucial in predicting the outcome.

In conclusion, although some researchers have paid attention to the topology information of traffic network in recent years, they have not make much of other external factors in traffic. In the field of traffic passenger flow prediction, in addition to traffic factors, other external factors also have a certain impact on passenger flow. Therefore, the proposed model can not only capture the dynamic temporal and spatial characteristics between subway stations, but also incorporate weather and air pollution index-related data to improve the performance of subway passenger flow prediction.

3 Methodology

Our model was built by ResNet and attention GRU. Next, we will introduce the components and ResGRU model architecture respectively.

3.1 Residual Network

Previous studies have pointed out that models with more layers in the network can capture more hidden features. However, deeper models are not always more effective due to vanishing or exploding gradients. Residual network solves the problem of gradient disappearance or explosion caused by increasing depth in deep neural network through shortcut connection. This study adopts an improved residual block, which contains 32 filters, as shown in Fig. 1. The residual network is mainly used to train the network output, as follows:

$$X_{l+1} = F\left(X_1\right) + X_l \tag{1}$$

where X_l and X_{l+1} represent the residual block input and output. In the residual block, "Conv" represents the convolutional layer, "BN" represents the batch normalization layer, "ReLU" represents the activation layer. Among them, convolution is to extract features from data, the purpose of activation is to reduce the dimension of feature maps, but important information is not discarded.

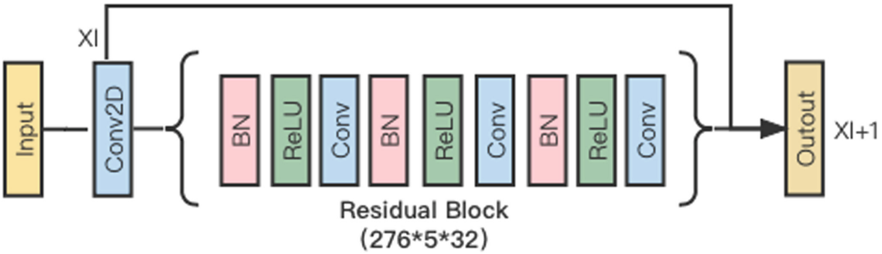


Fig. 1. Improved residual block

3.2 Attention GRU

RNN broadly adopts long short-term memory networks and gated recurrent units to solve the facing vanishing/exploding gradient problem. Attention mechanism in the fields of image recognition and natural language processing, what has extended sufficiently novel improvements and contributions. The related research in the field of traffic prediction still needs to be further developed. Therefore, in order to obtain different weights of features in different network layers, this study adds attention GRU to the model. Different from traditional weight assignment rules, since other factors for example weather conditions, network topology, and working days have a certain influence on subway passenger flow, instead of assigning weights based on timesteps, this study automatically scores in the model via the weights captured by the GRU.

The matrix output after GRU processing is $D\epsilon R_{a\times b}$,where a and b represent each time step and the number of features. D represents the output from the attention layer, which is obtained by

$$I = F(W \circ D + b) \tag{2}$$

$$D' = I \circ D \tag{3}$$

where I is the weight matrix of the same shape as D, "∘" represents the Hadamard product, F represents the fully connected layer (which can be activated by the RELU activation function), W is the weight matrix of F, b is the bias.

3.3 ResGRU Model Architecture

Our model architecture is shown in Fig. 2, it consists of two major modules, a feature extraction module and a feature fusion module. In the feature extraction module, the corresponding processing is carried out according to the input data category. The data are mainly divided into three types, passenger flow data, network topology data and weather and air pollution index.

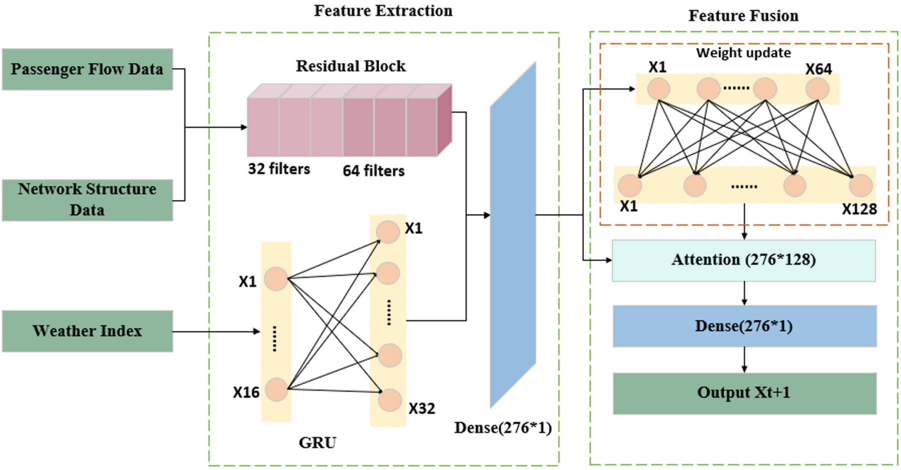


Fig. 2. ResGRU model architecture

Passenger Flow Data Historical passenger flow data is the most important for predicting short-term passenger flow. Moreover, the station location is fixed in the subway station network, the correlation between incoming and outgoing passenger flow is small. Treating incoming and outgoing passenger flow data separately does not affect the prediction accuracy of the model, while it could increase the model running speed. Therefore, this study divides the passenger flow data into inflow data and outflow data.

The subway management system stores the real-time passenger flow data of subway stations, this study has adopted three inflow modes based on the collected data: real-time, daily and weekly modes. In order to predict the passenger flow data of t+1, the passenger flow data of the three modes from t–4 to t are respectively input into different channels. The passenger flow data input is given by

$$K_1 = (X^r_{(m,t)}, X^d_{(m,t)}, X^w_{(m,t)}) \tag{4}$$

where X_r, X_d and X_w represent the passenger flow data corresponding to the current day, the previous day or the previous week, m represents the number of subway stations, adjacent stations are located in adjacent rows according to the train route, t represents the historical time step of the station .

The passenger flow data was fed into residual blocks containing 32 and 64 filters successively, then the data was flattened and fully connected with 276 neurons. The final output passenger flow will be input to the feature fusion module.

Network Topology Data In the field of traffic and passenger flow prediction, the addition of the subway network topology greatly improves the prediction accuracy. In this study, this study uses the residual network to obtain the weights of the subway network topology data as to the subway line and station composition. Since the subway network topology cannot be changed on the basis of the subway line construction, thus this study only needs to consider the real-time mode. The other processing methods are the same as the passenger flow data, the input of network topology data is

$$K_2 = \widehat{D}^{-\frac{1}{2}}\widehat{A}\widehat{D}^{-\frac{1}{2}}(X^r_{m,t}) \tag{5}$$

Weather and Air Pollution Index Till now, some studies have begun to attach importance to the influence of weather on traffic passenger flow forecasting, but the impact of air quality on traffic passenger flow forecasting has not been fully explored. When the weather is bad or the air is polluted, people will adjust their travel plans and travel patterns. Therefore, this study incorporates weather and air quality forecasts for subway passenger flow. When making related predictions in different time solt (TS), his study would select the weather and air pollution index data in the same time period during recent days. The input of weather-related data is given by the following formula:

$$K_3 = (X_{(n,t-i)}, X_{(n,t)}) \tag{6}$$

where K_3 is a two-dimensional matrix containing n rows and i columns, where n is the number of weather correlation coefficients and i is the time step.

After the weather and air pollution index related data is input, the data is first flattened and then fed into the fully connected layer to obtain the current weighted index. Next it goes through two layers of GRU with stacks of 16 and 32 neurons. Finally the processed data will be input to the feature fusion module.

Feature Fusion Module The data output by the feature extraction module enters the feature fusion module, during which the weight vector is randomly initialized compliance with the corresponding function before training, then it will continuously updated during backpropagation. After the data information features are fused, the data first passes through two GRU layers, the weights captured by the GRU are automatically scored in the model, the weight vector is continuously updated. It is then flattened after the attention layer, finally it would into a fully connected layer consisting of 276 neurons to output short-term passenger flow predictions. This study stipulates that the data format of each branch output is the same, the feature fusion is performed according to the following formula

$$Z = W_1 \circ D_1 + W_2 \circ D_2 + W_3 \circ D_3 \tag{7}$$

Among them, W is the weight vector of the degree of influence of different captured features on the prediction result. D_1,D_2, and D_3 represent the three kinds of data output by the feature extraction module. W has the same specification as the output, and Z represents the data after feature fusion.

4 Experiments

4.1 Dataset Description

The peak subway passenger flow data used in this study is from the Beijing Metro Public Data Set from February 29 to April 3. This study applies only 25 weekday peak passenger flow data, what covers 17 lines and 276 subway stations. Only 3 hrs are selected for each peak period, the morning peak period is 7:30–10:30, the evening peak period is 18:00–21:00. Each record contains the card number, entrance station number, exit station number, entry Outbound Time, Outbound Time, Outbound Outbound Name and Outbound Name. This study uses TSs of 10, 15 and 30 min, then it compares the prediction performance of different TSs depending on the evaluation metrics.

The weather and air pollution index includes 11 indicators, including real-time temperature, dew point temperature, relative humidity , wind speed and real-time air quality index (AQI), atmospheric particulate matter (PM2.5 and PM10) and air pollutants (SO_2,NO_2, CO and O_3), of which the weather data was documented every half an hour once. Air Pollution Index was charted every hour.

4.2 Model Settings

In this study, conducted with TensorFlow and Keras, this study used the first 20 days of peak passenger flow data to train the model and the last 5 days of data for testing. This study sets a validation split rate of 0.2 to tune the model, the optimization function is "Adam", the learning rate is 0.001. This study repeatedly adjusts the model network time step to find the optimal prediction time step, hoping to improve the operation efficiency while ensuring the prediction accuracy. Inside the model, the two residual blocks contain 32 and 64 filters respectively, the convolution kernel size is 3*3, the two-layer GRU consists of 16 and 32 neurons. The attention GRU consists of 64 and 128 neurons, the fully connected layer consists of 276 neurons.

4.3 Evaluation Indicators

The mean squared error (MSE) was used as the loss function in this study. To better evaluate the performance of this model and other methods, four metrics are used to quantify model performance: mean-absolute error (MAE), weighted mean-absolute percent error (WMAPE), accuracy (ACC) and coefficient of determination (R^2). Among them, the smaller the MAE and WMAPE values, the better the prediction effect. On the contrary, the larger the ACC value, the better the prediction effect. R^2 calculates the correlation coefficient, which measures the fitting ability of the prediction result to represent the actual data. The larger the value, the better the prediction effect.

They are given by:

$$Loss = MSE = \frac{1}{n}\sum_{i=1}^{n}(Y_t - \widehat{Y}_t)^2 \tag{8}$$

$$MAE = \frac{1}{n}\sum_{i=1}^{n}\left|Y_t - \widehat{Y}_t\right| \tag{9}$$

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(Y_t - \widehat{Y}_t)^2} \tag{10}$$

$$WMAPE = \sum_{i=1}^{n}\left(\frac{Y_t}{\sum_{j=1}^{n} Y_t}\left|\frac{Y_t - \widehat{Y}_t}{Y_t}\right|\right) \tag{11}$$

$$ACC = 1 - \frac{\left\|Y_t - \widehat{Y}_t\right\|}{\|Y_t\|} \tag{12}$$

$$R^2 = 1 - \frac{\sum_{i=1}^{n}(Y_t - \widehat{Y}_t)^2}{\sum_{i=1}^{n}(Y_t - \overline{Y})^2} \tag{13}$$

where Y_t is the actual value, $\hat{Y}_t$ is the predicted value, n is the number of samples, and $\sum_{i=1}^{n} Y_t$ is the sum of the actual values.

4.4 Comparing Models

This study compares ResGRU with single-model LSTM and GRU, combined model ResLSTM and employ an ablation study. These models all use the ResGRU architecture, only a few changes have been made inside the models. The models are described in detail as follows:

- LSTM: The data processing module uses two layers of LSTM with 16 and 32 neurons respectively, the data fusion module includes two layers of LSTM with 64 and 128 neurons.
- GRU: The data processing module has two layers of GRU containing 16 and 32 neurons respectively, the data fusion module has two layers of GRU with 64 and 128 neurons.
- GCN-No w: Input only passenger flow and network topology data, the data processing module has two layers of GCN, including 16 and 32 neurons respectively, and the data fusion module has two layers of GCN with 64 and 128 neurons.
- TGCN-No w: Input only passenger flow and network topology data, the data processing module adopts two layers including 32 and 64 GCNs, and the data fusion module adds a GRU layer containing 128 neurons.
- GCN: Add weather related data based on GCN-No w.
- TGCN: Add weather related data on the basis of TGCN-No w.
- ResLSTM: The data processing module uses two layers of residual blocks with 32 and 64 filters, the data fusion module adds an LSTM layer with 128 neurons.
- ResGRU-128: The GRU layers used by the data fusion module employ 128 and 276 neurons.
- ResGRU-No G: The network topology data is removed based on the ResGRU model.
- ResGRU-No w: Weather and air pollution index data were removed from the ResGRU model.

Table 1. The prediction results of each model

TS	10 min			15 min			30 min		
Indicators	MAE	WMAPE	ACC	MAE	WMAPE	ACC	MAE	WMAPE	ACC
GRU	21.534	8.38%	90.95%	27.975	7.32%	91.83%	40.324	5.25%	93.97%
LSTM	21.099	8.21%	90.88%	26.62	6.97%	92.07%	39.737	5.17%	93.87%
GCN-No w	27.318	12.85%	85.20%	36.375	11.93%	86.72%	44.962	9.71%	89.10%
TGCN-No w	25.641	11.42%	86.57%	34.712	10.75%	88.04%	42.841	8.93%	90.07%
GCN	21.652	8.40%	90.73%	28.102	7.44%	91.27%	41.355	5.38%	93.82%
TGCN	21.341	8.31%	90.90%	26.324	7.46%	92.22%	40.012	5.31%	94.10%
ResLSTM	20.095	7.81%	91.86%	25.914	6.78%	92.84%	41.392	5.39%	94.28%
ResGRU-128	20.628	8.02%	91.40%	26.795	7.01%	92.78%	39.958	5.20%	94.38%
ResGRU-No G	21.508	8.37%	91.19%	25.506	6.68%	92.92%	38.704	5.04%	94.59%
ResGRU-No w	20.407	7.94%	91.66%	25.144	6.58%	93.00%	38.253	4.98%	94.60%
ResGRU	18.389	6.84%	92.23%	23.663	6.05%	93.33%	36.853	4.53%	94.82%

4.5 Results and Discussion

The prediction results of each model are shown in Table 1. Almost all models adopt the ResGRU model architecture, the prediction results of TS at 10, 15 and 30 min are very good. It can be seen from the table that GCN and TGCN, which do not take into account weather-related data, perform the worst among all models. In the model that combines all data, when TS = 10 min, the MAE and WMAPE of GRU model are the highest and the accuracy is the lowest among all models. The relevant results of the LSTM model and GCN model are about the same as the GRU, they are hardly comparable to the combined model. As the forecast period increases, the gap between the forecast performance of the single model and the combined model widens. However, the T-GCN model with graph structure and GRU fusion has not achieved the expected results. With the increase of TS, the law of passenger flow becomes more obvious, the WMAPE of all models decreases accordingly. However, the prediction accuracy of the single model is still the worst. It indicates the single model captures fewer data features than the combined model, it has no ability to extract the deep features of the data. At 10 min, the prediction performance of ResLSTM is still relatively good, it is also the closest to ResGRU. With the increase of TS, the performance of ResLSTM improves slowly. The prediction performance is not effectively achieved, it gradually becomes the lowest prediction accuracy in the combined model. Due to the internal complexity of ResLSTM, the model learning rate is reduced. At TS = 30, it achieves the highest MAE and WMAPE among all models. In ResGRU and its variant models, the prediction performance of the variant model is very similar in the process of TS growth, but the accuracy of ResGRU is higher than that of both variants. It shows that the subway network topology data and weather index data still have a certain influence on the prediction of passenger flow data. As the prediction time increases, the prediction accuracy of ResGRU increases to 92.23, 93.33 and 94.82%, while WMAPE decreases from 6.84% to 6.05% and 4.53%. In addition, after deleting the network topology branch or the weather and air pollution index data, although the prediction accuracy decreased, the prediction results did not differ too much.That hints the model has high robustness.

In order to compare the prediction performance of composite models more intuitively, Fig. 3 shows the MAE comparison chart of each model when TS = 10, 15 and 30 min. It can be seen from the figure that when TS = 10min, MAE of all models is about 20. From TS = 10 min to TS = 15 min, MAE increased by about 6, but from TS = 15 min to TS = 30 min, MAE increased by nearly 13. When TS = 30min, the reduction of data leads to the increase of model error During this period, the regularity of passenger flow is more prominent, which improves the prediction accuracy of the model. In the whole process, the MAE of ResGRU is always the lowest among all models, what proves the superiority of the proposed ResGRU architecture.

ResGRU-128 adds a certain amount of hidden units on the basis of ResGRU. Compared with ResGRU-128, it is found that the prediction accuracy between the two is quite different. In addition, it can be seen in Table 2 that when TS = 10 min, the running time of the two models differs by 800s, then gradually differs by 2400 s. What is more, no matter which TS, the RMSE of ResGRU-128 is higher. Its fitting effect is always inferior to ResGRU. This manifests that the increase

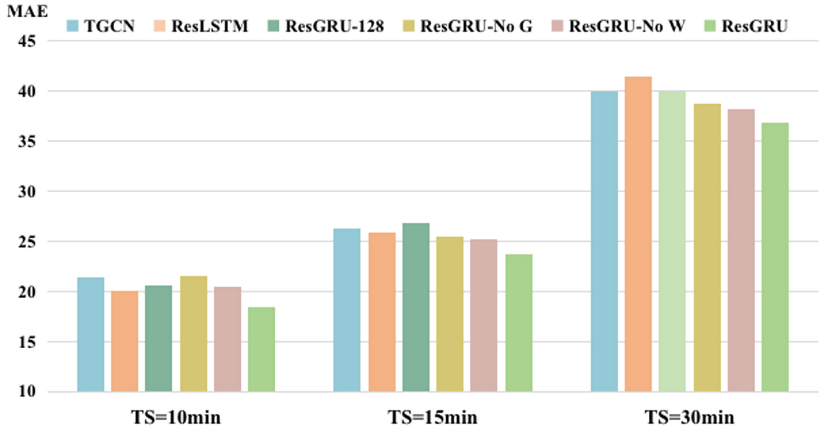


Fig. 3. The MAE values of composite models

Table 2. The prediction results of each model

TS	10 min			15 min			30 min		
Indicators	RMSE	R^2	Time(s)	RMSE	R^2	Time(s)	RMSE	R^2	Time(s)
ResGRU-128	35.58	93.96%	3959.6	44.37	94.70%	3161.3	69.45	96.62%	4730.3
ResGRU	33.38	94.76%	3175.9	42.83	96.03%	2585.7	66.47	97.35%	2108.5

in model complexity does not help the prediction performance. In the case of less data, the prediction performance of the model is worse. During the experiment, the R^2 of ResGRU gradually increased from 94.76% to 97.35%, which strongly proved the success of the ResGRU model. In a series of ablation experiments, the accuracy changes of ResGRU and its variant models during training are shown in Fig. 4. At 10 min, the change in prediction accuracy for each model from 160 to 200 epochs is shown. Among them, before 200epoch, the accuracy of variant models began to decline, while ResGRU was still growing steadily. At 15 min, it shows the change in prediction accuracy from 200 to 240 epochs. In the interim, ResGRU grew slowly, the accuracy of other models began to fluctuate and gradually decline. At 30 min, the change in prediction accuracy from 370 to 410 epochs is presented. At 370 epoch, the ResGRU accuracy dropped, then it continued to increase.

In addition, this study selected two typical stations to analyze the prediction performance of different TS. The selected station 1 has more passenger flow, while station 2 has less passenger flow. Figure 5 shows the prediction results of station 1 when TS = 10, 15 and 30 min. Figure 6 shows the prediction results of station 2 when TS = 10, 15 and 30 minutes. As shown in Figs. 4 and 5, the passenger flow of the two stations fluctuates greatly at 10 minutes. Due to the short time period selected at this time, the regularity of passenger flow is difficult to find, so the low-peak passenger flow prediction effect is not good. At 30 min, the forecast time period increases, the regularity of passenger flow is more

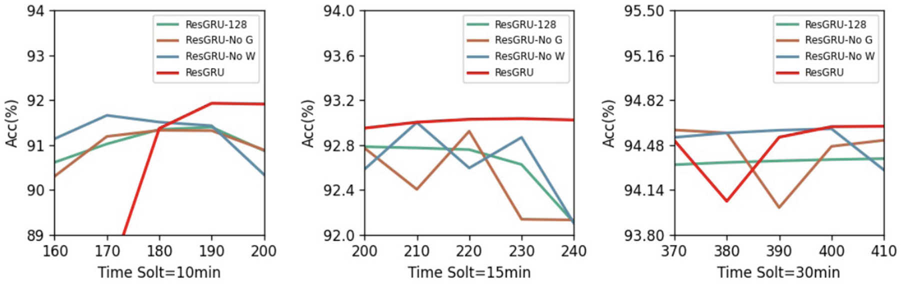


Fig. 4. The accuracy changes of models.

prominent. During the period, the low-peak passenger flow of the two stations is relatively gentle, the model prediction performance is greatly improved. The change trend of passenger flow is successfully captured. All in all, ResGRU has achieved satisfactory results in the prediction of subway passenger flow during peak hours, the model has strong stability, which promotes the development of GRU in the field of traffic passenger flow prediction.

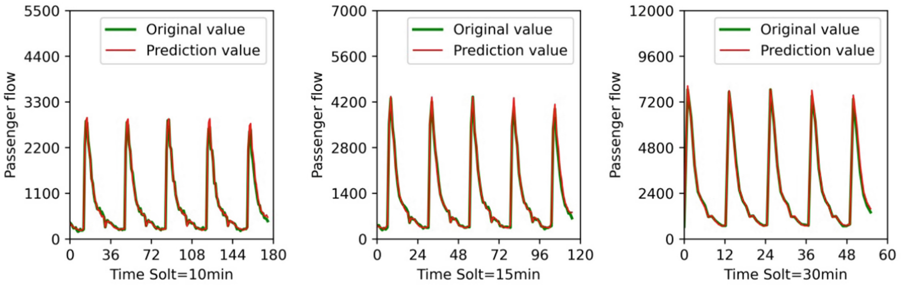


Fig. 5. The prediction results of station 1.

5 Conclusion

In this study, this study proposed a model named ResGRU, which is constructed by ResNet and attention GRU. ResGRU takes into account the subway network topology, the characteristics of subway passenger flow peak period, the spatial characteristics of passenger flow data and the influence of weather index, what achieved a higher accuracy rate of subway peak passenger flow prediction. In order to verify the effectiveness of the model, this study conducts related experiments on the Beijing subway dataset to demonstrate the superiority of the proposed ResGRU. However, this experiment did not predict the low-peak passenger flow data, the low-peak passenger flow data has poor regularity. What can

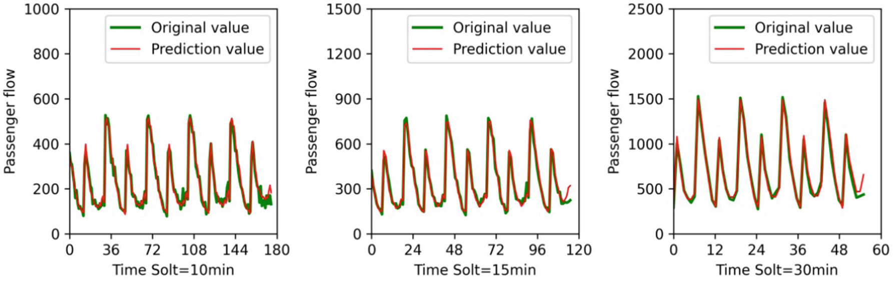


Fig. 6. The prediction results of station 2.

better test the prediction performance of the model. This study will do a separate study on the off-peak traffic data later. In the future, we will try to optimize the framework by adding transfer learning methods and conduct experiments on different traffic travel mode datasets. We would continue to explore in-depth in the field of traffic and passenger flow prediction.

Acknowledgment. This work was supported by National Natural Science Foundation of China (NSFC)(Grant No. 62162024, 62162022), the Key Research and Development Program of Hainan Province (Grant No. ZDYF2020040, ZDYF2021GXJS003),the Major science and technology project of Hainan Province (Grant No. ZDKJ2020012), Hainan Provincial Natural Science Foundation of China (Grant No. 620MS021, 621QN211), Science and Technology Development Center of the Ministry of Education Industry-university-Research Innovation Fund2021JQR017.

References

1. Wang, F., Zhu, M.: 6G-enabled short-term forecasting for large-scale traffic flow in massive IoT based on time-aware Locality-Sensitive Hashing. IEEE Internet Things J. **8**(7), 5321–5331 (2020)
2. Alipour, B., Tonetto, L., Ketabi, R.: Where are you going next? A practical multi-dimensional look at mobility prediction. In: The 22nd International ACM Conference. ACM, Utrecht, The Netherlands, pp. 5–12 (2019)
3. Sun, P., Aljeri, N., Boukerche A.: A fast vehicular traffic flow prediction scheme based on fourier and wavelet analysis. In: IEEE Global Communications Conference (GLOBECOM). IEEE, Abu Dhabi, United Arab Emirates, p. 2019 (2018)
4. Lee, K., Eo, M., Jung, E., Yoon, Y., Rhee, W.: Short-term traffic prediction with deep neural networks: a survey. IEEE Access **9**, 54739–54756 (2021)
5. Jie, H., Zou, H., Xu, Q.: Forecasting daily MRT passenger flow in taipei based on google search queries. In: 2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC). IEEE, Rome, Italy, pp. 46–50 (2021)
6. Liu, S.Y., Liu, S., Tian, Y., Sun, Q.L.: Research on forecast of rail traffic flow based on ARIMA model. J. Phys. Conf. Ser. **792**(1), 012065 (2021)
7. Run, L., Min, L.X., Lu, Z.X.: Research and comparison of ARIMA and grey prediction models for subway traffic forecasting. In: 2020 International Conference on Intelligent Computing, Automation and Systems (ICICAS), pp. 63–67 (2020)

8. Bai, L., Yao, L., Li, C., Wang, X., Wang, C.: Adaptive Graph Convolutional Recurrent Network for Traffic Forecasting. In press
9. Manibardo, E.L., Lana, I., Del Ser, J.: Transfer learning and online learning for traffic forecasting under different data availability conditions: alternatives and pitfalls. In: 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC) (2020)
10. Lana, I., Villar-Rodriguez, E.: A question of trust: statistical characterization of long-term traffic estimations for their improved actionability. In: 2019 IEEE Intelligent Transportation Systems Conference—ITSC. IEEE (2019)
11. Shen, C., Zhu, L., Hua, G., Zhou, L., Zhang, L.: A deep convolutional neural network based metro passenger flow forecasting system using a fusion of time and space. In: 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC). IEEE (2020)
12. Fafoutellis, P., Vlahogianni, E.I., Del Ser, J.: Dilated LSTM networks for short-term traffic forecasting using network-wide vehicle trajectory data. In: The 23rd IEEE International Conference on Intelligent Transportation Systems. IEEE (2020)
13. Zhao, S., Lin, S.: Urban traffic flow forecasting based on memory time-series network. In: 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC). IEEE (2020)
14. Shih, S.Y., Sun, F.K., Lee, H.Y.: Temporal pattern attention for multivariate time series forecasting. Mach. Learn. **108**(8–9), 1421–1441 (2019)
15. Grigsby, J., Wang, Z., Qi, Y.: Long-Range Transformers for Dynamic Spatiotemporal Forecasting. In press
16. Zhao, H., Yang, H., Wang, Y., Wang, D., Su, R.: Attention based graph Bi-LSTM networks for traffic forecasting. In: 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC). IEEE (2020)
17. Xiong, L., Hu, B., Huang, X., Huang, W.: Traffic flow prediction based on residual analysis. In: 2020 2nd World Symposium on Artificial Intelligence (WSAI) (2020)
18. Zhai, D., Liu, A., Chen, S., Li, Z., Zhang, X.: SeqST-ResNet: a sequential spatial temporal resnet for task prediction in spatial crowdsourcing. In: International Conference on Database Systems for Advanced Applications, (2019)
19. Vélez-Serrano.: Spatio-temporal traffic flow prediction in madrid: an application of residual convolutional neural networks. Mathematics **9** (2021)
20. Wang, B., Mohajerpoor, R., Cai, C., Kim, I., Vu, H.L.: Traffic4cast—Large-scale Traffic Prediction using 3DResNet and Sparse-UNet. In press
21. Barati, M., Petri, I., Rana, O.F.: Faster than real-time prediction of disruptions in power grids using PMU: gated recurrent unit approach. In: IEEE Power and Energy Society Innovative Smart Grid Technologies Conference (ISGT). IEEE, pp. 1–5 (2019)
22. Deng, Y., Jia, H., Li, P., Li, F.: A deep learning methodology based on bidirectional gated recurrent unit for wind power prediction. In: 2019 14th IEEE Conference on Industrial Electronics and Applications (ICIEA), IEEE, pp. 591–595 (2019)
23. An, Z., Feng, Z.: A stock price forecasting method using autoregressive integrated moving average model and gated recurrent unit network. In: 2021 International Conference on Big Data Analysis and Computer Science (BDACS), pp. 31–34 (2021)
24. Liu, L., Zhen, J., Li, G., Du, B.: Dynamic spatial-temporal representation learning for traffic flow prediction. In: IEEE Transactions on Intelligent Transportation Systems (2019)

25. Wu, Z., Pan, S., Long, G., Zhang, C.: Connecting the dots: multivariate time series forecasting with graph neural networks. In: Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, pp. 753–763 (2020)
26. Guopeng, L.I., Knoop, V.L.: Dynamic graph filters networks: a gray-box model for multistep traffic forecasting. In: 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC). IEEE (2020)

CCMFRNet: A Real-Time Semantic Segmentation Network with Context Cascade and Multi-scale Feature Refinement

Shuai Hua[1](✉), Jieren Cheng[2,3], Wenbao Han[1], Wenhang Xu[1], and Victor S. Sheng[4]

[1] School of Cyberspace Security, Hainan University, Haikou 570228, China
13510981651@163.com
[2] Hainan Blockchain Technology Engineering Research Center, Haikou 570228, China
[3] School of Computer Science and Technology, Hainan University, Haikou 570228, China
[4] Department of Computer Science, Texas Tech University, Lubbock, TX 79409, USA

Abstract. At present, many of the popular semantic segmentation networks focus on accuracy and require a lot of computational overhead, which results in a very slow inference speed and is difficult to deploy in practical application scenarios. On the other hand, many works sacrifice the performance of segmentation networks in pursuit of real-time inference speed. Therefore, in semantic segmentation, balancing accuracy and real-time performance becomes a formidable challenge. For this challenge, we propose a lightweight semantic segmentation network that takes into account both accuracy and real-time performance, named CCMFRNet. The core components of CCMFRNet are the Context Cascade Module (CCM) and the Multi-scale Feature Refinement Module (MFRM). CCM consists of three Dense Cascade Dilated Convolution Modules (DCDM), which are cascaded in a short-term dense cascade, aiming to obtain rich multi-scale context information to enhance information representation. MFRM adopts the attention mechanism to realize deep features to guide the captured shallow multi-scale spatial features. It aims to capture high-quality and multi-scale shallow features to enrich the feature space and more effectively refine the spatial details information. The proposed method achieves an accuracy of 72.6% MIoU at speed of 32 fps on Cityscapes test datasets.

Keywords: Lightweight semantic segmentation · Attention mechanism · Multi-scale context information · Feature refinement

1 Introduction

Semantic segmentation is a pixel-level classification task. Its goal is to correctly predict and classify each pixel in the image, by applying different colors to different types of pixels. As shown in Fig. 1, different colors represent Different category labels. Semantic segmentation has excellent performance in parsing and understanding application scenarios, so it has become an indispensable core method in scene understanding, such as autonomous driving [1], robot obstacle avoidance [2], and medical image analysis [3].

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 229–245, 2024.
https://doi.org/10.1007/978-981-99-7161-9_18

Since the advent of the fully convolutional network FCN [4], it has brought semantic segmentation to a new direction. Unlike the previous methods, the biggest change is to replace the last fully connected layer of the original CNN with a convolutional layer to achieve Pixel-level dense prediction, and greatly improves segmentation accuracy. Since then, many semantic segmentation models have emerged, all of which use the FCN architecture, such as U-Net [5], SegNet [6], DeepLab series [7–9], RefineNet [10], PSPNet [11], etc. There are some models that focus on accuracy [12–15]. The above segmentation models have achieved high accuracy on the CityScapes dataset [16]. These semantic segmentation models all use large and complex backbone networks, there are many operations with relatively large computational overhead. Although the features in the image can be fully extracted, a large number of complex computing operations also cause the inference speed of the network to be very slow, which cannot meet some application scenarios that require real-time performance.

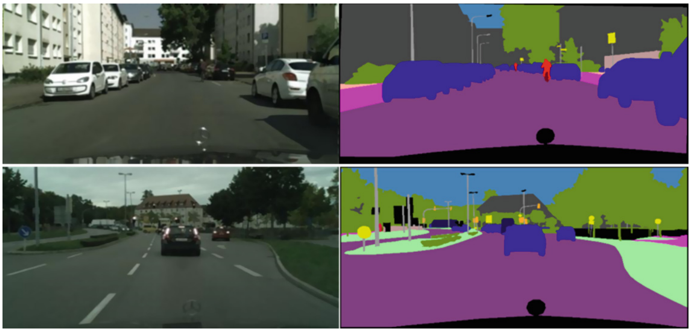


Fig. 1. Illustration of some urban scenes in Cityscapes dataset. From left to right: Image, Ground Truth.

In view of the above problems, real-time semantic segmentation that can meet real-time requirements is required. By comprehensively considering the parameters, computational complexity, accuracy, and inference speed in the segmentation network, a high inference speed can be achieved with high accuracy, which has very important research significance in the case of poor equipment resources. An important way to achieve real-time semantic segmentation is to keep the segmentation model as lightweight as possible. So far, in the research on realizing the lightweight network model, the work done is mainly divided into two categories, convolution factorization [17–23] and network compression [24–26]. Convolution factorization is to decompose standard convolutions by means of depth-wise separable convolution [20] and group convolution [22]. Depth-wise separable convolutions [20] and group convolutions [22] can achieve considerable accuracy while maintaining low computational complexity.

Network compression reduces computational complexity by compressing pretrained networks, among which methods include pruning [24], hashing [25], and quantization [26]. There are also some segmentation models [27–31] that focus on efficiency. Some models use lightweight backbone networks as encoders, such as MobileNet V2 [20], MobileNet V3 [21], these backbone networks all adopt a relatively shallow network structure design, which results in imperfect extraction of effective features. Some segmentation models do not refine the shallow spatial detail information, and the above mentioned reasons cause the poor accuracy of the current real-time semantic segmentation models. Therefore, it is of great research significance to design a real-time semantic segmentation that achieves a better balance between accuracy and inference speed.

This paper proposes an efficient real-time semantic segmentation network with context cascade and multi-scale feature refinement, named CCMFRNet, which can a-

achieve a better balance between accuracy and inference speed. We choose the improved MobileNet V2 [35] as the backbone of CCMFRNet. The two core modules of CCMFRNet are the Context Cascade Module (CCM) and the Multi-scale Feature Refinement Module (MFRM). CCM cascades three Dense Cascade Dilated Convolution Modules (DCDM) with different receptive fields through a short-term dense cascade method, and fusion of multi-scale context information captured at all levels, aiming to obtain richer multi-scale context information. Many works have shown that multi-scale context information can improve the segmentation effect, and there are many functional modules designed to capture multi-scale context information, such as ASP-P [9], PPM [11], Vortex [33], FPA [34] et al. Compared with the above modules, our CCM occupies less computing resources and achieves a considerable accuracy. Due to the successful application of various attention mechanisms [36–42] in computer vision in recent years, our MFRM also adopts an attention mechanism, MFRM first captures the multi-scale spatial information of the shallow stage, and then uses SE attention [36] to realize the deep features to guide the captured shallow multi-scale spatial features, and promote the deep feature fusion of deep features and shallow features, and more effectively refine the spatial details information. The segmentation network with symmetrical encoder-decoder structure, such as U-Net [5], RefineNet [10], combines the semantic information obtained in the encoding stage with the feature map of the corresponding size through upsampling in the decoding stage. It can better refine the spatial details information, but it increases the computational overhead to a large extent. In contrast, our MFRM achieves considerable accuracy with a more lightweight structure.

The main contributions of this paper are mainly in three aspects:

(1) semantic segmentation network named CCMFRNet is proposed, which takes into account both accuracy and real-time performance. Compared with some advanced methods, CCMFRNet achieves a better balance between accuracy and real-time performance.
(2) An efficient and lightweight Context Cascade Module (CCM) is proposed,whic-h cascades three Dense Cascade Dilated Convolution Modules(DCDM) with different receptive fields through a short-term dense cascade method, on the basis of keeping the amount of computation and parameters low, it captures rich multi-scale context information and improves the segmentation performance.
(3) An efficient Multi-scale Feature Refinement Module (MFRM) is proposed, which adopts the channel attention mechanism to realize deep features to guide the captured shallow multi-scale spatial features, enrich the feature space of the shallow stage, and promote the deep feature fusion between shallow features and deep features to effectively and efficiently refine spatial detail information.

2 The Proposed Method

2.1 Overview

In this section, we mainly introduce our proposed efficient real-time semantic segmentation network with context cascade and multi-scale feature refinement, named CCMFRNet, which is mainly composed of Context Cascade Module (CCM) and Multi-Scale Feature Refinement Module (MFRM). CCMFRNet can achieve a better balance between accuracy and real-time performance. As shown in Fig. 2, we choose the modified MobileNetV2 [35] as the encoder of CCMFRNet, where the red box part represents the MFRM.

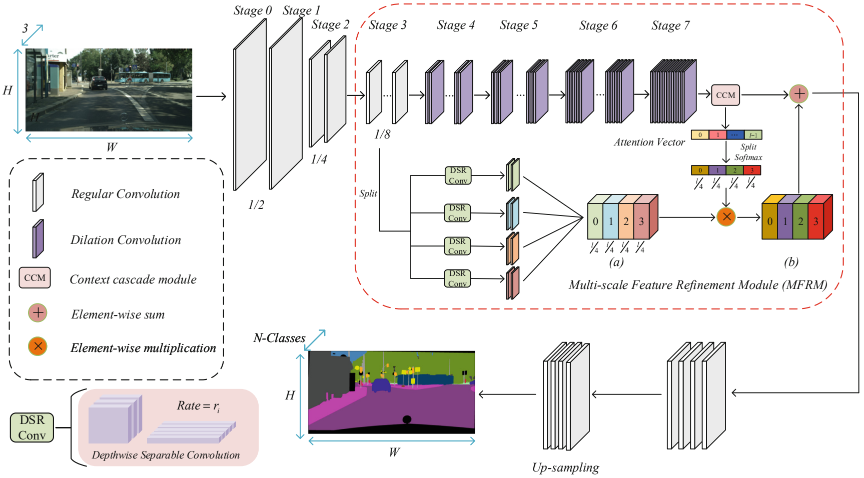


Fig. 2. Overview of Context Cascade and Multi-scale Feature Refinement Networks (CCMFR-Net). The red box represents the Multi-scale Feature Refinement Module (MFRM). **a** Shallow multi-scale spatial information. **b** Attention-guided multi-scale spatial information.

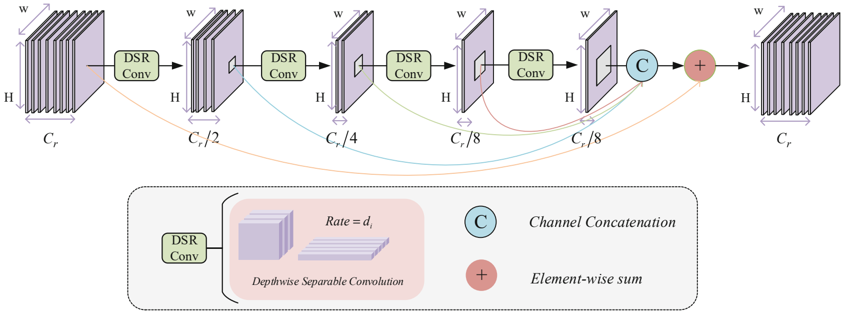


Fig. 3. Dense Cascade Dilated Convolution Module (DCDM).

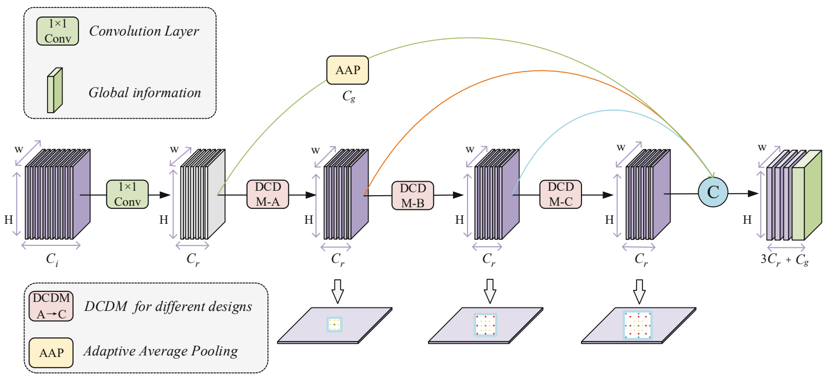


Fig. 4. Context Cascade Module (CCM).

2.2 Context Cascade Module (CCM)

Previous studies have confirmed that multi-scale context information is helpful for improving segmentation performance, such as ASPP [9], PPM [11], but ASPP and PPM have a large amount of computation and parameters, and consume a large amount of resources. Aiming at the above problems, inspired by the short-term dense cascade module [32], we propose the Context Cascade Module (CCM), CCM captures multi-scale context information through a novel single-branch cascade structure and takes up low computational resources.

As shown in Fig. 4, the feature map of the input CCM is denoted as $I^{H\times W\times C_i}$, CCM has four level operations. The first level operation is 1 × 1 convolution, which is used to compress the number of channels of the input feature map, aiming to reduce the amount of computation. The number of compressed channels is recorded as, and the compressed feature map is marked as $I'^{H\times W\times C_r}$. The above operation can be expressed by Eq. 1. Next, enter three Dense Cascade Dilated Convolution Modules (DCDM), namely DCDM_A, DCDM_B, DCDM_C, these DCDMs have different sets of dilation rates. Their average dilation rate is $\{D_a, D_b, D_c\}$, $D_a < D_b < D_c$, which aims to obtain multi-scale context information. The set of output feature maps of each level in CCM is denoted as M', the output of each level is $M' = \{I'^{H\times W\times C_r}, m_a'^{H\times W\times C_r}, m_b'^{H\times W\times C_r}, m_c'^{H\times W\times C_r}\}$, The specific operation can be expressed by Eqs. 2, 3, 4.

$$I'^{H\times W\times C_r} = \delta\left(w^{1\times 1} \times I^{H\times W\times C_i} + b\right) \tag{1}$$

$$m_a'^{H\times W\times C_r} = DCDM\_A\left(I'^{H\times W\times C_r}\right) \tag{2}$$

$$m_b'^{H\times W\times C_r} = DCDM\_B(m_a'^{H\times W\times C_r}) \tag{3}$$

$$m_c'^{H\times W\times C_r} = DCDM\_C(m_b'^{H\times W\times C_r}) \tag{4}$$

In Eq. 1, $w^{1\times 1}$ means 1 × 1 convolution, b is the bias vector, $\delta(*)$ denotes batch normaization(BN) and activation function (PReLU).

We cascades $Y'^{H\times W\times C_g}$ with the output feature map of the last three level operation of CCM, and the obtained feature map is denoted as $F^{H\times W\times(3\times C_r+C_g)}$. $Y'^{H\times W\times C_g}$ indicates the global feature information after global average pooling.The above operation can be expressed by Eq. 5.

$$F^{H\times W\times(3\times C_r+C_g)} = C\left(Y'^{H\times W\times C_g}, m_{p4}^{'H\times W\times C_r}\right) \tag{5}$$

where p4 = a, b, c.

2.3 Dense Cascade Dilated Convolution Module (DCDM)

We are inspired by short-term dense cascade modules [32], our Dense Cascade Dilated Convolution Module (DCDM) has made some improvements on its basis. DCDM is the core component of CCM.

Our DCDM adopts depth-wise separable convolution [20] and group convolution [22].The feature map $I'^{H\times W\times C_r}$ after channel compression will enter the first DCDM, which is DCDM_A, as shown in Fig. 3. Inside DCDM_A, four 3 × 3 depth-wise separable convolutions with different dilation rates are performed,the set of dilation rate is $D = \{d_1, d_2, d_3, d_4\}, d_1 < d_2 < d_3 < d_4$. We retain the channel decrement operation in the short-term dense cascade module [32] with a decrement rate of 1/2. $M = \left\{m_{p1}^{H\times W\times \frac{C_r}{p2}, d_{p1}}\right\}, p1 = 1, 2, 3, 4, p2 = 2, 4, 8, 8$. M represents the output feature map set of each level. The operation of the first level can be expressed by Eq. 6, the latter three level operations can be expressed by Eq. 7.

$$m_1^{H\times W\times \frac{C_r}{2}, d_1} = DSC_{d_1}\left(I'^{H\times W\times C_r}\right) \tag{6}$$

$$m_{q+1}^{H\times W\times \frac{C_r}{z}, d_{q+1}} = DSC_{d_{q+1}}(m_q^{H\times W\times \frac{C_r}{j}, d_q}) \tag{7}$$

In Eqs. 6 and 7, $DSC_{d_t}(*)$ denotes a 3 × 3 depth-wise separable convolution with dilation rate d_t. In Eq. 7, q = 1,2,3, z = 4,8,8, j = 2,4,8.

In practical application scenarios, there are objects of different sizes. If the network model learns from the receptive field of a single view, it is difficult to effectively extract features for objects of different sizes. Therefore, it is necessary to use the receptive field of multi-view to enable the network model to capture multi-scale context information and improve segmentation performance.

As shown in Fig. 3, first, the four level operations in DCDM_A are all 3 × 3 depth-wise separable convolutions with different dilation rates, dilation rate set $D = \{d_1, d_2, d_3, d_4\}, d_1 < d_2 < d_3 < d_4$. Such a configuration is to make each level of operation in DCDM have receptive fields of different views, and then cascade the outputs of each level through short-term dense cascades. Specifically, the output feature maps at all levels are cascaded through skip connections. Note that cascading here refers to channel concatenation. The above operation can be expressed by Eq. 8. $P_a^{H\times W\times C_r}$ represents the captured multi-scale context information.

$$P_a^{H\times W\times C_r} = C\left(m_{p1}^{H\times W\times \frac{C_r}{p2}, d_{p1}}\right) \tag{8}$$

where C(∗) represents channel concatenation.

Because DCDM is a single-branch cascade structure, the CCM containing 3 DCDMs is also a single-branch cascade structure, which deepens the depth of the network and may lead to network degeneration. To prevent network degeneration, we add the above $P_a^{H \times W \times C_r}$ to the original input feature map of DCDM_A through skip connections. The above operation can be expressed by Eq. 9. The structures of DCDM_B, DCDM_C and DCDM_A are the same, but the internal dilation rate is different, so I will not introduce it here.

$$m_a'^{H \times W \times C_r} = I'^{H \times W \times C_r} \oplus P_a^{H \times W \times C_r} \tag{9}$$

where $\oplus$ represents the element-wise sum.

2.4 Multi-scale Feature Refinement Module (MFRM)

Although the symmetrical encoder-decoder structure can well refine the spatial details information and improve the model performance. However, since upsampling enlarges the size of the feature map, and there are multiple feature fusion operations, these increase the computational overhead and memory usage, resulting in slow inference speed.

Aiming at the above problems, inspired by pyramid split attention [40], we propose an efficient Multi-Scale Feature Refinement Module(MFRM).Our MFRM can effectively refine the spatial details information. In addition, MFRM uses channel splitting and depth-wise separable convolution, so its computational complexity is low.

Although the shallow stage of the network model has rich spatial details information, it lacks multi-scale spatial information representation. As shown in the red box in Fig. 2. First,adjust the number of output channels of CCM, and record the adjusted number of channels as C_l. The output feature map of Stage 3 is denoted as $F_{stg3}^{H \times W \times C_3}$. Next, the channel splitting operation is performed, specifically, split C_l into 4 groups.Then let $F_{stg3}^{H \times W \times C_3}$ enter the multi-branch parallel structure. These branches are depth-wise separable convolutions with different dilation rates, and the set of dilation rates is denoted as $R = \{r_1, r_2, r_3, r_4\}$. As shown in Fig. 2a, the set of multi-scale spatial feature obtained by the above operations is denoted as $N = \{n_i^{H \times W \times (C_l/4), r_i}\}$, where i = 1,2,3,4. The operation can be expressed by Eq. 10. In this way, MFRM captures the multi-scale spatial information of the shallow stage and enriches the feature space of the shallow stage.

$$n_i^{H \times W \times (C_l/4), r_i} = DSC_{r_i}\left(F_{stg3}^{H \times W \times C_3}\right) \tag{10}$$

where $DSC_{r_i}(*)$ denotes depth-wise separable convolution with dilation rate r_i.

The shallow stage of the network is full of a lot of noise information. If shallow features and deep features are directly fused, these noise information will interfere with the final prediction. So we obtain the attention vector set of CCM output feature map through SE channel attention [36], which contains attention vectors. We use attention to guide the above N, so that it can choose to suppress noise information autonomously, so as to obtain high-quality and multi-scale spatial detail information. Specifically, split into 4 groups, and then normalized by the softmax function according to the group dimension, denoted as $V_l = \{v_{l/4}^{p3}\}$,where p3 = 0,1,2,3, multiply V_l and N according to the corresponding number of groups, and finally perform channel concatenation to obtain a multi-scale spatial feature map guided by attention, denoted as F_{se}, which means (b) in Fig. 2. The above operation can be expressed by Eq. 11.

$$F_{se} = C\left(v_{l/4}^{p3} \otimes n_i^{H\times W\times (C_l/4),r_i}\right) \tag{11}$$

where ⊗ means element-wise multiplication.

The output feature map of the channel-adjusted CCM is denoted as $F_{CCM}^{H\times W\times C_l}$. We sum F_{se} and $F_{CCM}^{H\times W\times C_l}$ element-wise to achieve effective and efficient refinement of spatial detail information and improve the segmentation performance. The resulting feature map is denoted as F_{MFRM}. The above operation can be expressed by Eq. 12.

$$F_{MFRM} = F_{se} \oplus F_{CCM}^{H\times W\times C_l} \tag{12}$$

3 Experimental Evaluation

3.1 Training Protocol

(1) **Datasets**. Cityscapes Dataset [16]: The cityscapes is a large-scale complex urban street scene dataset that provides pixel-level dense annotation. It is mostly used in semantic segmentation, instance segmentation, panoramic segmentation and video segmentation application scenarios. It consists of 25,000 annotated images of 2048 × 1024 resolution. The finely annotated dataset contains 5000 images including 19 valid classes. The entire urban street scene dataset contains 5000 pixel-level finely labeled images, of which 2975 are used for model training, 500 are used for model validation, and the remaining 1525 are used for model testing. We randomly subsample image resolution to 1024 × 512 patches for training.

Camvid dataset [44]: The Camvid dataset is the earliest urban road dataset applied in the field of autonomous driving. Its dataset capacity is smaller than that of Cityscapes, and the image resolution is only 960 × 720, including 12 classes in total. It consists of 367, 101 and 223 images for training, validation and testing, respectively. We randomly sub-sample all images to 480 × 360 patches for training.

2. **Evaluation Metrics**. Segmentation accuracy: The Mean Intersection over Union (MIoU) is commonly adopted for semantic segmentation accuracy.

Execution speed: The amount of forward pass time in millisecond (ms) that a network takes to process an image, which is generally measured by frames per second (FPS).

Network parameters: The sum of the parameters of each layer of the network.

Computational complexity: Floating point operations (FLOPs) are used to evaluate computational complexity.

3. **Training Details**. We implement all experiments in Pytorch with NVIDIA 1080Ti GPU cards. The training data for all ablation experiments on Cityscapes dataset is the”train” set, and the ablation results are evaluated on the validation set. We employ the mean subtraction and add a random rotation operation from –3 to 3 degrees during training process. We set initial learning rate to 0.005 and employ “Poly” learning rate policy by $1 - (iter/\max\_iter)^{power}$ with a power 0.9. In the end-to-end learning, the network is trained by using Stochastic Gradient Descent (SGD) optimization algorithm, of which the momentum is 0.9 and weight decay is 5e–4. In addition, the pixel-wise cross-entropy error is employed as our loss function.

3.2 Ablation for Context Cascade Module

In this section, we evaluate the performance of our Context Cascade Module (CCM). We take the improved MobileNet V2 [35] as our baseline network. The experimental results are shown in Table 1, Note that FLOPs is estimated on 320 × 256 × 128 inputs, A, B, C denote the three DCDMS of CCM, and GAP denotes the global average pooling. The dilation rate in group a is all 1. In this case, no multi-scale context information is obtained, resulting in an unsatisfactory segmentation effect. Let’s observe b,the dilation rate of each DCDM of b is constant, and the dilation rate of the overall DCDM is C > B > A. In this case, the multi-scale context information obtained by our CCM is not rich enough, and Poor segmentation. Let’s observe c, The dilation rate span of each DCDM of c is larger, and the subsequent dilation rate is larger, Because of the sparsity of the dilated convolution, it may not capture effective pixels, which seriously affects the correlation of long-distance information, and the segmentation effect is not ideal. By observing d and e, we found that the effect with global average pooling is the best, because global average pooling can obtain global features and further enhance the information representation. By contrast, we choose e as the best structure for CCM. In particular, group f is denoted as CCM(R), which further compresses the number of channels on the basis of group e.

Table 1. Performance comparison of CCMs with different designs.

Model	A	B	C	Params (M)	FLOPs (G)	GAP	MIoU (%)
a	{1,1,1,1}	{1,1,1,1}	{1,1,1,1}	0.18	5.9		69.83
b	{1,1,1,1}	{12,12,12,12}	{20,20,20,20}	0.18	6		71.92
c	{1,4,7,10}	{12,15,18,21}	{23,25,27,30}	0.18	6.02		70.67
d	{1,2,3,5}	{7,9,11,13}	{15,17,19,21}	0.18	5.97		71.96
e	{1,2,3,5}	{7,9,11,13}	{15,17,19,21}	0.18	5.18	✓	72.94
f	{1,2,3,5}	{7,9,11,13}	{15,17,19,21}	0.14	3.73	✓	72.19

3.3 Ablation for Multi-scale Feature Refinement Module

In this section, we evaluate our Multi-scale Feature Refinement Module (MFRM), and we use the modified MobileNet V2 [35] as our baseline network. In order to make the model as lightweight as possible, our context cascade module adopts the structural design of the optimal CCM(R) determined above. As shown in the red box in Fig. 2, MFRM is an abstraction module that includes context cascade module, so the ablation experiments of MFRM are performed on “baseline + CCM(R)”.

The results are shown in Table 2, Note that FLOPs is estimated on the 3 × 640 × 360 input, DR Stands for dilation rate, and AS stands for attention spliting. Comparing a and b, we found that adding attention mechanism can improve segmentation performance. This shows that through the attention mechanism, deep features provide constraints to shallow features, thereby suppressing noisy information in multi-scale shallow spatial features. Comparing b and c, we find that larger dilation rates achieves suboptimal segmentation because it increases noisy information in multi-scale shallow spatial features. Looking at d again, the span between the dilation rates in d is large, which weakens the degree of correlation between multi-scale shallow spatial features, resulting in poor segmentation. Through comprehensive comparison, we choose b as the best structure for MFRM.

Table 2. Performance comparison of different designs of MFRM

Model	DR	AS	Params (M)	FLOPs (G)	MIoU (%)
Baseline	–	–	1.82	6.95	68.12
Baseline + CCM(R)	–	–	1.97	7.39	72.19
a	{1,3,5,7}		2.21	8.24	72.87
b	{1,3,5,7}	✓	2.23	8.24	73.42
c	{5,7,9,11}	✓	2.23	8.24	72.6
d	{3,7,11,15}	✓	2.23	8.24	72.82

3.4 Evaluate in the Cityscapes Dataset

In this section, we will perform ablation experiments on the components of CCM(R) and MFRM on the improved MobileNet V2. The experimental results are shown in Table 3, Note that FLOPs is estimated on the 3 × 640 × 360 input. As mentioned above, MFRM includes a context cascade module, so adding MFRM to the baseline network is equivalent to our best model.We can see from Table 4 that when CCM and MFRM are added to our baseline network, the accuracy is improved accordingly. In conclusion, both qualitative and quantitative results verify that the proposed two modules can effectively improve the network learning ability.

In addition to the above ablation experiments, we compare CCMFRNet with other advanced methods on the Cityscapes test set. Our results are submitted to the official Cityscapes server for evaluation. The comparison results are shown in Table 4. The inference speed is the average of 100 runs on NVIDIA 1080Ti, and “–” means no corresponding values have been published. Compared with methods that focus on efficiency, such as Enet [27], FSSNet [45], our CCMFRNet, although inferior in inference speed, improves the accuracy by at least 13% MIOU. Recently, relatively new methods, such as

Table 3. Ablation studies on the components of CCM(R) and MFRM

Baseline	CCM (R)	MFRM	Params (M)	FLOPs (G)	MIoU (%)
✓			1.82	6.95	68.12
✓	✓		1.97	7.39	72.19(+4.35)
✓		✓	2.23	8.24	73.42(+5.58)

CIFReNet [35], DSANet [50], our CCMFRNet has similar inference speed to them, and the most valuable thing is that the accuracy of CCMFRNet is improved by 1.7% MIOU and 1.21% MIOU, respectively. Compared with methods that focus on accuracy, such as DeepLabV2 [7], CCMFRNet has about 24 times fewer FLOPs, about 20 times fewer parameters, 2.2% MIOU higher accuracy,and inference speed is also greatly improved. By comparison, it can be seen that our proposed method achieves a better balance between accuracy and speed. Figure 5 shows some visual examples of the Cityscapes validation set.

3.5 Evaluation on CamVid Dataset

In this section, we further evaluate the performance of CCMFRNet on the CamVid dataset [44]. Compared with the CityScapes dataset, the image size of the Camvid dataset is relatively small, so we set the dilation rate sets of the 3 DCDMs in the CCM to {1,2,3,5},{7,9,11,13},{13,15,17,19}, which aim to capture multi-scale context information in low resolution feature maps. Also change the dilation rate of the parallel branch structure in MFRM to {1,2,3,5}.The comparison results are shown in Table 5. CCMFRNet achieves 65.8% MIOU accuracy using only 2.2M parameters. Compared with methods focusing on accuracy (e.g. DeconvNet [55], DeepLab-LFOV [58]) and methods focusing on efficiency (e.g. Enet[27], Skip-Mobilenet [57], FC-DenseNet56 [12]), Our CCMFRNet achieves a better balance between accuracy and efficiency.

Table 4. Performance comparisons on Cityscapes test set

Method	Backbone	Resolution	FPS	FLOPs (G)	Params (M)	MIoU (%)
Segnet [6]	–	640 × 360	16.7	286.0	29.5	56.1
Enet [27]	–	640 × 360	135.4	3.8	0.4	58.3
FSSNet [45]	–	1024 × 512	51.0	–	0.2	58.8
ERFNet [46]	–	1024 × 512	14.7	53.5	2.1	68.0
Fast-SCNN [47]	MobileNetV2	2048 × 512	123.5	–	0.1	68.0
CANet [48]	MobileNetV2	1024 × 512	95.3	18.5	4.8	69.5
aESNet [49]	MobileNetV2	1024 × 512	63.0	–	1.6	70.7
CIFReNet [35]	MobileNetV2	1024 × 512	34.5	16.5	1.9	70.9
DSANet [50]	–	1024 × 512	34.08	37.4	3.47	71.39
FCN [4]	VGG16	1024 × 512	2.0	136.2	134.5	65.3
DRN [51]	ResNet50	1024 × 512	–	355.2	20.6	67.3
DeepLabV2 [7]	ResNet101	1024 × 512	0.3	457.8	44	70.4
DLC [52]	IRNet	1024 × 512	–	26.5	–	71.1
RefineNet [10]	ResNet101	1024 × 512	0.9	118.1	–	73.6
DenseASPP [13]	DenseNet121	1024 × 512	–	155.8	28.6	76.2
PSPNet [11]	ResNet101	713 × 713	0.8	412.2	250.8	78.4
SFNet [53]	ResNet101	1024 × 1024	–	417.5	50.3	81.8
HANet [54]	ResNet101	768 × 768	–	–	65.4	82.1
CCMFRNet	MobileNetV2	640 × 360 512 × 512 713 × 713 1024 × 448 1024 × 512	66.7 62.5 30.4 35.7 32	8.2 9.4 18.5 16.4 18.7	2.2	72.6

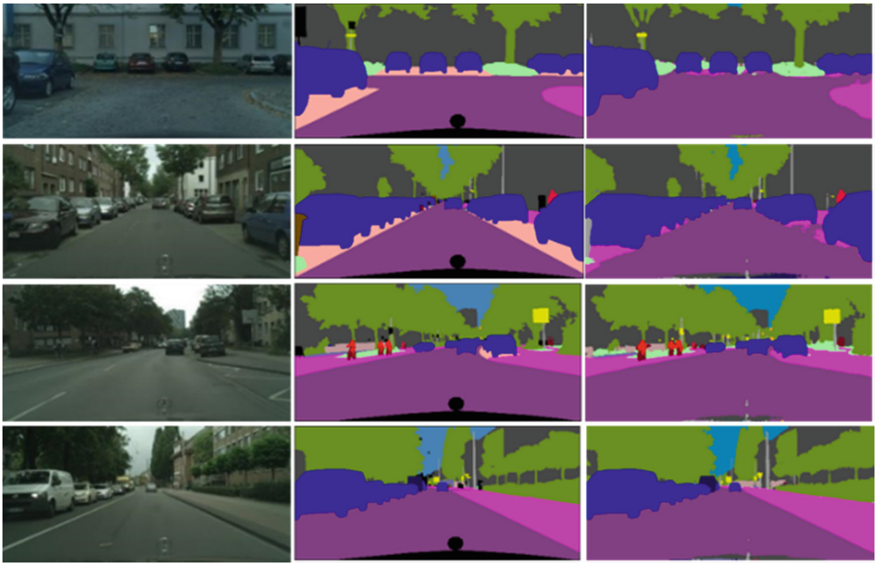


Fig. 5. Qualitative results on the cityscape validation dataset when using our best model. From left to right: Image, Ground Truth, CCMFRNet.

Table 5. Performance comparisons on CamVid test set

Method	Params (M)	MIoU (%)
Segnet [6]	29.5	46.4
DeconvNet [55]	252	48.9
Enet [27]	0.4	51.3
LinkNet [56]	11.5	55.8
FCN [4]	134.5	57.0
Skip-Mobilenet [57]	3.4	58.8
FC-DenseNet56 [12]	1.5	58.9
DeepLab-LFOV [58]	37.5	61.6
CIFReNet [35]	1.9	64.5
CCMFRNet	2.2	65.8

4 Conclusion

This paper proposes an efficient real-time semantic segmentation network (CCMFR-Net) with context cascade and multi-scale feature refinement. Our CCMFRNet has two core components, the Context Cascade Module (CCM) and the Multi-scale Feature Refinement Module (MFRM). CCM cascades three Dense Cascade Dilated Convolution Modules (DCDM) with different receptive fields through a short-term dense cascade method, aiming to obtain richer multi-scale context information. MFRM adopts the attention mechanism to realize the deep features to guide the captured shallow multi-scale spatial features, enrich the feature space of the shallow stage, and promote the deep feature fusion of shallow features and deep features,and effective refinement of spatial details information. Experiments show that the proposed CCMFRNet not only occupies less computing resources, but also achieves a considerable prediction accuracy.

Acknowledgment. This work was supported by National Natural Science Foundation of China (NSFC) (Grant No. 62162024,62162022), the Key Research and Development Program of Hainan Province (Grant No. ZDYF2020040, ZDYF2021GXJS003), the Major science and technology project of Hainan Province (Grant No. ZDKJ2020012), Hainan Provincial Natural Science Foundation of China (Grant No. 620MS021,621QN211), Science and Technology Development Center of the Ministry of Education Industry-university-Research Innovation Fund (2021JQR017).

References

1. Jla, B., Fjab, D., Jing, Y., et al.: Lane-DeepLab: Lane semantic segmentation in automatic driving scenarios for high-definition maps. Neurocomputing, (2021)
2. Teso-Fz-Betoo, D., Zulueta, E., Sanchez-Chica, A. et al.: Semantic segmentation to develop an indoor navigation system for an autonomous mobile robot. (2020)
3. Yang, R., Yu, Y.: Artificial convolutional neural network in object detection and semantic segmentation for medical imaging analysis. Front. Oncol. **11**, 638182 (2021)
4. Long, J., Shelhamer, E., Darrell, T.: IEEE, Fully convolutional networks for semantic segmentation. In: IEEE Conference on computer vision and pattern recognition (CVPR), pp. 3431–3440. IEEE, Boston, MA, (2015)
5. Ronneberger, O., Fischer, P., Brox, T.: U-Net: Convolutional networks for biomedical image segmentation. Springer International Publishing, (2015)
6. Badrinarayanan, V., Kendall, A., Cipolla, R.: SegNet: A deep convolutional encoder-decoder architecture for image segmentation. IEEE Trans. Pattern Anal. Mach. Intell., 1–1 (2017)
7. Chen, L.C., Papandreou, G., Kokkinos, I., et al.: DeepLab: Semantic image segmentation with deep convolutional nets, Atrous convolution, and fully connected CRFs. IEEE Trans. Pattern Anal. Mach. Intell. **40**(4), 834–848 (2018)
8. Chen, L.C., Papandreou, G., Schroff, F et al.: Rethinking atrous convolution for semantic image segmentation. (2017)
9. Chen, L.C., Zhu, Y., Papandreou, G., Schroff, F., Adam, H.: Encoder-decoder with atrous separable convolution for semantic image segmentation. In: Proceedings of the European conference on computer vision (ECCV), pp 801–818 (2018)
10. Lin, G., Milan, A., Shen, C., Reid, I.: RefineNet: Multi-path refinement networks for high-resolution semantic segmentation.In: Proceedings of the IEEE conference on computer vision and pattern recognition (CVPR), pp 5168–5177 (2017)
11. Zhao, H., Shi, J., Qi, X., Wang, X., Jia, J.: Pyramid scene parsing network. In: Proceedings of the IEEE conference on computer vision and pattern recognition (CVPR), pp 6230–6239 (2017)
12. Jegou, S., Drozdzal, M., Vazquez, D., Romero, A., Bengio, Y.: The one hundred layers tiramisu: fully convolutional densenets for semantic segmentation. In: Proceedings of the IEEE conference on computer vision and pattern recognition workshops, pp. 11–19 (2017)
13. Yang, M., Yu, K., Zhang, C., Li, Z., Yang, K.: Denseaspp for semantic segmentation in street scenes. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 3684–3692 (2018)

14. Yu, C., Wang, J., Gao, C., Yu, G., Shen, C., Sang, N.: Context prior for scene segmentation. In: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 12416–12425 (2020)
15. Liu, J., He, J., Qiao, Y., Ren, J.S., Li, H.: Learning to predict context-adaptive convolution for semantic segmentation. In: European conference on computer vision, pp.769–786 (2020)
16. Cordts, M., Omran, M., Ramos, S., Rehfeld, T., Enzweiler, M., Benenson, R., Franke, U., Roth, S., Schiele, B.: The cityscapes dataset for semantic urban scene understanding. In: Proceedings of the IEEE conference on computer vision and pattern recognition(CVPR), pp 3213–3223 (2016)
17. Szegedy, C., Ioffe, S., Vanhoucke, V., Alemi, A.A.: AAAI, Inception-v4, Inception-ResNet and the impact of residual connections on learning. In: Thirty-First AAAI Conference on artificial intelligence, pp. 4278−4284 (2017)
18. Zhao, H., Qi, X., Shen, X., Shi, J., Jia, J.: ICNet for real-time semantic segmentation on high-resolution images, computer vision–Eccv 2018. Pt Iii **11207**, 418–434 (2018)
19. Romera, E., Alvarez, J.M., Bergasa, L.M., Arroyo, R.: ERFNet: Efficient residual factorized ConvNet for real-time semantic segmentation. IEEE Trans. Intell. Transp. Syst. **19**(1), 263–272 (2018)
20. Sandler, M., Howard, A., Zhu, M., Zhmoginov, A., Chen, L.-C.: IEEE, MobileNet V2: Inverted residuals and linear bottlenecks. In: IEEE/CVF Conference on computer vision and pattern recognition 2018, pp 4510–4520 (2018)
21. Howard, A., Sandler, M., Chu, G., Chen, L.-C., Chen, B., Tan, M., Wang, W., Zhu, Y., Pang, R., Vasudevan, V., Le, Q.V., Adam, H.: IEEE, Searching for MobileNetV3. IEEE/CVF International conference on computer vision (ICCV), pp. 1314–1324. South Korea, Seoul. (2019)
22. Zhang, X., Zhou, X.Y., Lin, M.X., Sun, R.: IEEE, ShuffleNet: An extremely efficient convolutional neural network for mobile devices. In: 31st IEEE/CVF Conference on computer vision and pattern recognition (CVPR), pp. 6848–6856. IEEE, Salt Lake City, UT. (2018)
23. Chollet, F.: IEEE, Xception: Deep learning with depthwise separable convolutions. In: 30th IEEE/CVF Conference on computer vision and pattern recognition (CVPR), pp. 1800–1807. Honolulu, HI, IEEE (2017)
24. Han, S., Mao, H., Dally, W.J.: Deep Compression: Compressing deep neural networks with pruning, trained quantization and huffman coding, pp. 3–7. ICLR (2015)
25. Chen, W., Wilson, J.T., Tyree, S., Weinberger, K.Q., Chen, Y.: Compressing neural networks with the hashing trick. Comput. Sci., 2285–2294 (2015)
26. Wu, J., Cong, L., Wang, Y., Hu, Q., Jian, C.: Quantized convolutional neural networks for mobile devices. In: 2016 IEEE Conference on computer vision and pattern recognition (CVPR), (2016)
27. Paszke, A., Chaurasia, A., Kim, S.: Culurciello EE. Enet: A deep neural network architecture for real-time semantic segmentation. (2016). arXiv preprint. arXiv:1606.02147
28. Yu, C., Wang, J., Peng, C., Gao, C., Yu, G., Sang, N.: Bisenet: bilateral segmentation network for real-time semantic segmentation. In: Proceedings of the European conference on computer vision (ECCV), pp. 325–341 (2018)
29. Emara, T., AbdElMunim, H.E., Abbas, H.M.: LiteSeg: a novel lightweight ConvNet for semantic segmentation. In: 2019 Digital image computing: Techniques and applications (DICTA), pp. 1–7 (2019)
30. Mehta, S., Rastegari, M., Caspi, A., Shapiro, L., Hajishirzi, H.: Espnet: efficient spatial pyramid of dilated convolutions for semantic segmentation. In: Proceedings of the European conference on computer vision (ECCV), pp. 552–568 (2018)
31. Jiang, W., Xie, Z., Li, Y., Liu, C., Lu, H.: LRNNET: a light-weighted network with efficient reduced non-local operation for real-time semantic segmentation. In: 2020 IEEE International conference on multimedia expo workshops (ICMEW), pp. 1–6 (2020)

32. Fan, M., Lai, S., Huang, J. et al.: Rethinking bisenet for real-time semantic segmentation. In: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 9716–9725 (2021)
33. Xie, C.W., Zhou, H.Y., Wu, J.: Vortex pooling: Improving context representation in semantic segmentation. (2018)
34. Li, H., Xiong, P., An, J., Wang, L.: Pyramid attention network for semantic segmentation. In: Proc Brit Mach Vis Conf (BMVC), p. 285 (2018)
35. Jiang, B., Tu, W., Yang, C., et al.: Context-integrated and feature-refined network for lightweight object parsing. IEEE Trans. Image Process. **29**, 5079–5093 (2020)
36. Hu, J., Shen, L., Sun, G.: IEEE, Squeeze-and-excitation networks. In: 31st IEEE/CVF Conference on computer vision and pattern recognition (CVPR), pp. 7132–7141. IEEE, Salt Lake City, UT (2018)
37. Wang, Q., Wu, B., Zhu, P., Li, P., Zuo, W., Q.J.I.C.C.o.C.V. Hu, P.: Recognition, ECANet: Efficient channel attention for deep convolutional. Neural Netw., 11531–11539 (2020)
38. Hou, Q., Zhou, D., Feng, J.: Coordinate attention for efficient mobile network design. (2021)
39. Sagar, A.: DMSANet: Dual multi scale attention network. (2021)
40. Zhang, H., Zu, K., Lu, J et al.: EPSANet: An efficient pyramid split attention block on convolutional neural network. (2021). arXiv preprint arXiv:2105.14447
41. Zhao, H., Jia, J., Koltun, V.: Exploring Self-attention for image recognition. (2020)
42. Huang, Z., et al.: CCNet: Crisscross attention for semantic segmentation. In: IEEE/CVF International Conference on Computer Vision (ICCV), pp. 603–612 (2019)
43. Dong, G., Yan, Y., Shen, C., et al.: Real-time high-performance semantic image segmentation of urban street scenes. IEEE Trans. Intell. Transp. Syst. **22**(6), 3258–3274 (2020)
44. Brostow, G.J., Fauqueur, J., Cipolla, R.: Semantic object classes in video: A high-definition ground truth database. Pattern Recognit. Lett. **30**(2), 88–97 (2009)
45. Zhang, X., Chen, Z., Wu, Q.J., Cai, L., Lu, D., Li, X.: Fast semantic segmentation for scene perception. IEEE Trans Industr Inform. **15**(2), 1183–1192 (2018)
46. Romera, E., Alvarez, J.M., Bergasa, L.M., Arroyo, R.: Erfnet: efficient residual factorized convnet for real-time semantic segmentation. IEEE Trans Intell Transport Syst. **19**(1), 263–272 (2017)
47. Poudel, R.P., Liwicki, S., Cipolla, R.: Fast-scnn: Fast semantic segmentation network. (2019). arXiv preprint.arXiv:1902.04502
48. Zhang, C., Lin, G., Liu, F., Yao, R., Shen, C.: Canet: Class-agnostic segmentation networks with iterative refinement and attentive few-shot learning. In: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 5217–5226 (2019)
49. Wang, Y., Zhou, Q., Xiong, J., Wu, X., Jin, X.: Esnet: An efficient symmetric network for real-time semantic segmentation. In: Chinese conference on pattern recognition and computer vision (PRCV), pp. 41–52
50. Elhassan, M., Huang, C., Yang, C., et al.: DSANet: dilated spatial attention for real-time semantic segmentation in urban street scenes. Expert Syst. Appl. **183**, 115090 (2021)
51. Li, X., Liu, Z., Luo, P., Change Loy, C., Tang, X.: Not all pixels are equal: difficulty-aware semantic segmentation via deep layer cascade. In: Proceedings of the IEEE Conference on computer vision and pattern recognition, pp. 3193–3202 (2017)
52. Yu, F., Koltun, V., Funkhouser, T.: Dilated residual networks. In: Proceedings of the IEEE Conference on computer vision and pattern recognition, pp. 472–480 (2017)
53. Li, X., You, A., Zhu, Z et al.: Semantic flow for fast and accurate scene parsing. In: European conference on computer vision, pp. 775–793 (2020)
54. Choi, S., Kim, J.T., Choo, J.: Cars can't fly up in the sky: Improving urban-scene segmentation via height-driven attention networks. In: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 9373–9383 (2020)

55. Noh, H., Hong, S., Han, B.: Learning deconvolution network for semantic segmentation. In: Proceedings of the IEEE International conference on computer vision, pp. 1520–1528 (2015)
56. Chaurasia, A., Culurciello, E.: Linknet: exploiting encoder representations for efficient semantic segmentation. In: 2017 IEEE Visual Communications and Image Processing (VCIP), pp. 1–4
57. Siam, M., Gamal, M., Abdel-Razek, M., Yogamani, S., Jagersand, M.: Rtseg: real-time semantic segmentation comparative study. In: 2018 25th IEEE International Conference on Image Processing (ICIP), pp. 1603–1607
58. Chen, L.C., Papandreou, G., Kokkinos, I., et al.: Semantic image segmentation with deep convolutional nets and fully connected CRFs. Computer Science **4**, 357–361 (2014)

A Survey of Low-Resource Named Entity Recognition

Xiangyan Tang[1,2,3], Dongwan Xia[1,3](✉), Yajing Li[1,3], Taixing Xu[1,3], and Neal N. Xiong[4]

[1] School of Computer Science and Technology, Hainan University, Haikou 570228, China
1220474455@qq.com

[2] College of Intelligence and Computing, Tianjin University, Tianjin 300072, China

[3] Hainan Blockchain Technology Engineering Research Center, Haikou 570228, China

[4] Department of Computer Science and Mathematics, Sul Ross State University, Alpine, TX 79830, USA

Abstract. Named Entity Recognition, as one of the typical tasks of information extraction, has a wide range of applications. However, the difficulty of data collection and the lack of data annotation are common problems in real scenarios. It is difficult for classical named entity recognition methods to fully obtain hidden information when the dataset and data labels are insufficient. In this case, the recognition accuracy will drop significantly. In resource-poor scenarios, the use of multi-task learning, data augmentation, and transfer learning methods can effectively utilize limited data resources or introduce data from other fields to optimize model performance. In this survey, firstly, we introduce the reader to the state of research on named entity recognition, and outline the reasons for the survey and the contribution of this paper. Then, we comprehensively describe the datasets and evaluation methods included in named entity recognition, and propose a Classification of named entity recognition in the case of lack of resources. Finally, we analyze the existing problems on the basis of the above, and further look forward to the future development direction.

Keywords: Named entity recognition · Resource scarcity · Multi-task learning · Data augmentation · Transfer learning

1 Introduction

Named Entity Recognition (NER) task is the process of detecting, locating and segmenting named entities in text, i.e. assigning named entity labels to words or words in sentences that contain specific meanings. A named entity is an expression of a word or word with a specific meaning, such as a date, a person's name, an institution, a geographic location name, a domain proper name, etc. in the text. Accurate partitioning of entities can provide a good foundation for many applications in natural language processing (NLP).

Since the concept of "named entity" was first defined, NER has been widely studied and applied. Many domain and task-specific entities are constantly being mentioned,

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 246–260, 2024.
https://doi.org/10.1007/978-981-99-7161-9_19

the types of entities are constantly expanding, and scholars in different fields have also shown strong interest in NER in solving various tasks. For example, in the construction of knowledge base, the unsupervised method combined with named entity extraction is used to improve the recall rate of knowledge system [1]. In the question answering system, the named entity recognizer is used as the core to help filter the question answering content [2]. In the information retrieval task, NER is used to detect the named entities in the retrieval [3]. In entity link, accurate entity division to eliminate entity ambiguity [4, 5]. In text understanding, entities are extracted from the text to help build a knowledge map [6], or to increase attention to entity knowledge to help text understanding [7].

In the past, many scholars have sorted out and summarized the research on NER. For example, early classification is based on different factors, model learning methods and selected features [8], or classification is based on the importance of NER in field application [9]. In specific fields such as biomedicine, there is also a summary of NER [10, 11]. With the emergence of deep learning, NER has made many new progress [12]. Yadav and Bethard [13] compared the deep learning framework with the previous feature engineering. Gao and Zhang [14] classified NER according to different supervision methods in cyberspace security systems. Although some researchers have investigated and reviewed the work in this field in the past, according to the survey, there are very few research reviews on NER in resource-poor fields, and there is also a lack of research reviews on the classification of NER solutions in resource-poor environments. In response to these problems, we investigate and summarize the representative and widely used deep learning-based methods in named entity recognition in recent years, as well as related datasets and general evaluation indicators, and propose a new NER classification method in low-resource environments. Finally, by summarizing and thinking about a large number of articles in this research direction, we briefly introduce the future development of NER field to readers.

2 Background

In this section, we first outline the recent research status and representative articles of deep learning methods for named entity recognition, then list the datasets widely used by researchers in the field of NER, and finally introduce reasonable evaluation metrics for NER.

2.1 Research Status of NER

The rapid development of deep learning methods in the direction of NER benefits from its ability to more easily discover hidden features in data. In NER, the role of the encoder is generally to process character or word information and learn the feature semantic information contained in it, and the role of the decoder is generally to receive semantic representations and convert them into sequence labels. In recent years, for the research and implementation of NER deep learning methods, different scholars usually choose different encoders and decoders to combine according to different needs. In terms of input representation of model architecture, it can be divided into character, word and joint representation. This aspect will be discussed next.

Word-level embeddings. Using the word-level representation (Word-level Representation) form means that the word is the smallest input unit, and it is represented in the form of a vector through word embedding, Word level representation is used, which means that words are used as the minimum input unit and are expressed in vector form after word embedding. The dimensional representation of words in the vector space can express its features in an implicit way, and similar words have more similar representations in the vector space, which is more conducive to model learning.

Collober and Weston et al. [15] were the first to propose word embeddings as the first layer input of neural network models in natural language tasks. After this, Passos and Kumar et al. [16] introduced dictionaries to implement NER systems and demonstrated that word embeddings can improve the performance of NER. Pennington and Socher et al. [17] proposed the Global Vectors model in order to compensate for the lack of representation method for word variables (such as not considering the word order or distribution of words in sentences or paragraphs), which increased the global information while improving the training speed of the model. Yao and Liu et al. [18] use the words in the sliding window as model input and extract data features based on convolutional neural network (CNN). After that, Huang and Xu et al. [19] applied the BiLSTM-CRF network architecture to the sequence tagging task for the first time on the basis of word-level representation, combining the forward sequence and backward sequence features of sentences, and correspondingly reducing the dependence of the model on word embedding. By contrast, Strubell and Verga [20] also use word-level representation, but instead use Dilated Convolutional Neural Networks (ID-CNNs) as context encoders to implement NER, because in the process of the implementation, the previous step of RNN calculation The result produced has a significant impact on the calculation of the latter step (calculated in sequence order), but CNN does not have this problem, so not only can more non-local features in the text be extracted, but also the model can be improved compared to using LSTM parallel computing power. For nested entity recognition, Shen and Ma et al. [21] used coding to divide words, and then used boundary regression to locate word boundaries. In this step-by-step process, entity types could be divided more accurately.

Character-Level Embeddings. In some languages, tokens cannot be obtained directly like english and other languages, and there is no natural separation symbol such as spaces in the text. When using word-level representation, the performance of the final model may be degraded due to the occurrence of word segmentation errors. For example, in the use of Chinese, the "word" used to express semantics may be a Chinese character, word or idiom. In the research of NER, the use of character-based word embedding representation can not only reduce the impact of word segmentation errors to a certain extent, but also reduce the excessive dependence of the NER model on the word information in the training data, which is more conducive to improving the generalization of the model.

The character-level embedding experiment shows its advantages in many languages [25], especially in Chinese [22, 26, 27]. Gillick and Brunk et al. [23] take the read byte sequence as input, resulting in a large vocabulary reduction. Kim and Jernite et al. [24] verified the advantages of character-level input for language models based on the CNN-LSTM network architecture, that is, they can achieve more advanced results with fewer training parameters. In order to solve the lack of data in practical tasks, Petersh and

Neumann et al. [28] used readily available unlabeled data to pre-train LM embeddings using semi-supervised methods to enhance the originally limited semantic information of words. Later, they [29] proposed a lexical representation method ELMo that simulates multiple features and contextual changes of words, which not only improves the performance of the language models, but also is easily added to the model. Zhu and Wang et al. [30] in order to avoid using only character-level embedding model to learn only limited information, integrated local attention into CNN to locate key feature information, and proposed a CAN network structure to enhance the hidden information of character sequences in context learning ability.

Hybrid Architecture. If we only pay attention to the character information or lexical information in the sentence, it will have an omission effect on the acquisition of global information. compared with using character level or word level representation alone, combining the two or adding additional features has a significant effect on enhancing the correlation between named entities in text, and is compared in Table 1. In addition, the introduction of external dictionaries, shallow parsing, place names, spelling features, radicals, parts of speech, etc. Will help improve the performance of NER. As shown in Fig. 1.

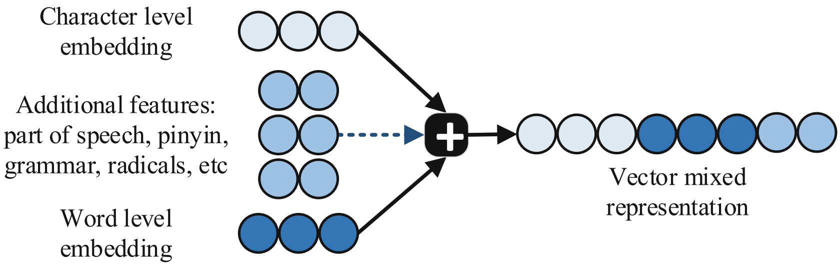

Character level embedding
Additional features: part of speech, pinyin, grammar, radicals, etc
Word level embedding
Vector mixed representation

Fig. 1. Multi-feature mixed input representation.

Ma and Hovy et al. [31] combine word representation with character-level representation generated by CNN, taking advantage of CNN's ability to efficiently learn characters or word morphological features. Lample and Ballesteros et al. [33] combined supervised and unsupervised learning methods to learn character-level and word-level representations in order to improve the dependence of NER model training on a large amount of manually labeled data. In addition to the combination of these two embedding types, many scholars have also done corresponding research on the introduction of external knowledge and additional features [32, 37]. Bharadwaj and Mortensen et al. [34] added phonetic character representation, which enables the model to adapt quickly in cross-language/cross-domain applications because of its global representation. Later, in response to the problems of NER in the social media field, such as the rapid development of social media, the rapid increase of new named entity types in a large number of generated texts, and the large amount of informal communication information contained in the texts, Lin and Xu et al. [35]proposed a multi-channel model to generate a more comprehensive representation of the words input into the sentence, such as syntactic features. Gui and Zou et al. [36] used graph structure to improve the problem of sequence structure limitation in RNN, introduced dictionaries to obtain word and word interactions, and designed relay nodes to obtain high-level information of entities, and also to solve the purpose of ambiguous words. In order to prevent the phenomenon of overfitting of the named entity recognition model. Compared with the introduction of toponymic dictionaries as additional features, the use of lexical features can reduce the restriction that some words brought by toponymic dictionaries can only be used as specific types [38], and embed words and entity types into multi-dimensional space to reflect the similarity from the dimension (Table 1).

Table 1. Comparison of advantages and disadvantages based on different distributed input representations.

Distributed representation of inputs	Advantage	Deficiencies
Word level embedding	The semantic information and boundary information of words that can be provided	Inaccurate segmentation will lead to different meanings of words in different contexts
Character level embedding	Be able to infer the word representation outside the vocabulary	Lack of ability to capture boundary information of words
Mixed input distributed representation	It can provide more prior knowledge for the model	It may reduce the generalization ability of the model

In the research and application of NER in the Chinese field, many scholars also have attainments. Zhang and Yang [39] proposed an LSTM model of lattice structure in the implementation of Chinese NER, which can fuse the potential lexical information existing in the sentence, which not only avoids the error of entity boundary division caused by word segmentation errors, but also integrates word sequence information. If a fixed-size remote word information is added at each Chinese character connection [41], it will be more conducive to batch training. Different from using a chain structure to fuse words and word information, Ding and Xie et al. [42] use multi-dimensional automatic learning dictionary to fuse feature information, complete the interaction between dictionary and character information, and have the characteristics of disambiguation and reducing error matching rate. It has the characteristics of disambiguation and reducing the false matching rate. Later, in order to avoid the effect of no available dictionary, additional interference caused by introduced features, and out-of-vocabulary (OOV) words, Zhu and Wang et al. [30] use convolutional attention layer to enhance the learning and coding ability of the information and features contained in the character sequence, and increase the global attention mechanism to improve the capture ability of sentence context information [40]. Wu and Liu et al. [43] proposed a model that jointly trained word segmentation and NER, shared the parameters of the word segmentation model to improve the accuracy of word boundary segmentation, and used CNN to capture contextual information in character embeddings, the number of training samples is increased by generating pseudo samples by synonymous replacement of entities in the text. Song and Sehanobish et al. [44] added the idea of computer vision to encode Chinese character image extraction features by processing images, and then used Chinese glyph semantic information as additional information to help NER model training.

2.2 Dataset

Building reliable NER systems often requires task-specific annotated public corpora. Labeled dataset documents often contain many different types of entities. The widely used datasets in the NER field will be presented in Table 2. NER is usually regarded as a sequence labeling task, that is, given a series of input sequences, the model learns features, rules and relationships according to a series of data, and finally outputs a sequence with labels according to the learned knowledge.

Table 2. Enumeration of commonly used datasets in NER.

Dataset name	Language	Named entity type	Data source
CoNLL2003	English, German, Spanish, Dutch	LOC, ORG, PER, MISC	Reuters news
OntoNotes	English, Arabic, Chinese	7 types	Weblogs, news, broadcast, etc
MSRA NER	Chinese	LOC, ORG, PER	–
People's daily NER	Chinese	LOC, ORG, PER	People's daily news corpus
Weibo NER	Chinese	LO, ORG, PER, GPE	Chinese social media (Weibo)
CLUENER 2020	–	10 types	
MUC-6	English	LOC, ORG, PER,	Wall Street Journal
ACE	Chinese, Arabic, English	7 types	Broadcast, news, weblogs
KBP2017	English, Chinese, Spanish	GPE, ORG, PER, LOC, FAC	–
GENIA	–	DNA, RNA, Rrotein, Cell line, Cell type categories	Clinical text and biology
WiNER	–	LOC, ORG, PER, MISC	Wikipedia

Depending on the data set selected, the labeling scheme may also have corresponding differences. The labeling scheme is usually distinguished by BIO, BIOS and BIOES. B (Begin) refers to the initial starting position of a named entity. I (Intermediate) refers to the interior of the named entity. E (End) refers to the last end position of the named entity. S (Single) means that only one word or character belongs to a single named entity. O

(Other) means this is not an entity, refers to the outside of an entity. In addition, different named entities also belong to different entity types. For example, LOC (ie location) refers to a geographic location or building location, such as Qiaogori Peak, Jiuzhaigou. PER (Person) refers to the formal or informal name, title and nickname of the real world or virtual character, such as Zhang San, Li Hua, Iron Man, etc. ORG (Organization) refers to the name of an organization with a management system, such as Ali, Baidu, etc. GPE (Geo-political Entity) refers to the geographic name of the region containing government agencies. MISC (Miscellaneous) refers to named entities other than those explicitly specified. As another example, B-GPE indicates the starting location of a geopolitical entity.

2.3 Evaluation Indicators

Judging an evolving NER system requires a comprehensive evaluation of the designed system. Accurate detection of entity boundaries and correct identification of the entity type are the essence of NER tasks. In NER, the F1 value is usually used as a comparison and evaluation criterion. The F1 value refers to the harmonic average of the accuracy (Represented by the letter P) and the recall rate (Represented by the letter R), that is, it can balance the precision rate P and the recall rate R, and get rid of the insufficiency of using only one of them.

$$P = \frac{TP}{TP + FP} \; R = \frac{TP}{TP + FN} \; F1 = 2 \times \frac{P \times R}{P + R} \tag{1}$$

Among them, P represents the percentage of positive examples judged by the model to be correct in all positive examples judged by the model. Discriminated as a correct positive example means that the instance determined by the model as a positive example is also a positive example in the comparison standard, all positive examples judged by the model means that the instance is not necessarily a positive example, but the model considers it to be a positive example. R indicates that the model discriminates as a correct positive example, which accounts for the percentage of all positive examples in fact. Actual all positive examples refer to all positive examples in the discrimination criteria. TP (True Positive): it is recognized as a positive example by the model and is also a positive example in the comparison standard; TN (True Negative): it is recognized as a negative example by the model and is also a negative example in the comparison standard; FP (False Positive): It is recognized by the model It is a positive example but is a negative example in the comparison standard; FN (False Negative): It is recognized as a negative example by the model but it is a positive example in the comparison standard.

3 Resource-Scarce NER

3.1 The Purpose of Studying Scarce Resource NER

In practical scenarios, there are various types of entities, and the corpus used for training may not cover all of them. Collecting new language or new domain data, and manually constructing labels for a large amount of data requires a lot of time, energy, financial resources and manpower, which is not a good way. Therefore, it is necessary to sort out and adjust the model. At the same time, these existing problems have stimulated the research enthusiasm of domestic and foreign scholars for low-resource NER.

3.2 Difficulties

Implementing NER in low-resource domains and languages is often difficult for the following reasons. First, there may be a small number of labeled datasets available for training. The NER model cannot fully learn enough feature information in the small dataset, resulting in the final trained model can only recognize a small number of types of entities, and the effect is far from ideal. Second, there may be problems with the low quality of the data used for training, such as missing labels in the dataset, wrong entity type labeling, etc. Wrong annotations will have a negative effect on the NER system, and the lack of annotations may prevent the system from learning the feature information of certain entity types, and treat them as negative examples during the training process. Finally, there may also be cases where there is no labeled data at all.

3.3 Methods

According to the different ways of model learning and feature acquisition, the NER method in low resource environment is divided into the following three different ways.

NER method based on multi-task learning. When implementing the NER method, the advantage of using multi-task learning to achieve NER is that by sharing the parameters of the side tasks, introducing additional knowledge to the NER model may help it to extract difficult-to-extract features, identify more types of entities, and learn to a wider variety of text generic features. For Chinese NER, the high accuracy of word segmentation is the core premise of the NER task, which is related to the accuracy of the word boundary information judgment. For example, combining the Chinese word segmentation task and integrating the word boundary label information into the NER model can improve the sensitivity of word boundary recognition [45]. Using the explicit feedback strategy, Zhao and Liu et al. [46], who studied in the medical field, processed the normalization task in parallel while clearly dividing the entity boundary to realize the NER task. The two tasks interact with each other, using each other's output to achieve improvements. Liu and Winata et al. [47] split the NER task into an entity discrimination task and an entity type labeling task. The splitting of the task enhances the model's sensitivity to entity judgment. They share the feature extraction layer and add an expert hybrid module. Expert weighted values are used as prediction benchmarks to solve the problem of ambiguous entities that arise.

NER method based on data augmentation. Usually, the data augmentation method can overcome the shortcomings of the model in the problem of few samples to a certain extent. For example, after the samples are screened and the weights are adjusted to improve the quality of the data, the model performance will be improved. Data enhancement methods are often divided into two categories. One is to use the original text without introducing additional label types, and to achieve it by adding replacement words, translation, adversarial enhancement, and syntactic exchange. The other is to introduce additional information, such as using methods such as pre-training of the model. Zhou and Zhang et al. [48] proposed the DATNet method to improve the generalization ability of the model with an adversarial training method. Zhang and Guo et al. [49] added GAN on the basis of using the BiLSTM-Attention-CRF model. Compared with only using the BiLSTM-CRF model, this method utilizes the characteristics of GAN and can filter out the unremarkable ones that are consistent with the distribution of real labeled data features. Label the data so that the training data can be augmented. Ding and Liu et al. [50] took the annotation model and language model as the foothold, the linearization of the sentence sequence can obtain the state distribution of words and their annotation labels, and the language model is used to add available data to flexibly use labeled data and unlabeled data. Zhou and He et al. [51] fine-tune the MLM by processing the labeled data with a linearization operation, and combine the original data with the augmented data generated with MLM to ensure that the augmented data entities match the original data labels. Tsygankova and Marini et al. [52] recruited volunteers who were not proficient in the target language application but proficient in the native language application, and asked them to annotate the set target language to produce additional training data. Liu and Ding et al. [53] used a simple placeholder method to translate the labeled source language data into the target language, transfer its labels to generate new training data, and apply it to the language model for training to generate diverse. The label data is mixed with the original data to achieve the purpose of data expansion (Fig. 2).

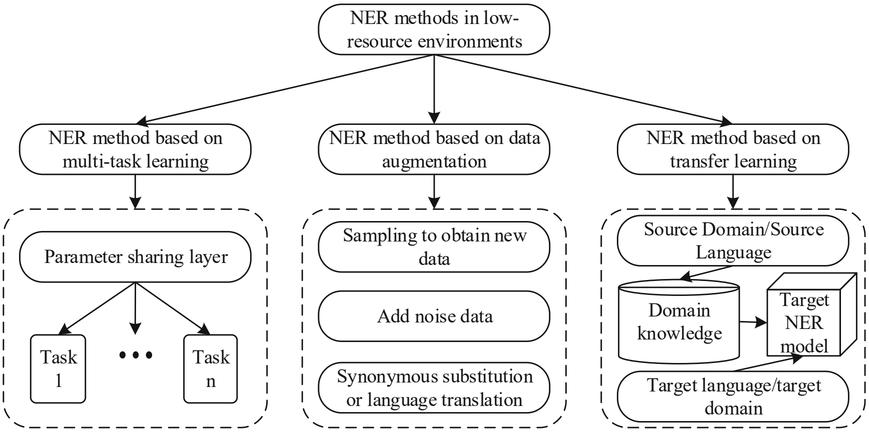

NER methods in low-resource environments
NER method based on multi-task learning
NER method based on data augmentation
NER method based on transfer learning
Parameter sharing layer
Task 1
• • •
Task n
Sampling to obtain new data
Add noise data
Synonymous substitution or language translation
Source Domain/Source Language
Domain knowledge
Target NER model
Target language/target domain

Fig. 2. Three NER methods in low-resource environments.

NER method based on transfer learning. Pang and Yang et al. [54] believe that using the idea of transfer learning, the model can quickly adapt to the target task through the knowledge of the source task that has been learned when dealing with different target tasks. By transferring training modules or knowledge, the recognition of specific entity categories in different domains can be enhanced. Extracting data information from domains that are relevant to the target domain and transferring it into the target model is an effective way to solve the problems of difficult, expensive and inaccessible data collection in the target domain. For the problem that both the source domain/language and the target domain dataset contain labels, the types of labels in the two training data are different, and the target domain data is scarce, the transfer learning method is a good method. For example, Giorgi and Bader [55] migrated the knowledge in the easily accessible silver corpus in the biomedical field where relevant literature and materials were rapidly added, and obtained more reliable information resources (Table 3).

Table 3. Comparison of several different methods in low-resource environment.

Method	Features	Advantages	Challenges
Multi-task learning	Find and utilize relevant information between tasks	Prevention of over-fitting	Poor task relevance will bring negative impact
Based on data augmentation	Can increase the amount of available data	Simpler to use	It is difficult to guarantee the quality and diversity of data
Based on transfer learning	Utilize a large number of existing resources to assist in learning new knowledge	Possesses the ability to enhance model robustness	How to grasp the measure of migration

In cross-language tasks, domain data translation, projection, etc. can be used. Xie and Yang et al. [56] proposed a method based on the combination of continuous embedding and discrete dictionary to realize the relationship mapping between different languages, and used the attention mechanism to solve the problem of the difference in the lexical order between different languages in the cross-lingual NER task. Strengthen the correspondence between synonyms in different languages. Johnson and Karanasou et al. [57] took English as the source language and transferred their trained weights to the target Japanese language. The projection-based method of Chaudhary and Xie et al. [58] maps the label information of the source language into the target language to complete the transfer of language knowledge, using only a small amount of human annotations. Compared with the use of bilingual dictionaries, Bari and Joty et al. [59] achieved the purpose of knowledge transfer through adversarial mapping between different languages and data sharing through pseudo-label-guided training. Wu and Lin et al. [60] trained a multi-corpus NER model, and predicted the target corpus to generate a probability distribution value with rich information as additional auxiliary training information for the target model. Chen and Jiang et al. [61] also used high-quality corpus to train a high-performance model to generate pseudo-labels for the target model, but constructed a discriminator to screen corpus independent of language features for use by the target model, so as to reduce the impact of language features on the model.

4 Development Direction

After the above discussion, it is found that although the research on low resources in this field has been progressing in recent years, there are still many problems that need to be considered and dealt with in practical applications. In this part, we will share and discuss the main challenges in the NER field in low-resource settings and possible future trends.

4.1 Named Entity Recognition Based on Image and Text Fusion

Considering that the domain entity dictionary will help the current target application, it is appropriate to accumulate, build and improve the relevant domain dictionary to improve the performance of the model. It is the key to dig deep into relevant information and embed it perfectly into the model. Make good use of the resources in the current large amount of data, such as integrating the graphical representation of a large number of words into the NER model as additional features to provide richer semantic information.

4.2 More General Named Entity Identification

When the current domain or language training resources are scarce, the data obtained from multi-resource domain training can be used to achieve the required domain entity recognition. Generally, in order to achieve better performance, data from similar domains are often selected for resource data sharing, but this method will also reduce the generality of the target task to a certain extent. How to make the target model not only identify the unique model in the current domain or language according to the auxiliary resources, but also make the model have the generalization ability and facilitate the iterative optimization of the subordinate model when it is used as a subtask is a problem that should be considered in the actual application process.

5 Summary

This survey introduces the basic situation of NER, the existing research results of NER based on deep learning, and the existing implementation methods of NER in the case of few training samples or data lacking labels, and some important opinions are drawn through the analysis. It aims to help researchers quickly and comprehensively understand the development trend of deep learning NER, how to improve NER performance under low resource conditions, and future research trends. The combination of NER and related parties can share relevant information, improve the generalization ability within a certain range, and complement each other to achieve the purpose of improving performance. The increase in the transformation of training samples can obtain more labeled data on the basis of the existing limited labeled data. The transfer of training parameters in similar domains is helpful to improve the performance of the target task and improve the generalization ability.

Acknowledgment. This work was supported by Hainan Provincial Natural Science Foundation of China (Grant No. 620MS021, 621QN211), National Natural Science Foundation of China (NSFC) (Grant No. 62162024, 62162022), the Key Research and Development Program of Hainan Province (Grant No. ZDYF2020040, ZDYF2021GXJS003), the Major science and technology project of Hainan Province (Grant No. ZDKJ2020012), Science and Technology Development Center of the Ministry of Education Industry-university-Research Innovation Fund (2021JQR017), the Key Laboratory of PK System Technologies Research of Hainan.

References

1. Etzioni, O., Cafarella, M., Downey, D., Popescu, A. M., Shaked, T., Soderland, S., Weld, D., S., Yates, A.: Unsupervised named-entity extraction from the Web: An experimental study. Artificial Intelligence. 165.1:91–134(2005)
2. Mollá, D., Van Zaanen, M., Smith, D.: Named entity recognition for question answering. In: Proceedings of the Australasian language technology workshop, pp. 51–58 (2006)
3. Guo, J., Xu, G., Cheng, X., Li, H.: Named entity recognition in query. In: Proceedings of the 32nd international ACM SIGIR conference on Research and development in information retrieval, pp. 267–274 (2009)
4. Ganea, O.E., Hofmann, T.: Deep joint entity disambiguation with local neural attention. In: Proceedings of the 2017 Conference on empirical methods in natural language processing, pp. 2619–2629. Association for Computational Linguistics (2017)
5. Le, P., Titov, I.: Improving entity linking by modeling latent relations between mentions. In: Proceedings of the 56th Annual meeting of the association for computational linguistics, vol. 1, Long Papers, pp. 1595–1604 (2018)
6. Zhang, Z., Han, X., Liu, Z., Jiang, X., Sun, M., Liu, Q.: Ernie: enhanced language representation with informative entities. In: Proceedings of the 57th Annual meeting of the association for computational linguistics (2019)
7. Cheng, P., Erk, K.: Attending to entities for better text understanding. Vol. 34, No. 05, pp. 7554–7561. In: Proceedings of the AAAI conference on artificial intelligence (2020)
8. Nadeau, D., Sekine, S.: A survey of named entity recognition and classification. Lingvisticae Investigationes **30**(1), 3–26 (2007)
9. Marrero, M., Urbano, J., Sánchez-Cuadrado, S., Morato, J., Gómez-Berbís, J.M.: Named entity recognition: fallacies, challenges and opportunities. Comput. Stand. & Interfaces **35**(5), 482–489 (2013)
10. Campos, D., Matos, S., Oliveira, J.L.: Biomedical named entity recognition: a survey of machine-learning tools. Theory Appl. Adv. Text Min. **11**, 175–195 (2012)
11. Alshaikhdeeb, B., Ahmad, K.: Biomedical named entity recognition: a review. Int. J. Adv. Sci., Eng. Inf. Technol. **6**(6), 889–895 (2016)
12. Li, J., Sun, A., Han, J., Li, C.: A survey on deep learning for named entity recognition. IEEE Trans. Knowl. Data Eng. **34**(1), 50–70 (2020)
13. Yadav, V., Bethard, S.: A Survey on Recent Advances in Named Entity Recognition from Deep Learning models. In: Proceedings of the 27th International Conference on Computational Linguistics, pp. 2145–2158 (2018)
14. Gao, C., Zhang, X., Han, M., Liu, H.: A review on cyber security named entity recognition. Front. Inf. Technol. & Electron. Eng. **22**(9), 1153–1168 (2021)
15. Collobert, R., Weston, J., Bottou, L., Karlen, M., Kavukcuoglu, K., Kuksa, P.: Natural language processing (almost) from scratch. J. Mach. Learn. Res. **12**(ARTICLE), 2493–2537 (2011)

16. Passos, A., Kumar, V., McCallum, A.: Lexicon infused phrase embeddings for named entity resolution. In: Proceedings of the eighteenth conference on computational natural language learning, pp. 78–86 (2014)
17. Pennington, J., Socher, R., Manning, C. D.: Glove: Global vectors for word representation. In: Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP), pp. 1532–1543 (2014)
18. Yao, L., Liu, H., Liu, Y., Li, X., Anwar, M.W.: Biomedical named entity recognition based on deep neutral network. Int. J. Hybrid Inf. Technol. **8**(8), 279–288 (2015)
19. Huang, Z., Xu, W., Yu, K.: Bidirectional L1STM-CRF models for sequence tagging. Computer Science (2015)
20. Strubell, E., Verga, P., Belanger, D., McCallum, A.: Fast and accurate entity recognition with iterated dilated convolutions. In: Proceedings of the 2017 Conference on empirical methods in natural language processing, pp. 2670–2680 (2017)
21. Shen, Y., Ma, X., Tan, Z., Zhang, S., Wang, W., Lu, W.: Locate and Label: A Two-stage Identifier for Nested Named Entity Recognition. In: Proceedings of the 59th Annual meeting of the association for computational linguistics and the 11th international joint conference on natural language processing, vol. 1, Long Papers, pp. 2782–2794 (2021)
22. Zheng, X., Chen, H., Xu, T.: Deep learning for chinese word segmentation and pos tagging. In: Proceedings of the 2013 conference on empirical methods in natural language processing, pp. 647–657 (2013)
23. Gillick, D., Brunk, C., Vinyals, O., Subramanya, A.: Multilingual language processing from bytes. In: Proceedings of NAACL-HLT, pp. 1296–1306 (2016)
24. Kim, Y., Jernite, Y., Sontag, D., Rush, A.: Character-aware neural language model, vol. 30, no. 1. In: Proceedings of the AAAI conference on artificial intelligence (2016)
25. Kuru, O., Can, O. A., Yuret, D.: Charner: Character-level named entity recognition. In: Proceedings of COLING 2016, the 26th International conference on computational linguistics: Technical Papers, pp. 911–921 (2016)
26. Dong, C., Zhang, J., Zong, C., Hattori, M., Di, H: Character-based LSTM-CRF with radical-level features for chinese named entity recognition. In Natural Language Understanding and Intelligent Applications, pages 239–250. Springer (2016)
27. Akbik, A., Blythe, D., Vollgraf, R.: Contextual string embeddings for sequence labeling. In: Proceedings of the 27th international conference on computational linguistics, pp. 1638–1649 (2018)
28. Peters, M., Neumann, M., Iyyer, M., Gardner, M., Zettlemoyer, L.: Deep contextualized word representations. (2018)
29. Peters, M.E., Ammar, W., Bhagavatula, C., Power, R.: Semi-supervised sequence tagging with bidirectional language models. In: Proceedings of the 55th Annual meeting of the association for computational linguistics, vol. 1, Long Papers, pp. 1756–1765, Vancouver, Canada, July. Association for Computational Linguistics (2017)
30. Zhu, Y., Wang, G.: CAN-NER: Convolutional attention network for chinese named entity recognition. In: Proceedings of NAACL-HLT, pp. 3384–3393 (2019)
31. Ma, X., Hovy, E.: End-to-end sequence labeling via Bi-directional LSTM-CNNs-CRF. In: Proceedings of the 54th Annual meeting of the association for computational linguistics, vol.1, Long Papers, pp. 1064–1074 (2016)
32. Chiu, J.P., Nichols, E.: Named entity recognition with bidirectional LSTM-CNNs. Trans. Assoc. Comput. Linguist. **4**, 357–370 (2016)
33. Lample, G., Ballesteros, M., Subramanian, S., Kawakami, K., Dyer, C.: Neural Architectures for named entity recognition. In: Proceedings of NAACL-HLT, pp. 260–270 (2016)
34. Bharadwaj, A., Mortensen, D. R., Dyer, C., Carbonell, J. G.: Phonologically aware neural model for named entity recognition in low resource transfer settings. In: Proceedings of the conference on empirical methods in natural language processing, pp. 1462–1472 (2016)

35. Lin, B.Y., Xu, F. F., Luo, Z., Zhu, K.: Multi-channel bilstm-crf model for emerging named entity recognition in social media. In: Proceedings of the 3rd Workshop on Noisy User-generated Text, pp. 160–165 (2017)
36. Gui, T., Zou, Y., Zhang, Q., Peng, M., Fu, J., Wei, Z., Huang, X. J.: A lexicon-based graph neural network for Chinese NER. In: Proceedings of the 2019 Conference on empirical methods in natural language Processing and the 9th International joint conference on natural language processing, pp.1040–1050 (2019)
37. Liu, T., Yao, J. G., Lin, C. Y.: Towards improving neural named entity recognition with gazetteers. In: Proceedings of the 57th annual meeting of the association for computational linguistics, pp. 5301–5307 (2019)
38. Ghaddar, A., Langlais, P: Robust lexical features for improved neural network named-entity recognition. In: Proceedings of the 27th International conference on computational linguistics, pp. 1896–1907 (2018)
39. Zhang, Y., Yang, J.: Chinese NER Using Lattice LSTM. In: Proceedings of the 56th Annual meeting of the association for computational linguistics, vol. 1: Long Papers, pp. 1554–1564 (2018)
40. Cao, P., Chen, Y., Liu, K., Zhao, J., Liu, S.: Adversarial transfer learning for Chinese named entity recognition with self-attention mechanism. In: Proceedings of the 2018 conference on empirical methods in natural language processing, pp. 182–192 (2018)
41. Liu, W., Xu, T., Xu, Q., Song, J., Zu, Y.: An encoding strategy based word-character LSTM for Chinese NER. In: Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, vol. 1. Long and Short Papers. pp. 2379–2389 (2019)
42. Ding, R., Xie, P., Zhang, X., Lu, W., Li, L., Si, L.: A neural multi-digraph model for Chinese NER with gazetteers. In: Proceedings of the 57th Annual meeting of the association for computational linguistics. pp. 1462–1467 (2019)
43. Wu, F., Liu, J., Wu, C., Huang, Y., Xie, X.: Neural Chinese named entity recognition via CNN-LSTM-CRF and joint training with word segmentation. In: The World Wide Web Conference. pp. 3342–3348 (2019)
44. Song, C.H., Sehanobish, A.: Using chinese glyphs for named entity recognition (student abstract). In Proceedings of the AAAI Conference on Artificial Intelligence. **34**(10), 13921–13922 (2020)
45. Peng, N., Dredze, M.: Improving named entity recognition for Chinese social media with word segmentation representation learning. In: Proceedings of the 54th Annual meeting of the association for computational linguistics, vol. 2: Short Papers. pp. 149–155 (2016)
46. Zhao, S., Liu, T., Zhao, S., Wang, F.: A neural multi-task learning framework to jointly model medical named entity recognition and normalization. In Proceedings of the AAAI Conference on Artificial Intelligence. **33**(01), 817–824 (2019)
47. Liu, Z., Winata, G.I., Fung, P.: Zero-resource cross-domain named entity recognition. In: Proceedings of the 5th workshop on representation learning for NLP. pp. 1–6 (2020)
48. Zhou, J.T., Zhang, H., Jin, D., Zhu, H., Fang, M., Goh, R. S. M., Kwok, K.: Dual adversarial neural transfer for low-resource named entity recognition. In: Proceedings of the 57th Annual meeting of the association for computational linguistics, pp. 3461–3471 (2019)
49. Zhang, H., Guo, Y., Li, T.: Domain named entity recognition combining GAN and BiLSTM-attention-CRF. J. Comput. Res. Dev. **56**(9), 1851–1858 (2019)
50. Ding, B., Liu, L., Bing, L., Kruengkrai, C., Nguyen, T. H., Joty, S., Miao, C.: DAGA: Data augmentation with a generation approach for low-resource tagging tasks. In: Proceedings of the 2020 conference on empirical methods in natural language processing, pp. 6045–6057 (2020)

51. Zhou, R., Li, X., He, R., Bing, L., Cambria, E., Si, L., Miao, C.: MELM: Data augmentation with masked entity language modeling for low-resource NER. In: Proceedings of the 60th annual meeting of the association for computational linguistics, vol. 1: Long Papers, pp. 2251–2262 (2022)
52. Tsygankova, T., Marini, F., Mayhew, S., Roth, D.: Building low-resource NER models using non-speaker annotations. In: Proceedings of the second workshop on data science with human in the loop: language advances, pp. 62–69 (2021)
53. Zhou, R., Li, X., He, R., Bing, L., Cambria, E., Si, L.: MulDA: A multilingual data augmentation framework for low-resource cross-lingual NER (2021)
54. Pan, S.J., Yang, Q.: A survey on transfer learning. IEEE Trans. Knowl. Data Eng. **22**(10), 1345–1359 (2010)
55. Giorgi, J.M., Bader, G.D.: Transfer learning for biomedical named entity recognition with neural networks. Bioinform. **34**(23), 4087–4094 (2018)
56. Xie, J., Yang, Z., Neubig, G., Smith, N. A., Carbonell, J. G.: Neural cross-lingual named entity recognition with minimal resources. In: Proceedings of the 2018 Conference on empirical methods in natural language processing. pp. 369–379 (2018)
57. Johnson, A., Karanasou, P., Gaspers, J., Klakow, D.: Cross-lingual transfer learning for Japanese named entity recognition. In: Proceedings of the 2019 conference of the North American Chapter of the association for computational linguistics: Human language technologies, vol. 2. Industry Papers. pp. 182–189 (2019)
58. Chaudhary, A., Xie, J., Sheikh, Z., Neubig, G., Carbonell, J. G.: A little annotation does a lot of good: a study in bootstrapping low-resource named entity recognizers. In: Proceedings of the 2019 conference on empirical methods in natural language processing and the 9th International joint conference on natural language processing. pp. 5164–5174 (2019)
59. Bari, M.S., Joty, S., Jwalapuram, P.: Zero-resource cross-lingual named entity recognition. In Proceedings of the AAAI conference on artificial intelligence. **34**(05), 7415–7423 (2020)
60. Wu, Q., Lin, Z., Karlsson, B. F., Lou, J. G., Huang, B.: Single-/Multi-source cross-lingual NER via teacher-student learning on unlabeled data in target language. (2020)
61. Chen, W., Jiang, H., Wu, Q., Karlsson, B., Guan, Y.: AdvPicker: Effectively leveraging Unlabeled data via adversarial discriminator for cross-lingual NER (2021)

Health Big Data Analysis Based on Visualization and Prediction Techniques

Jinhai Li(✉), Jia Xu, and Mengfan Zhang

Taizhou University, Taizhou 225300, China
ljh-hk@163.com

Abstract. With the expansion of population and the increase of infectious diseases, more and more attention has been paid to the investment in public health. In the context of big data, the medical industry has produced a large amount of structured and unstructured data, which is difficult to directly serve the public health field. Visualization technology conveys and communicates information clearly, quickly and effectively with the help of graphical means. At the same time, it can also assist users to make corresponding judgments and better understand the value behind the data. Therefore, this paper uses web crawler technology to collect public health information of microblog as experimental data, uses visualization technology to sort out and analyze the data, shows the real valuable data, and completes the establishment of public health infectious disease prediction model. Finally, it puts forward countermeasures and suggestions for the development of public health, so as to improve the ability of public health managers to detect early warning signals of infectious diseases, to track and respond to the epidemic situation of infectious diseases, to manage the large-scale outbreak of infectious diseases, and to complete the reasonable allocation of health and medical and health resources.

Keywords: Public health system · Health big data · Data visualization · Prediction model · Disease early warning

1 Introduction

In recent 20 years, the total population of China continues to grow, which makes the medical demand rise in recent years. The expansion of population has brought about a high risk of infectious diseases, infectious diseases have the characteristics of wide prevalence, high cost, long course of disease and high mortality, and they cause far more medical needs than other diseases. The increasing medical needs has led to the difficulty of seeing a doctor and the low efficiency of medical services. To cope with these problems, efficient medical services need to be provided.

The use of heath big data can improve the efficiency of medical services. With the rise of information technology such as Internet, Internet of Things and cloud computing, data visualization technology has been widely applied in various fields, as an indispensable means and tool for big data analysis, such as medicine, aerospace, basic physics and

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 261–270, 2024.
https://doi.org/10.1007/978-981-99-7161-9_20

other subjects. The theory of visualization was introduced into China in the 1970s and began to flourish in 2000 [1]. Visualization analysis is characterized by presenting big data in an intuitive graphical way. It is an organic integration of human brain and machine intelligence to mine the hidden information behind data by using the perception ability of human eyes and convert it into knowledge [2]. Among them, in the medical field, the application prospect of visualization technology is very broad, which often leads to intense research and discussion.

Under the influence of global scale, health big data has risen to become an important strategic resource for the country. Visualization research on health big data can not only improve medical efficiency and the overall level of medical treatment, but also better improve the comprehensive national strength of a country.

In the era of big data, data visualization technology promotes the development of many scientific fields and all walks of life, but also brings unprecedented challenges. The generation and flow of information are changeable, it accumulates into an ocean of redundant data, and humans generate more data than traditional processing tools can handle [3]. At present, the application status of data visualization in medical field is not optimistic and there are many problems to be solved urgently, such as the application range needs to be expanded, the data is difficult to share, and the complete theoretical system has not been formed. The characteristics of health big data itself also pose more urgent requirements and severe challenges to visualization analysis. Therefore, the research on health big data visualization technology becomes particularly critical. Health big data visualization is by far the most effective tool to solve the complex medical data and the increasing demand for medical treatment. With the help of this technology, functions such as assisting clinical diagnosis, mining data value and predicting disease development trend can be realized, thus promoting the continuous progress of modern intelligent medical technology under the background of big data. This paper guides the formulation of health policy or clinical practice by studying the application status of data visualization technology in public health data and the analysis of potential health influencing factors. It has important theoretical significance and application value for health management and health monitoring.

2 Relevant Theoretical Analysis

The application of big data analysis technology in the health care field has promoted the integration of medical big data, improved the medical level of hospitals and reduced the medical risks of patients. Medical big data has become a strategic industry in many countries and gradually developed into a national strategy.

Although the state strongly advocates and actively guides the use of technology concept of health care big data to solve the key and difficult problems in the health care field, there are still many bottleneck problems that are difficult to break through at present. How to quickly acquire and structure the data is an urgent problem for public health research at present [4].

Based on the urgency of health care big data research, in recent years, domestic and foreign scholars have carried out extensive research on health care big data from multiple aspects. Wang Ruojia et al. from the computer technology level, comprehensively analyze the application status of data mining technology in assisting to complete medical tasks, managing medical resources reasonably, improving health information services, and put forward the cooperative development direction in the fields of diversified data sources, semantic mining of electronic medical records, cloud computing and artificial intelligence [5]. From the perspective of personal privacy security, Tong Feng et al. sort out the current situation of personal information protection in China and relevant laws in the United States and The European Union, and they put forward relevant suggestions on the legislative protection of personal health care information in China [6].

In order to show how health big data analysis can realize precision medicine, Wu et al. provide two case studies, including identifying disease biomarkers from multiple sets of data and incorporating basic data information into electronic medical records, which provides support for the paradigm shift of precision medicine [7]. Rehman et al. discuss the application of health big data analysis in the healthcare industry, mainly including medical image analysis and image informatics, bioinformatics, clinical informatics, public health informatics and medical signal analysis [8].

In addition, in the field of visualization of health big data, Ahlbrandt et al. analyzed based on visualization technology and proposed the balance between the need for big data and patient data privacy—an IT infrastructure for a decentralized emergency care research database [9]. Lupse et al. analyzed based on visualization technology and elaborated the supporting diagnosis and treatment in medical care based on big data processing [10].

Relatively speaking, the development history of health care big data in China is short, lacking a continuous and systematic health data integration platform. As the research on health care big data spans two disciplines of medicine and computer, it is necessary to cultivate interdisciplinary talents. Moreover, health care data has many problems, such as privacy security and information island, making it difficult to carry out further research. At present, relevant work is mainly focused on theoretical research, including the discussion on the characteristics and application scenarios of health care big data. In terms of technological breakthroughs, most of the work is only in data collection and storage, and there are still relatively few substantive researches on the basic aspects of deep mining, data relationship analysis and visualization technology of health care big data itself.

3 Health Big Data Acquisition of Infectious Diseases Based on Crawlers

3.1 Data Analysis Process

Health big data analysis based on visualization technology can be divided into three stages:

STEP1 Python crawler, firstly determine the collected data, give the keyword “infectious disease”, use the articles about infectious disease information published by users on microblog to analyze and predict the outbreak of infectious diseases.
STEP2 Clean the data that has been captured to make data format more standardized.

STEP3 Use the data visualization related library pyecharts etc. to do data visualization analysis. Through a series of analyses, the distribution of infectious diseases in Chinese population can be found, which further provides data support for the public health security prediction model below.

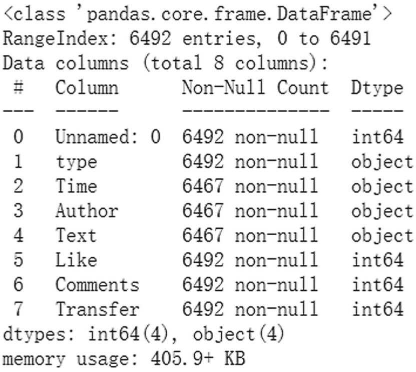
3.2 Data Preprocessing

Firstly, determine six statistical data of related tweets on microblog: blogger id, tweet content, publication time, the number of transfers, the number of comments and the number of like. The crawler technology was used to crawl the experimental data.

The data collected from websites are usually inconsistent, incomplete and disorderly, with many unnecessary spaces and some labels, which cannot be directly visualized for data analysis. To improve data aesthetics and visual quality, we used pandas library to filter web pages.

Firstly, call pd.read_csv() method to open info.csv file, and use for loop to iterate through the data in the file in turn. The nested if() expression was used to determine whether there are spaces, and the try except syntax was used to handle exceptions. When it fails to work properly, the exception is caught and saved as an empty string. The second time we used the for loop to count the numbers by field, and when the number is less than 2 in if () expression, the loop ends and the data is discarded.

Then call dropna() method to delete the missing data. Finally, use info command to check the number of non-null values and data types of each column. It can be seen that the total number was 6492, after data cleaning, the data of publication time, author, like, transfer and comments were reduced. Data statistics after data cleaning are shown in Fig. 1.



```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 6492 entries, 0 to 6491
Data columns (total 8 columns):
 #   Column      Non-Null Count  Dtype
---  ------      --------------  -----
 0   Unnamed: 0  6492 non-null   int64
 1   type        6492 non-null   object
 2   Time        6467 non-null   object
 3   Author      6467 non-null   object
 4   Text        6467 non-null   object
 5   Like        6492 non-null   int64
 6   Comments    6492 non-null   int64
 7   Transfer    6492 non-null   int64
dtypes: int64(4), object(4)
memory usage: 405.9+ KB
```

Fig. 1. The figure of data cleaning analysis

It can be seen that the data is no longer messy, valuable data is extracted, invalid numbers and letters are cleaned out, which is conducive to the following data visualization.

4 Visualization Analysis Based on Health Big Data

4.1 Experimental Data

This paper used the keyword “infectious disease” to filter the data, and after data reprocessing, 6492 data were included in total. The data were classified according to type, Time, Author, Text, Like, Comments and Transfer lists, corresponding to the type of infectious diseases, time, author, specific information, number of like, number of comments and number of transfer respectively.

4.2 Visual Graphic Design

If we only do data crawling without visual processing, the real value of the data cannot be played, and the data can be more intuitive and clearer after visual processing, which is more conducive to data analysis. Four visualization analysis methods have been designed: time series scatter chart and scatter chart.

On the basis of experimental data, we carried out data visualization analysis on the distribution and prevention of infectious diseases. Numpy and pyecharts libraries were used for data visualization.

4.2.1 Time Series Scatter Chart Analysis

Time trend linear graph visualizes the number of tweets for different diseases from time dimension. The horizontal axis shows time, from 2012 to 2021, the vertical axis shows the number of diseases during that time, and different colors show different types of infectious diseases. The time trend of infectious diseases is shown in Fig. 2.

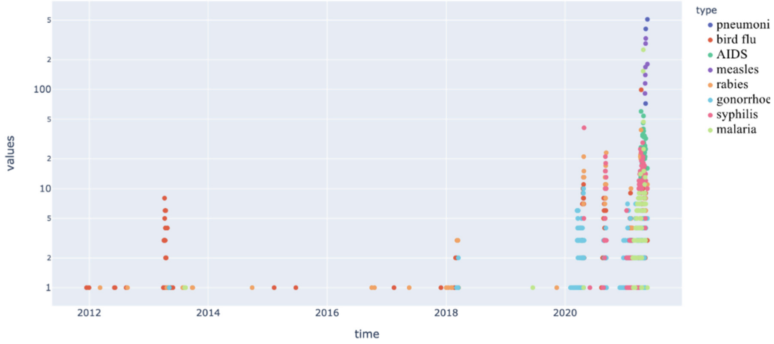


Fig. 2. Time series scatter chart

As we can see from the graph, the distribution of pneumonia first appeared in 2021 and was most discussed, we can infer that 2021 will be the year of a severe outbreak of COVID-19. Rabies emerged in 2012 and has been a chronic infectious disease ever since. Throughout history, people have a strong prevention awareness of AIDS. The large-scale outbreak of infectious diseases in recent two years may be related to the poor social living environment after the improvement of living standards.

4.2.2 Scatter Chart Analysis

Use scatter chart to judge the relationship between the like and comments. Use data values as x and y coordinates to plot points, and axes define areas of the chart. Different colors represent different types of diseases, and graphs are drawn based on values. The more data a scatter chart contains, the better the comparison. Scatter charts are especially useful when there exist a large number of data points, allowing us to see the distribution of the data and what problems might arise. As the x-coordinate is increasing, the y-coordinate is increasing, so it's a positive correlation, and we can probably see that the scatter is on a straight line. The scatter chart is shown in Fig. 3.

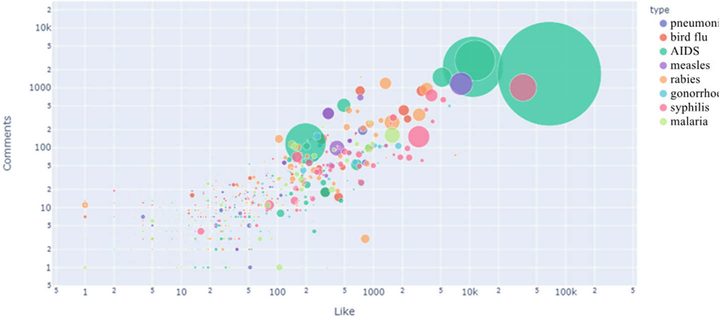


Fig. 3. Scatter chart

4.2.3 Pie Chart Analysis

As can be seen from the pie chart of transfer distribution in Fig. 4, in microblog tweets about infectious diseases, 62.57% of the users transfer the microblog about AIDS, accounting for the largest proportion, indicating that the public has a strong prevention awareness of AIDS. The users transfer the microblog about gonorrhoea topic accounts for the least proportion, only 1.78%, indicating that the public attention to gonorrhoea is low. The pie chart of comments distribution and the pie chart of like distribution can be visualized in the same way.

5 Establishment of Public Health Infectious Disease Prediction Model

5.1 Principles and Methods of the Model

There are thousands of machine learning methods. What type of model and method should be usen is based on the size of the data set and the complexity of the problem itself. For general complex problems, simple models may also obtain the optimal solution. The machine learning methods involved in the comparison include: Naive Bayes, SVM, GBDT, RF, KNN. Take GBDT as an example.

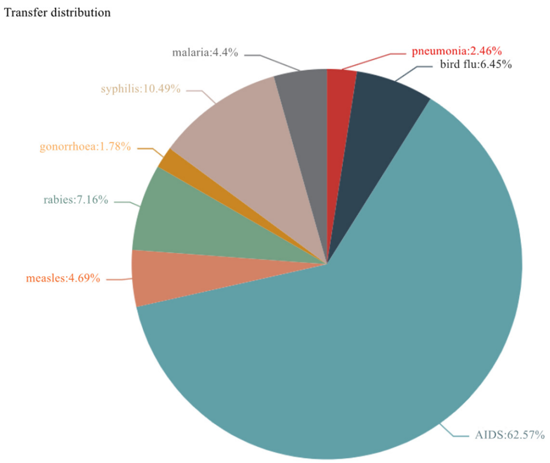


Fig. 4. Pie chart of transfer distribution

GBDT, full name Gradient Boosting Decision Tree, is one of the best machine learning algorithms for real distribution fitting effect. It adopts the addition model to continuously reduce the difference generated in the training process, which can be used for classification and regression. The training process of GBDT is shown in Fig. 5.

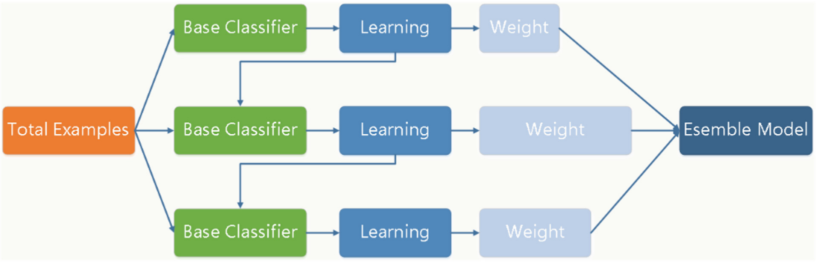


Fig. 5. Training process of GBDT

5.2 Model Construction

5.2.1 Design of Naive Bayes Model

Use Naive Bayes to train and verify, the design idea is to do the disease prediction by randomly selecting a tweet on microblog, so as to get disease type results correctly. This paper used sklearn library and called NB model to train and predict.

First load the sklearn library, use train_test_split to split the data into training sets and test sets, use TfidfVectorizer to generate the TFIDF matrix of article words, and use the NB model of MultinomialNB—sklearn.

Secondly, divide the data set. Read the article data set after word segmentation, load the words and label list, and shred through train_test_split in a 4:1 ratio, that is 80%

training set and 20% test set. Feature extraction is carried out to facilitate the classification of the later algorithm.

Next, vectorize the sliced training set and use TfidfVectorizer to find the tfidf of the words in the article and construct the word vector. MultinomialNB model was then used to train the vector data of the training set, and the TfidfVectorizer and MultinomialNB model were saved.

Finally, read text data from the test set, use jieba to cut Chinese text into words. Because Chinese word segmentation has great ambiguity in different contexts, word segmentation is essential. Remove stop-words and separate the word segmentation results with spaces. TfidfVectorizer model was used to construct the vector space of the test, then put it into MultinomialNB model to predict. Use the established model to make bayesian prediction of species to see which category the disease mentioned in this microblog article belongs to. Visualization through plt.show() function, the predicted result under the operation of jupyter belonged to “pneumonia” category.

The construction and application of SVM model, GBDT model, RF model and KNN model are similar to the principle of Naive Bayes model, which will not be described one by one.

5.3 Model Results and Analysis

Establish a variety of models. Accuracy, precision, recall and F1 are commonly used to measure the quality of a model.

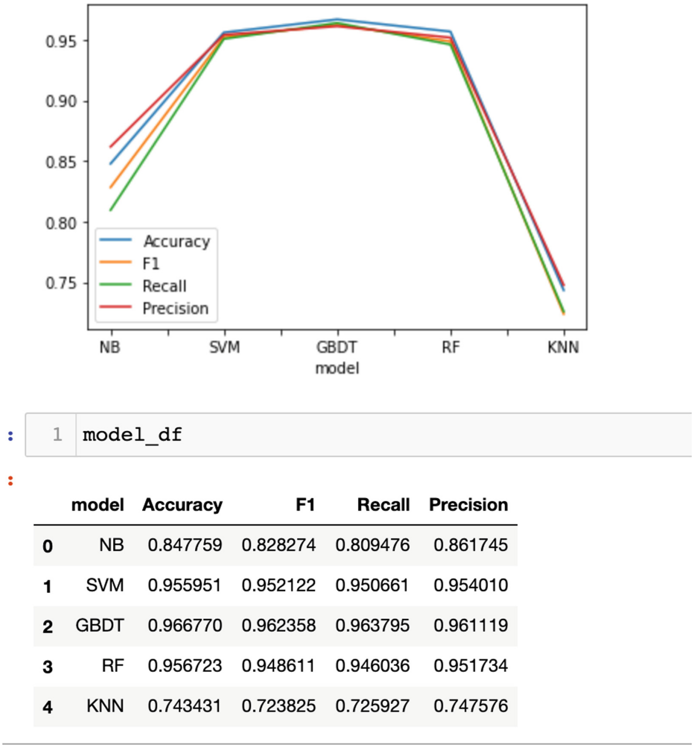
Parameters are constantly adjusted to make the model as optimal as possible. The comparative analysis of various models is shown in Fig. 6.

The final results are as follows: the accuracy of NB model is 0.861745, SVM model is 0.954010, GBDT model is 0.961119, the accuracy is amazing, RF model is 0.951734, KNN model is 0.747576. In terms of accuracy, GBDT has the best effect, while KNN has the worst. In general, recall rate and accuracy rate are mutually restrictive, low accuracy rate means high recall rate, low recall rate means high accuracy rate, and a balance point should be found according to the actual application situation. In this paper, GBDT model is recommended for disease prediction to improve recall rate under the condition of ensuring accuracy.

The construction of public health security prediction GBDT model can give play to the application of health big data in disease prediction and prevention, evidence-based public health decision-making, health management, health monitoring and other aspects, and better promote the positive guiding role of big data in the medical field.

6 Conclusion

In the era of big data, medical informatization develops rapidly. The generation and flow of information are changeable, it accumulates into an ocean of redundant data. At present, the application of data visualization in medical field is not optimistic and there are many problems. In general, the following work has been completed: some data of public health infectious diseases have been obtained through python web crawler, and the obtained data have been analyzed visually; the obtained data and results have been analyzed to build a public health security prediction model.



```
model_df
```

	model	Accuracy	F1	Recall	Precision
0	NB	0.847759	0.828274	0.809476	0.861745
1	SVM	0.955951	0.952122	0.950661	0.954010
2	GBDT	0.966770	0.962358	0.963795	0.961119
3	RF	0.956723	0.948611	0.946036	0.951734
4	KNN	0.743431	0.723825	0.725927	0.747576

Fig. 6. Comparative analysis of various models

This paper only makes a simple analysis of infectious disease data in public security, and other factors threatening population health, such as chronic non-communicable diseases, are not studied in depth, which has certain limitations. This paper uses infectious disease information on microblog as experimental data, privacy information such as the location of microblog users could not be obtained. Population location information is helpful to understand the behavior of infectious diseases. Through spatial visualization of case data, we can try to analyze the clues to the source of infectious diseases and their geographical connections. However, the geographical location of microblog users is difficult to parse, and JS mixed in HTML is not put out separately. In addition, the publication of location information involves personal privacy security, so this experiment is stopped here. Moreover, this paper only selects the distribution and prevention data of infectious diseases to analyze public health security, and there are gaps in experimental data and data analysis. With the development and improvement of Internet technology and the interconnection of everything, it is reasonable to believe that the application prospect of health big data in the medical industry is very broad and worthy of further research.

Acknowledgments. This work was supported by the Social Development Program Project Supported by Science and Technology of Taizhou (TS202032), the "Qinglan Project" of Jiangsu Universities, the Yangzhou Science and Technology Planning Project (YZ2022063), and the Scientific Research Foundation of Taizhou University (QD2016036).

References

1. Xu, Q., Huang, Z., Cai, J., et al.: Visualization of medical data based on big data research. Chin. J. Health Stat. **34**(02), 347–349 (2017)
2. Shen, E.: Big data visualization technology and applications. Big Data Vis Technol Appl **38**(03), 68–83 (2020)
3. Meng, R., Luo, Y., Yu, C., et al.: Application and challenges of healthy big data in the field of public health. Chin. Gen. Pract. **18**(35), 4388–4392 (2015)
4. Yu, M., Zhang, N., Li, Y.: The key technologies and decision support of big data analytics in healthcare. Forum Sci. Technol. China **11**, 53–62 (2018)
5. Wang, R., Wei, S., Zhao, Y., et al.: Review of data mining techniques' application in medical and healthcare field. Doc. Inf. Knowl. **185**(05), 114–123 (2018)
6. Tong, F., Zhang, X., Liu, J.: Legislative protection of personal health and medical information in the era of big data. Inf. Doc. Serv. **41**(03), 107–114 (2020)
7. Wu, P.Y., Cheng, C.W., Kaddi, C.D., et al.: Omic and electronic health record big data analytics for precision medicine. IEEE Trans. Biomed. Eng. **64**(2), 263–273 (2017)
8. Rehman, A., Naz, S., Razzak, I.: Leveraging big data analytics in healthcare enhancement: trends, challenges and opportunities. Multimed. Syst. **1**, 1–33 (2021)
9. Ahlbrandt, J., Brammen, D., Majeed, R.W., et al.: Balancing the need for big data and patient data privacy—An IT infrastructure for a decentralized emergency care research database. Stud. Health Technol. Inform. **205**, 750–754 (2014)
10. Lupşe, O.S., Crişan-Vida, M., Stoicu-Tivadar, L., et al.: Supporting diagnosis and treatment in medical care based on big data processing. Stud. Health Technol. Inform. **197**, 65–69 (2014)

Dual-Layer FL and Blockchain Empowered High Accurate Edge Training Framework

Xinyan Wang(✉), An Hu, Jingli Jia, Jiacheng Du, Yongjie Ning, and Ying Zhu

The State Grid Henan Information & Telecommunication Company (Data Center), Zhengzhou, Henan, China
lzhan2018@163.com

Abstract. With the popularization of the smart city and the explosion of vehicles, the emergence of large amounts of data has boosted research. Distributed machine learning (DML) is an effective solution to improve the accuracy and timeliness. However, schemes based on traditional DML have the problems of high network delay, vehicle privacy leakage, and falling to provide customized models for multiple users. To solve the above problems, this paper constructs a dual-layer federated learning and blockchain-empowered high-accuracy edge training (DFLB-ET) framework for assisted driving. First of all, a dual-layer semi-asynchronous federated learning (FL) mechanism based on blockchain and local Directed Acyclic Graph are proposed to improve the efficiency and accuracy of FL and achieve high-accuracy model sharing among edge servers. Secondly, a regional node selection algorithm is proposed based on the mobility and model accuracy of vehicles, so as to better utilize the computational resources of Road-Side Units. Simulation results show that the proposed DFLB-ET framework outperforms both the local training and synchronous/asynchronous FL schemes in terms of the training delay and model accuracy.

Keywords: Smart city · Machine learning · Blockchain · Federated learning

1 Introduction

In the smart city, machine learning (ML) is often used for providing intelligent and accurate traffic services. Recently, a good number of researchers analyze and train driving data to predict driving behavior [1]. Distributed machine learning (DML) uses multiple computing nodes for model training and computes in parallel. Therefore, it can solve the congestion problem of centralized training. With the increasing demand for computing resources in smart cities, the traditional DML techniques require the frequent exchange of gradients and model parameters, which leads to excessive network traffic and high communication overhead [2]. Actually, different types of vehicles have different characteristics, such as prior right-of-way and maximum weight/height.

FL is designed to carry out efficient machine learning among multi-computing nodes on the premise of guaranteeing the privacy of terminal data and personal data. Some studies use mobile edge computing (MEC) to move cloud services to Road-Side Units

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 271–283, 2024.
https://doi.org/10.1007/978-981-99-7161-9_21

(RSUs), providing communication, computing, storage, and data resources for vehicles and ensuring high bandwidth connections. Furthermore, RSUs can help FL to perform peer-to-peer model aggregation and improve the training efficiency.

There are two main types of FL mechanisms, including synchronous FL and asynchronous FL. In synchronous FL, after the parameter server receives local models from all data owners (workers), the coordinator aggregates these local models into an updated global model. While in asynchronous FL, the coordinator performs a global update after receiving the local model from any data owner, and then sends the updated global model back to all workers.

At present, many FL researches mainly focus on improving security and efficiency. Wu et al. [2] proposed a multi-layer FL protocol called HybridFL to design different aggregation strategies for edge aggregation and cloud aggregation to improve the process of federated learning training. VerifyNet [3] is a privacy-preserving and verifiable FL framework that secures data through a double-masking protocol. Many schemes [4, 5] considered synchronous FL, which significantly increases the waiting time for the nodes that finish training early before synchronous aggregation. While, some work has investigated asynchronous learning mechanisms. For example, the author of [6] proposed an asynchronous small-batch algorithm to address the issue of idle waiting for heterogeneous terminals. Lu [7] proposed an asynchronous FL scheme to guarantee user privacy while improving training efficiency. To further reduce the communication cost and increase the accuracy of FL model, previous research has focused on FL performance optimization though training node selection. Chen [8] jointly optimized the wireless resource allocation and worker selection to minimize the FL loss function. FedTrace [9] clustered the training traces to select nodes with similar data distribution, thus to solve the problem of data heterogeneity at different nodes.

Besides, FL security issues during the transmission of model parameters also remain unresolved. Lu et al. [10] considered a data-sharing scheme for asynchronous FL based on Directed Acyclic Graph (DAG) and blockchain. A two-layer blockchain architecture for FL is proposed to improve blockchain efficiency [11], which has two types of blockchains: the local model update chain and the global model update chain. Therefore, we use blockchain to store model parameters, and transmit model parameters through consensus process.

Therefore, this paper designs a dual-layer federated learning and blockchain-empowered high-accuracy edge training framework for assisted driving services, where the local training data and training capability of each terminal are fully utilized. And the security of data sharing can be ensured through blockchain.

2 System Model

2.1 Network Architecture

In Fig. 1, a dual-layer FL and blockchain-empowered high-accuracy edge training framework is proposed, which uses a semi-asynchronous FL approach for training. In the secondary layer, vehicles are divided into subregion sets by a regional node selection algorithm. Each subregion has an RSU for local model training, and the local model is transmitted between the RSU and vehicles via blockchain. In the primary layer, RSUs collect all the local aggregation model parameters through the blockchain and aggregate them peer-to-peer to obtain a weighted global model according to trust values.

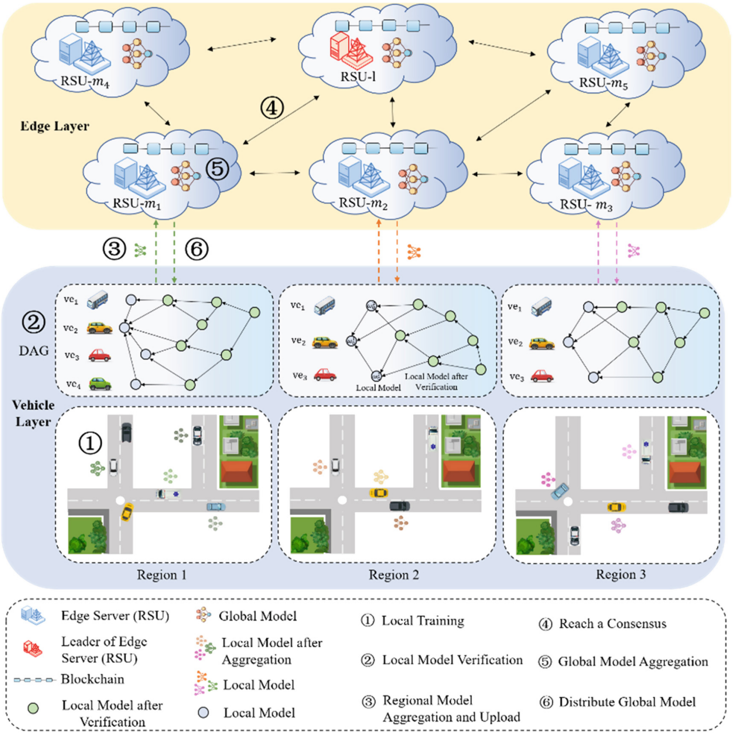

RSU-m_4
RSU-l
RSU-m_5
Edge Layer
④
RSU-m_1
⑤
RSU-m_2
RSU- m_3
③
⑥
②
DAG
ve1
ve2
ve3
ve4
Local Model after Verification
Local Model
Vehicle Layer
①
Region 1
Region 2
Region 3
Edge Server (RSU)
Leader of Edge Server (RSU)
Blockchain
Local Model after Verification
Global Model
Local Model after Aggregation
Local Model
Local Model
① Local Training
② Local Model Verification
③ Regional Model Aggregation and Upload
④ Reach a Consensus
⑤ Global Model Aggregation
⑥ Distribute Global Model

Fig. 1. Network architecture.

2.2 Delay Model

2.2.1 Initial Model Download Delay

When the vehicle is traveling at normal speed, the data transmission rate between vehicle and RSU can be obtained by the Shannon formula:

$$U_{i,j} = \omega_{i,j} log_2 \left\{ 1 + \frac{p_{i,j} g_{i,j} (d_n)^{-\theta}}{\sigma^2} \right\}, \tag{1}$$

$$d_n = \sqrt{h_n^2 + (d/2 - l_i - v_n t)^2}, \tag{2}$$

where $\omega_{i,j}$ and $g_{i,j}$ are the channel bandwidth and channel gain between vehicle i and RSU j, respectively. $p_{i,j}$ represents the transmission power, σ^2 represents the background noise power, d_n is the distance between the vehicle and RSU, h_n is the height of RSU, l_i is the initial position of vehicle i, and d is the range length of RSU.

Assuming that the initial model data volume downloaded by vehicle i from RSU j via vehicle to roadside unit (V2R) communication is $D_{\mathrm{mod\ el},j}$ (in bits), the time taken can be expressed as:

$$T_{download,i} = \frac{D_{\mathrm{mod\ el},j}}{U_{i,j}}. \tag{3}$$

(1) Local model training delay

Considering the delay of the local model training:

$$T_{train,i} = \frac{D_{m,i} X_{\mathrm{mod}\ el}}{g_i}, \tag{4}$$

where X_{model} is the number of CPU cycles required to train model m on unit data, and g_i is the computing power of vehicle i.

Queuing delay

Queuing delay is waiting time for tasks in the task buffer before transmission. Assume that the total number of CPU cycles to be processed is Q_i^t. Then the queuing delay can be calculated by the following formula:

$$T_{queue,i} = \frac{Q_i^t}{g_i}. \tag{5}$$

Local model upload delay

Assuming that the amount of model data from vehicle i to RSU j via V2R communication is $D_{i,\ \mathrm{mod}\ el}$ (in bits), the time spent can be expressed as:

$$T_{upload,i} = \frac{D_{i,\ \mathrm{mod}\ el}}{R_{i,j}}. \tag{6}$$

Therefore, the total delay can be expressed as:

$$\begin{aligned} T_{tot,i} &= T_{download,i} + T_{train,i} + T_{queue,i} + T_{upload,i} \\ &= \frac{D_{\mathrm{mod}\ el,j}}{U_{i,j}} + \frac{D_i^r X_{\mathrm{mod}\ el}}{g_i} + \frac{Q_i^t}{g_i} + \frac{D_{i,\ \mathrm{mod}\ el}}{U_{i,j}}. \end{aligned} \tag{7}$$

3 Dual-Layer Semi-Asynchronous FL Based on DAG and Blockchain

In the FL network, both the vehicle and edge server (RSU) participate in federated learning training. The vehicle node is responsible for local model training and regional model aggregation. The vehicle node transmits the local model to the RSU node in the same region through the consensus mechanism, and the RSU node is responsible for global model aggregation.

3.1 Local Model Training Process

Vehicle nodes use the DAG structure to train local models, and each local model is recorded as a TIP in the DAG. The vehicle node needs to verify the legitimacy of the two TIPs in the DAG by computing the accuracy of its model, then it can add new transactions and broadcast in DAG.

To speed up the aggregation process, the model parameters of vehicle nodes with longer training time, more computing resources, and greater contribution to model training are given higher weights.

The weight of each transaction is proportional to the vehicle computing resources and the accuracy of the model. So, it can be expressed as:

$$\Upsilon(tr_i(t)) = \frac{|d_i| + \varepsilon \cdot \sum_s d_{tr_s}}{\sum_{i=1}^{N} |d_i| + \sum_s d_{tr_s}} \cdot e_i \cdot Acc(tr_i(t)), \tag{8}$$

where $\sum_s d_{tr_s}$ indicates the size of the total data volume of the vehicles submitted to the transaction for regional aggregation, e_i is the duration of the training, and $Acc(tr_i(t))$ is the model accuracy.

Then we calculate the cumulative weight of the transaction:

$$CW(tr_i(t)) = \Upsilon(tr_i(t)) + \frac{1}{L}\sum_{l=1}^{L} \Delta Acc(tr_i(l)) \cdot \Upsilon(tr_i(l)), \tag{9}$$

where $\Delta Acc(tr_i(l)) = Acc(tr_i(l)) - \Upsilon(tr_i(l))$, and L is the number of transactions submitted by other vehicles before the submission of transaction $tr_i(t)$.

Assume that the regional aggregation model of the vehicle stored in the TIPs is expressed as ω. Thus, the regional aggregation model trained by the vehicle V_i on the round t can be expressed as ω_i^t. For V_i in FL iteration starting from t_0, we choose φ TIPs (which have k local model). The vehicle uses its test data set to calculate the accuracy of the model and then obtains the cumulative transaction weight. Vehicle V_i selects some transactions whose number is lower than φ for aggregation and obtains a local model:

$$\omega^{t_0} = \sum_{i=1}^{\varphi} cw(tr_i(t))_i w_{v_i}^{t_i}. \tag{10}$$

3.2 Regional Model Aggregation

The overall process of semi-asynchronous federated learning mechanism is shown in Fig. 2.

The vehicle i acquires the model parameters of other vehicle training through DAG for regional aggregation. By using random gradient descents, the weight and gradient of the model under the specified data can be calculated. The loss function of vehicle i during local training is defined as the difference between its predicted value and actual value on the sample data set $d_{m,i}$, expressed as

$$F_{m,i}(\omega') \triangleq \frac{1}{d_{m,i}} f(\omega';), \tag{11}$$

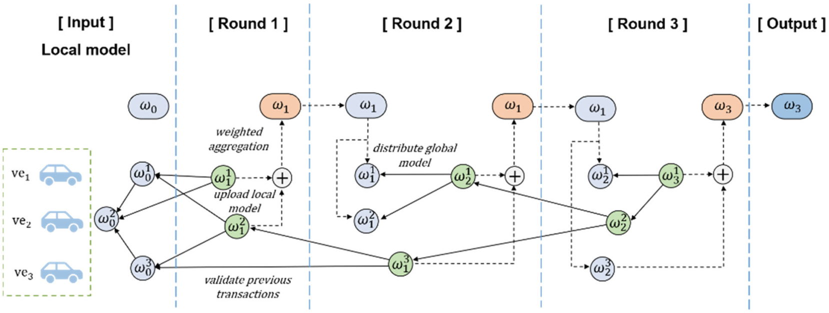


Fig. 2. Semi-asynchronous federated learning process.

where ω' is a parameter vector and $f(.)$ is a user-specified loss function such as linear regression, logistic regression, and support vector machine.

The loss function of assisted driving model FL task of ve$_m$ models on all datasets can be defined as:

$$F_m(\omega') \triangleq \frac{1}{|D_m|} \sum_{i \in ve_m} f(\omega'; d_{m,i}). \tag{12}$$

The goal of FL is to find the optimal parameter vector to minimize the loss function, that is:

$$\omega^* = \arg \min_{\omega} F_m(\omega'). \tag{13}$$

After vehicle i trains the model based on local data $\mathrm{D}_{m,i}$, the updates of the model parameters can be expressed as:

$$\omega'_{k+1} = \omega'_k - \eta \nabla F(\omega'_k). \tag{14}$$

3.3 Regional Node Selection Algorithm

The different number of regional aggregation rounds (i.e., Y) and the number of vehicles involved in global aggregation (i.e., Z) can lead to a different performance in terms of communication resource consumption and time consumption. Therefore, we need to determine the optimal value of Y and Z to balance the total training delay and the final accuracy of the model. The problem is expressed as follows:

$$\begin{aligned} &\mathrm{P2}: \min(\chi \sum_{k=1}^{K} t_k + \delta(1 - Acc)) \\ &s.t \quad C1: F_m(\omega_\psi) - F_m(\omega^*) \le \varepsilon, \\ &\qquad\; C2: Y \in \{1, 2, ..., N_{m,r}\} \\ &\qquad\; C3: Z \in \{1, 2, ..., N_{m,r}\} \end{aligned} \tag{15}$$

where constraint C1 indicates that the global model converges after ψ rounds, and constraints C2 and C3 ensure that the values of Y and Z are taken reasonably.

ALGORITHM 1: A3C-based node selection

```
Initialization:
    The number of local iterations $t$, the maximum length of single iteration time series in a thread $t_{\max}$, the number $W$ of agents.
Iteration:
1.  RSU collects the information on all vehicles and obtains
    the initial state $\boldsymbol{S}(t) \triangleq \{\boldsymbol{C_s}(t)\}$
2.  For $\omega = 1$ to $W$ do
3.      $t_0 = t$
4.      Perform actions based on policy $\pi(a(t_0) \mid s(t_0); \theta)$
5.      Get a reward $r_s$ and the next state $s(t_0 + 1)$
6.      If $s_t$ is in the termination state, or $t - t_0 = t_{\max}$,
7.          Go to step 4
8.      End
9.      Update the gradient of the actor's local network and
        the critic's local network
10. End
11. Update the model parameters
Output: node selection result
```

3.4 Delay-Accuracy-Balancing Factor-Based Aggregation Mechanism

The total delay consists of the local training time and regional aggregation time, due to the global aggregation only contains linear operations, the training time can be ignored. Therefore, the model preparation time T^p and regional aggregation time T^a are considered. Model preparation time is defined as the average duration from the time the global model is distributed to vehicle i from RSU to the end of training and uploaded to the DAG. We define regional aggregation time as the average duration between model uploading to the DAG and uploading the regional aggregation model to the edge server, consisting of the duration of DAG validation, regional model aggregation and regional model uploading.

As shown in Fig. 3, supposing that the system contains four vehicles ve_1, ve_2, ve_3, ve_4, the total training time of each selected vehicle is b_i. It is assumed that the model preparation time T^p is much larger than the regional aggregation time T^a, so changes in the number of local aggregation rounds Y do not affect the vehicles selected for each round. As the number of regional aggregation rounds Y increases, there will be a training delay l_i in the local aggregation time of each vehicle t_i^a, then the delay

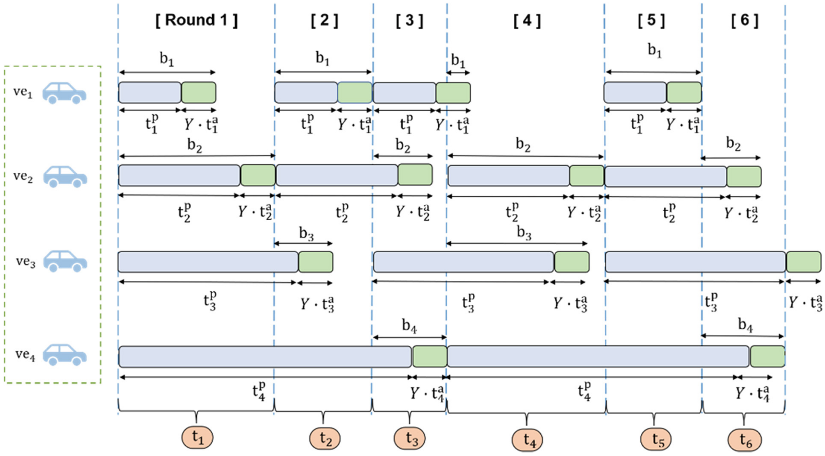


Fig. 3. Aggregation process.

of the global training model of this round is:

$$L_k = Max(l_1, l_2, l_3, ..., l_{|Z|}). \tag{16}$$

The total delay of the round k is:

$$\begin{aligned} t_k &= t_i^p + t_i^a + L_{(k)}(t_k \geq b_i) \\ &= t_i^p + t_i^a + L_k - \sum_{m}^{k-1} t_i(t_k \leq b_i), \end{aligned} \tag{17}$$

where m is the number of initial training rounds of the model.

Therefore, through multiple iterations, on the premise of model accuracy reaches the threshold, we let Y and Z satisfy the delay-accuracy-balancing factor:

$$\min(\chi T + \delta(1 - Acc)). \tag{18}$$

ALGORITHM 2: Semi-asynchronous federated learning mechanism based on DAG and blockchain

```
Input: Vehicles nodes $VE_m^{'}$={ve$_1$,ve$_2$,...,ve$_{n_m}$}
    The dataset of vehicles $D_m^{'}$={D$_{m,1}$,D$_{m,2}$,...,D$_{m,n_m}$}
    Initialize the blockchain and DAG
    The initial global model $\omega_0^{t_0}$
    Threshold staleness of tips $\tau$
$K = 0$
Get training nodes set $VE_m$={ve$_1$,ve$_2$,...,ve$_{n_m}$}
While $F_m(\omega_k) - F_m(\omega^*) > \varepsilon$ do
  For each vehicle ve$_i \in VE_m$ do
    publish the initial global model $\omega_0^{t_0}$ to ve$_i$
  For each vehicle ve$_i \in VE_m$ do
    $n_k$=0
    ve$_i$ update the local model on its local data D$_{m,i}$ by $E(.)$
    While $n_k < Y$ do
      $n_k = n_k + 1$
      ve$_i$ gets the local model from DAG
      ve$_i$ executes local aggregation and obtains updated local model $M_{i,k}$
      ve$_i$ add the parameters of the model $M_{i,k}$ as a transaction to the DAG
  $VE_k$=∅
  While $|VE_k| < Z$ do
    Receive local model $M_{i,k}$ from ve$_i$
    VE$_k$=$VE_k \cup \{ve_i\}$
  Update the global model by $E(.)$ and add it to the blockchain $B$
  For each $ve_i \in VE_m$ do
    If $ve_i \in VE_k$ or $\tau_i < \tau$ then
      $ve_i$ retrieves the updated model $\omega_k$ from the blockchain $B$
  $K = K + 1$
Return the final global model $\omega_k$
```

4 Simulation Results and Analysis

The algorithm was simulated using TensorFlow 2.5.0 on a Python 3.8-based simulator. To ensure the accuracy of the results, 50 experiments were carried out and the average was taken as the final result. The MNIST dataset is used as the training data, and we set 10% nodes as malicious nodes to simulate the poor training quality of the vehicle. Table 1 lists the relevant parameters in the simulations.

Table 1. Relevant parameters.

Parameter	Value
η_a (Learning rate for the actor)	0.001
η_c (Learning rate for the critic)	0.01
D (Local dataset)	[100, 2000]
Terminal kernel	[10, 100%]
Local iterations	5
Convolution layer	2
Fully connected layers	4
Noise power density (N_0)	−174 dBm/Hz
Wireless bandwidth of each link (B)	100 kHz
Propagation and verification delay effect ($H_{data}/R + l$)	0.1

To verify the performance of the proposed algorithm, we compared our algorithm (proposed) with the following three different algorithms:

(1) **Local CNN**: The FL mechanism is not used, and the model training is only performed on the local device.
(2) **SFL (Synchronous Federated learning)**: Using a synchronous FL mechanism, the algorithm selects all vehicles for model aggregation in each iteration of FL training.
(3) **ASFL (Asynchronous Federated learning)**: Using an asynchronous FL mechanism, the algorithm updates the global model after receiving a local model from any worker in each iteration of FL training.
(4) **Proposed**: Using a two-layer FL mechanism, the mechanism avoids excessive waiting time caused by vehicle heterogeneity in synchronous FL, and the large consumption of communication resources caused by frequent communication in asynchronous FL, which balances the time delay and accuracy.

The experiments analyzed the algorithm from various perspectives: accuracy, loss function, and time delay. Using the control variable method, the simulation is carried out with a definite Z value.

We first evaluated the impact of different Y and Z values on the proposed algorithm. The effect of different Y and Z values on the delay of the proposed algorithm is shown in Fig. 6. After several rounds of training, we found that the model accuracy has almost completed convergence at 0.93, which can achieve the ideal training effect of FL. Finally, on the premise of model accuracy ≥0.93, the optimal Y value is $n/10$, and the optimal Z value is $3n/5$ (n is the total number of vehicles).

As shown in Fig. 4, when the number of vehicles changes from 10 to 30–50, the time taken by the proposed scheme does not change significantly. Therefore, the proposed scheme is superior to other methods in terms of delay, which indicates that the proposed algorithm has high efficiency.

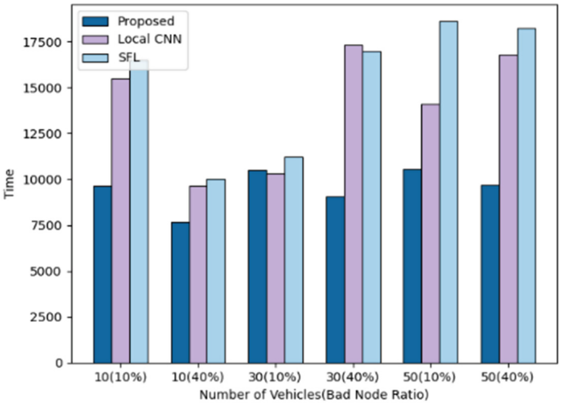


Fig. 4. Time delay.

For FL accuracy, Fig. 5 shows the changes in the accuracy of the 4 algorithms when there are 8 normal nodes and 2 bad nodes under MEC. It shows that the proposed mechanism has the fastest convergence and improves the accuracy by about 3.5% compared to ASFL. This is because the proposed mechanism selects nodes to avoid the influence of low-quality nodes on the training results, which shows that the proposed algorithm can still maintain good training performance when dealing with malicious nodes and differentiated data quality.

For FL loss function, Fig. 6 illustrates the changes in the loss functions of the three algorithms when the number of bad nodes in MEC accounts for 10%. The proposed algorithm converges the fastest and has the smallest loss function value. Because Local CNN is trained locally, it can only obtain the local optimal solution, so the loss function is high and always cannot converge.

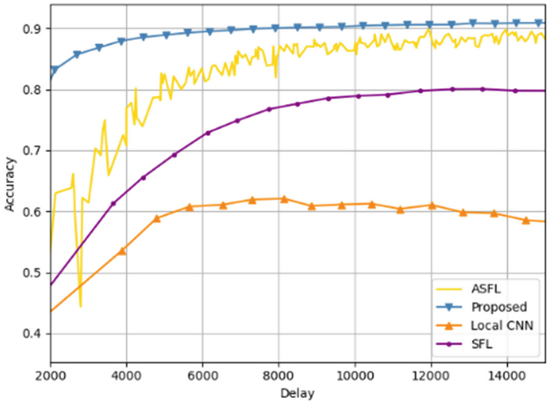


Fig. 5. Accuracy (Bad nodes in the MEC is 10%).

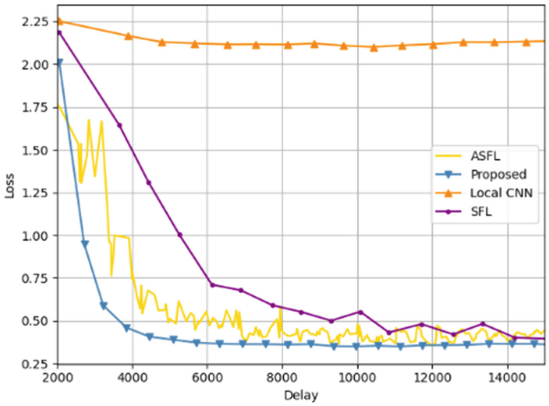


Fig. 6. Loss function (Bad nodes in the MEC is 10%).

5 Conclusion

This paper proposes a dual-layer federated learning and blockchain-empowered high-accuracy edge training mechanism for assisted driving models based on semi-asynchronous FL to provide both trust and efficiency in the assisted driving, which has a dual-layer FL and blockchain networks. Furthermore, we propose a DRL-based node selection algorithm and set a delay/accuracy impact factor to reduce total delay and improve model accuracy. The simulation results show that the proposed mechanism improves the FL delay and improves the ac-curacy by about 3.5% compared to ASFL.

Acknowledgment. This work is supported by the Self-funded technology project of the State Grid Henan Information and Telecommunication Company: Blockchain sharing technology for data privacy.

References

1. Haque, M.M., Sarker, S., Dewan, M.A.A.: Driving maneuver classification from time series data: a rule-based machine learning approach. Appl Intell (2022)
2. Wu, W., He, L., Lin, W., Mao, R.: Accelerating federated learning over reliability-agnostic clients in mobile edge computing systems. IEEE Trans. Parallel Distrib. Syst. **32**(7), 1539–1551 (2021)
3. Xu, G., Li, H., Liu, S., Yang, K., Lin, X.: VerifyNet: secure and verifiable federated learning. IEEE Trans. Inf. Forens. Secur. 15, 911–926 (2020)
4. McMahan, B., Moore, E., Ramage, D., Hampson, S., Arcas, B. A.: Communication-efficient learning of deep networks from decentralized data. In: Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, pp. 1273–1282 (2017)
5. Samarakoon, S., Bennis, M., Saad, W. Debbah, M.: Federated learning for ultra-reliable low-latency V2V communications. In: 2018 IEEE Global Communications Conference (GLOBECOM), pp. 1–7 (2018)
6. Feyzmahdavian, H.R., Aytekin, A., Johansson, M.: An asynchronous mini-batch algorithm for regularized stochastic optimization. IEEE Trans. Autom. Control 61(12), 3740–3754 (2016)
7. Lu, Y., Huang, X., Zhang, K., Maharjan, S., Zhang, Y.: Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Trans. Veh. Technol. **69**(4), 4298–4311 (2020)
8. Chen, M., Yang, Z., Saad, W., Yin, C., Poor, H. V., Cui, S.: A joint learning and communications framework for federated learning over wireless networks. IEEE Trans. Wirel. Commun. **20**(1), 269–283 (2021)
9. Zhu, Z., Sun.: Federated trace: a node selection method for more efficient federated learning. In: 2021 IEEE International Conference on Image Processing (ICIP), pp. 1234–1238 (2021)
10. Feng, L., Yang, Z., Guo, S., Qiu, X., Li, W., Yu, P.: Two-layered blockchain architecture for federated learning over the mobile edge network. IEEE Netw. **36**(1), 45–51 (2022)
11. Yuan, Y., Wang, F.: Blockchain:the state of the art and future trends. Acta Autom. Sin. **42**(4), 481–494 (2016)

Integrated Allocation Model for Communication, Storage and Computing Resource in Local Integrated Network

Jianding Fu[1], Cheng Zhong[2], Di Zhai[1], Yang Lu[1], and Jiajia Tang[3](✉)

[1] State Grid Smart Grid Research Institute Co.Ltd., Beijing, China
[2] State Grid Xiong'an New Area Electric Power Supply Company, Hebei, China
[3] Beijing University of Posts and Telecommunications, Beijing, China
tangjiajia@bupt.edu.cn

Abstract. With the rapid development of various wireless access technologies, there are various types of wireless communication networks in local converged communication network, which can provide services for users together. Diverse services on the network also require different communication, storage, and computing resources and require the collaboration of multiple nodes. Aiming at the problems of high complexity of three-dimensional resource cooperative allocation and difficulty in obtaining the optimal solution in a short time, this paper proposes an integrated storage and computing resource allocation model of local converged network, which converts communication resources into node delay attribute, solves the problem of computing and storage resource allocation with delay attribute, and converts three-dimensional resource allocation into two-dimensional. In a short time, the solution of the resource allocation problem is realized. The improved genetic algorithm is used to verify the effectiveness of the model.

Keywords: Converged network · Resource allocation · Wireless network

1 Introduction

In recent years, a variety of wireless access technologies have developed rapidly. Different types of wireless communication networks, such as 5G, Wi-Fi and wireless mesh, are integrated with each other to provide communication services for users, forming a local converged communication network. A local converged network that integrates various heterogeneous communication networks has many advantages, such as stronger network scalability, fuller network resources, and diversified service capabilities. It can meet the diversified requirements of network users and improve network reliability and anti-attack capability. At the same time, due to the features of dense networking and multiple wireless networking modes, local converged networks usually contain a large number of different types of terminals, and users have different requirements, resulting in different service resource requirements in the network. On the other hand, network applications are also gradually developing towards diversification and personalization. The

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 284–294, 2024.
https://doi.org/10.1007/978-981-99-7161-9_22

development of various networks brings about new service forms constantly emerging, and typical application scenarios such as small-particle acquisition, large bandwidth, real-time interaction and other services with differentiated QoS coexistence requirements [1]. However, the traditional local network can no longer guarantee the service quality of users and diversified business requirements of users due to its shortcomings such as low frequency band utilization rate and relatively simple function [2]. Due to the complex and diverse network structure, resources of a single network node or terminal are also limited in local converged networks. It is difficult for a single node to simultaneously meet the multi-dimensional resource requirements of various services, such as communication, storage and computing, etc. In general, resource collaborative allocation among multiple nodes is required [3]. At the same time, due to the dynamic and organic unity of the network, The change of resources of one dimension in the network will also affect the use of resources of other dimensions, so it is necessary to consider the joint allocation of resources of multiple dimensions [4]. Therefore, it is necessary to establish an integrated allocation model of general storage and computing resources to realize the cooperative allocation of resources in the local converged communication network.

To solve the above problems, there have been some researches on multidimensional resource allocation models at home and abroad. Literature [1] establishes a communication computing resource joint allocation model aiming at minimizing user delay to carry out two-dimensional resource allocation in multi-user mobile edge networks. In literature [3], the author abstracts communication, computing and storage resources digitally, and uses virtualization technology to establish a 3D resource scheduling model. In literature [5], ICN cache and computing technology is used to establish a scheduling model for the integration of three-dimensional network, computing and storage resources, so as to realize dynamic resource scheduling in wireless networks. The author of reference [6] established a communication and computing resource allocation model with the goal of minimizing the total energy consumption of the system under specified delay limits, and designed a prioritization based solution to solve the problem. In order to coordinate communication and computing resource allocation, literature [7] established a communication and computing resource model with the goal of minimizing the total energy consumption of the system, and designed an iterative algorithm based on successive convex approximation to solve the problem. However, most of the existing multi-dimensional resource allocation algorithms only consider the allocation problem of a certain one-dimensional resource, or in the allocation problem of multi-dimensional resources, each one-dimensional resource involved is dealt with separately, and the impact of three-dimensional resources on optimization objectives is not taken into account jointly, and the complexity and dynamics of the system are ignored. Therefore, the obtained resource allocation results cannot guarantee better performance of the system [8]. In addition, simultaneous collaborative allocation of 3D resources has high complexity, so there is no good efficient solution algorithm.

To solve the above problems, this paper proposes an integrated allocation method of storage and computing resources in local converged network, establishes an integrated allocation model of storage and computing resources in local converged network, and transforms the problem of three-dimensional cooperative allocation of communication, storage and computing resources among multiple nodes into a collaborative allocation problem of two-dimensional storage and computing resources among multiple nodes with delay attribute. The solution complexity is reduced and the efficiency is improved. The improved genetic algorithm is used to solve the problem model, and the effectiveness of the resource cooperative allocation model is verified.

2 System Model

2.1 System Scenario

This paper considers the local converged communication network scenario where a variety of wired and wireless communication networks coexist. As shown in Fig. 1, the service terminal accesses the converged communication terminal through different gateways, and the converged communication terminal accesses the power communication transmission network through the wired/wireless private network, and finally connects to the power communication service system to achieve various business functions. Nodes in the same access network can be connected to each other, and fusion communication terminals can be connected to each other. At present, there have been many studies on cross-domain communication between heterogeneous networks through protocol conversion [9–11]. Therefore, in the scenario of this paper, it is believed that there are network nodes in different networks that can communicate cross-domain, and this node can transmit service data to other networks.

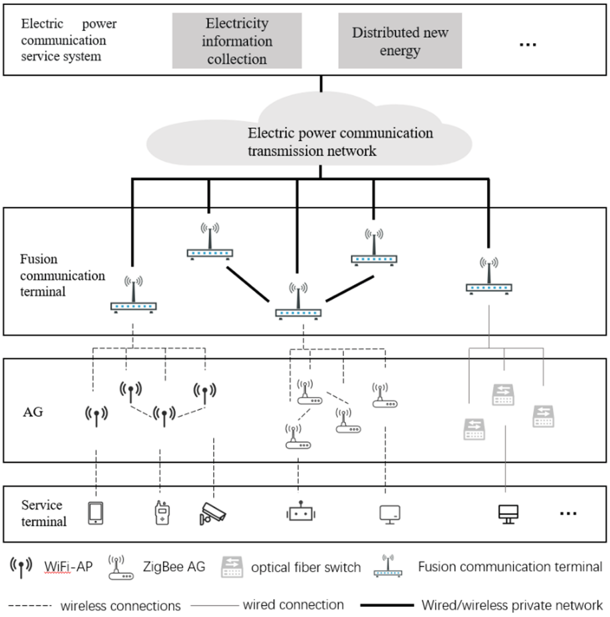

Electric power communication service system
Electricity information collection
Distributed new energy
...
Electric power communication transmission network
Fusion communication terminal
AG
Service terminal
...
WiFi-AP
ZigBee AG
optical fiber switch
Fusion communication terminal
wireless connections
wired connection
Wired/wireless private network

Fig. 1. System scene diagram

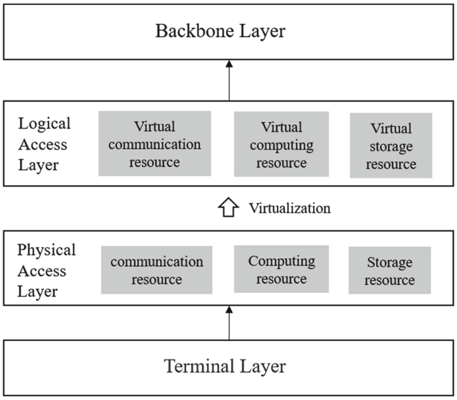


Fig. 2. Abstraction of resources

Services generated by terminals are scheduled and allocated resources at the access layer between service terminals and converged communication terminals. In this paper, virtualization technology is used to abstract network nodes in the access layer into nodes with communication, storage and computing resources that are connected to each other, forming a logical access layer, in which resources are allocated for services, as shown in Fig. 2.

With G = {V, E} to indicate the current topology of network infrastructure, including V in the network nodes, $\{v_i \in V | i \in (1, m)\}$, E said set of communication links between the nodes, $\{(v_i, v_j) \in E | v_i, v_j \in V\}$. Node attributes include node computing power $C_i^N (cycles/bit)$ and storage capacity $S_i^N (bits)$, link attributes include link communication bandwidth $R_{ij}^N (bps)$ and transmission distance $Dis_{ij}^N (m)$. Set business requests with $\text{T} = \{t_i | i = 1, \ldots, n\}$, service requests can be described by four parameters, namely, amount of data transmitted $D_i^T (bits)$, amount of data stored $D_i^S (bits)$, amount of data calculated $D_i^C (cycles/bit)$, communication bandwidth $R_i^T (bps)$ and maximum allowable delay $\tau_i (s)$. To facilitate calculation, a network node is considered to provide computing services for only one service at a time with all CPU resources.

This paper considers the cooperative allocation of communication, computing, and storage resources among network nodes. Communication resources refer to the communication bandwidth between nodes, in bps; computing resources are defined in cycles/bit of CPU; storage resources refer to the memory capacity of nodes, in bits. Local converged networks provide a differentiated combination of communication, computing, and storage resources to meet different service requirements. Therefore, resource allocation policies that match services must be adopted to meet service requirements. However, since communication, computing and storage resources belong to different resource categories and have different definitions and measurement forms, they need to be mapped into the same one-dimensional space and adopt the same measurement form to establish the constraint and transformation relationship between multi-dimensional resources and network performance. In this paper, the joint allocation of total storage and computing resources is carried out with the goal of minimizing service delay. The system optimization objectives are as follows:

$$\min_{(R,S,C)} T \tag{1}$$

s.t.

$$R_i^T \leq R_{ij}^N (i,j) \in P_i \tag{2}$$

$$D_i^S \leq S_j^N, j = S_i \tag{3}$$

$$T \leq \tau_i \tag{4}$$

That is, under the condition that service requirements are met and network node resources are not exceeded, function optimization is carried out with the goal of minimizing service delay, where P_i is the path through which service i is transmitted in the network.

2.2 Problem Transformation

Services in a local converged communication network have various types and requirements. In the process of resource allocation, it is found that a single node cannot meet the resource requirements of all dimensions of the business during resource allocation, so it is necessary to search for other nodes with sufficient resources in the network for collaborative processing under the premise of not exceeding the service delay limit, and conduct collaborative allocation of (R, S, C) three-dimensional resources in the multi-node combination. However, due to the high complexity and difficulty of joint allocation of 3D resources among non-directly connected multi-nodes, and the communication bandwidth is usually represented in the form of time delay generated during data transmission between nodes, each node can be regarded as a block of storage and computing resources with communication delay. Based on this characteristic, the (R, S, C) three-dimensional resource cooperative allocation problem is transformed into a (S, C) two-dimensional resource allocation strategy calculation problem with delay attribute.

Therefore, the calculation model after transformation is as follows:

Communication Resource Model. The local converged communication network supports various networking modes, such as wireless mesh, Wi-Fi, and 5G. The communication resources in the network are communication bandwidth resources between nodes. However, different networking modes support different communication bandwidth resources. Because the service request bandwidth cannot be larger than the maximum bandwidth resource R_{max} that can be provided by the current network node, the communication bandwidth is subject to the following constraints:

$$R_i^T \leq R_{ij}^N (i,j) \in P_i \tag{5}$$

On the one hand, service transmission from the current node needs to be carried out after the previous service transmission through the current node is completed. Therefore, the waiting time before service transmission from the current node is as follows:

$$T_w^{ij} = max\left\{0, T_{latest}^j - T_{cur}^i\right\}, i \in [0, n], j \in [0, m] \tag{6}$$

In the command, T_{latest}^j indicates the time when the last task is transmitted or computed on node j, and T_{cur}^i indicates the total delay generated by the transmission of task i to the current node.

On the other hand, according to the transmission rate of the service request in the network, the transmission delay generated when the request is transmitted between nodes is also related to the amount of data transmitted by the service and the communication bandwidth of the link between the sending node and the receiving node. The calculation formula is as follows:

$$T_t^{ijk} = \frac{D_i^s}{R_{jk}^N}, i \in [0, n], j, k \in [0, m], j \neq k \tag{7}$$

Therefore, the delay generated by the transmission of task i between nodes is as follows:

$$T_R^{ijk} = T_w^{ij} + T_t^{ijk}, i \in [0, n], j, k \in [0, m], j \neq k \tag{8}$$

Storage Resource Model. Storage resources refer to the memory resources owned by each node. Considering that storage resources must at least meet the service storage resource request S_l, storage resources for service requests must meet the following constraints:

$$D_i^S \leq S_j^N, j = S_i \tag{9}$$

The storage delay of services is related to the amount of data to be stored for services and the storage rate of nodes. Generally, the amount of data to be stored for services is not too large. Therefore, the storage time of different devices is similar. Therefore, in this paper, the differences in data storage rates between different devices are ignored, and the storage rates of nodes are regarded as v_j^N. Therefore, the formula for calculating the delay of service storage data is as follows:

$$T_S^i = \frac{D_i^S}{v_j^N}, i \in [0, n], j \in [0, m] \tag{10}$$

Computational Resource Model. Computing resources refer to CPU resources in this article. CPU resources owned by each network node are represented by C_i^N (cycles/bit).

Computing delay occurs when services are calculated on a node. The computing delay is related to the amount of calculated data and CPU resources of the node. The calculation formula is as follows:

$$T_C^i = \frac{D_i^T}{C_i^N}, i \in [0, n] \tag{11}$$

Then, the delay generated from the sending to the completion of a service request consists of three parts: request transmission delay between nodes, storage delay and calculation delay. The calculation formula is as follows:

$$T_i = \left(\sum_{(j,k) \in P_i} T_s^{ijk} \right) + T_S^i + T_C^i \tag{12}$$

System Optimization Objectives. When a service request is generated, our goal is to complete the request with minimum delay in the current local converged communication network, occupy as little unnecessary system resources as possible, and ensure the maximization of system throughput. During service request forwarding, although computing and storage resources of intermediate nodes are not occupied, communication resources of nodes are occupied during service request forwarding. Other requests to use the node resources cannot be answered, resulting in waste of system resources and throughput reduction. Therefore, we want to minimize the number of intermediate nodes in the process of service transmission. Therefore, the number of intermediate nodes is punished in the optimization goal. The system optimization objectives and constraints are as follows:

$$\min f(x) = min\left(\left(\sum_{(j,k) \in P_i} T_R^{ijk} \right) + T_S^i + T_C^i + \lambda n_i \right) \tag{13}$$

s.t.

$$R_i^T \le R_{ij}^N (i,j) \in P_i \tag{14}$$

$$D_i^S \le S_j^N, j = S_i \tag{15}$$

$$\left(\sum_{(j,k) \in P_i} T_R^{ijk} \right) + T_S^i + T_C^i \le \tau_i \tag{16}$$

Of $\sum_{(j,k) \in P_i} T_s^{ijk}$ for business i total transmission delay in transmission between each node, P_i for business i offered by a path in the network transmission, T_S^i for business request i storage time delay, T_C^i for business I computing time delay, λ for business request i punish coefficient, the number of intermediate nodes n_i indicates the number of intermediate nodes in service request i. Restriction Condition (14) Ensure that the communication bandwidth of the path through which services are transmitted can meet the bandwidth requirements of services. Restriction Condition (15) Ensure that the storage resources of the node where services are stored can meet the storage resource requirements of services. Equation (16) Ensure that the delay for completing service requests does not exceed the maximum allowed delay specified by the service.

2.3 Improved Genetic Algorithm

The solution of the above model is NP-hard, so intelligent algorithm can be used for iterative optimization. Compared with other intelligent optimization algorithms, genetic algorithm has advantages such as parallelism and fast convergence. Therefore, improved genetic algorithm is used to solve the optimal resource allocation strategy when designing the integrated joint allocation method of computing and storage resources in local converged network communication [12].

The specific solving steps of this model are as follows:

Step1: The population G, population size M and iteration number N were initialized by genetic algorithm.
Step2: Calculate the fitness value of each individual in the population $U(x) = 1/f(x)$.
Step3: Select individuals from the population to iterate into the next generation population, then cross and mutate them according to probability.
Step4: Calculate the fitness of the new population and select the optimal individual in the new population.
Step5: Judging whether the fitness of the new optimal individual is greater than that of the original optimal individual.
Step6: If yes, the current optimal solution will be updated, and the number of iterations will be increased by one.
Step7: Judge whether the maximum number of iterations has been reached. If yes, terminate the program; otherwise, perform Step3.

The flow chart of the algorithm is shown as follows (Fig. 3).

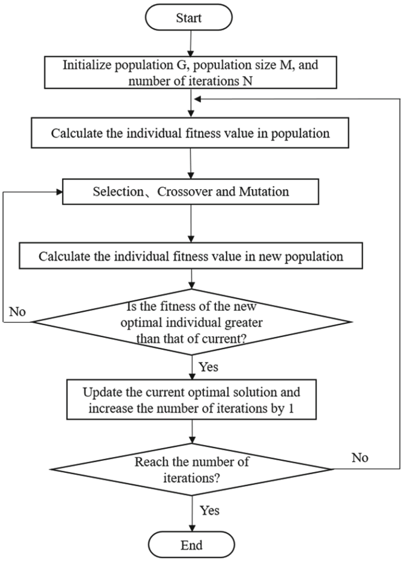

Start
Initialize population G, population size M, and number of iterations N
Calculate the individual fitness value in population
Selection、Crossover and Mutation
Calculate the individual fitness value in new population
Is the fitness of the new optimal individual greater than that of current?
No
Yes
Update the current optimal solution and increase the number of iterations by 1
Reach the number of iterations?
No
Yes
End

Fig. 3. Algorithm flow chart

3 Simulation

In order to verify the performance of this scheme, the software MATLAB R2020b is used to simulate the operation of the algorithm, in which the main data parameters are as follows (Table 1).

Table 1. Simulation parameters

Parameter meaning	Value
Communication bandwidth of wireless mesh, WiFi network R_1, R_2/Mbps	200
Communication bandwidth of 5G network R_3/Mbps	1000
Communication bandwidth between different networks R_4/Mbps	100
CPU frequency of a network node f/GHz	1–4
Storage resources of a network node D/GB	2–256
Maximum number of iterations I	500

The figure below shows the service delay sizes obtained under different iterations with different population sizes for the model proposed in this paper. Populations with sizes of 30, 100 and 300 are selected respectively for comparison. As can be seen from the figure below, when the population size is 100, the algorithm obtains the optimal solution around the 400th iteration, which is the optimal resource allocation scheme of the current business. It can be seen that the allocation scheme has the minimum delay, which proves the effectiveness of the model. However, when the population size is too small, due to the limited genotype in the population, it is difficult for interindividual hybridization in the population to generate new and better genotypes, resulting in premature convergence of the algorithm, which falls into the local optimal solution and fails to obtain the optimal allocation scheme. However, when the population size is too large, although the convergence speed is accelerated, the larger calculation amount will slow down the algorithm running speed and waste computing resources. Thus, the validity of the model proposed in this paper can be seen. Among them, the reasonable value of population size is 100 (Fig. 4).

The following figure shows the time delay of the distribution strategy obtained by each iteration number under different mutation probability value conditions in solving the proposed model. As can be seen from the figure below, when the mutation probability is 0.1, the optimal solution can be obtained around the 400th iteration; while when the mutation probability is 0.01, the probability of jumping out of the local optimal solution decreases as the mutation probability is too small, resulting in the local optimal solution, and the optimal solution cannot be obtained through further iteration. However, when the mutation probability is too large, the mutation result will be uncontrollable, and it is difficult to converge to get the optimal solution. It can be seen that the reasonable value of variation probability in this method is 0.1 (Fig. 5).

The following figure shows the influence of different cross probability values on the results during the solution of the proposed model. As can be seen from the figure below,

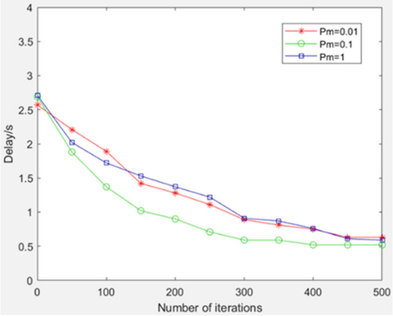


Fig. 4. Average service delay

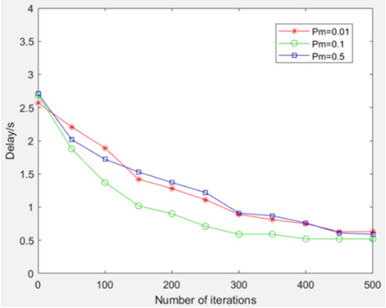


Fig. 5. Maximum service delay

when the mutation probability is 0.9, the current algorithm can iterate at a proper rate and obtain the optimal solution around the 400th iteration. However, when the mutation probability is too large, all the selected individuals will be mutated, which may destroy the better genes and easily fall into the local optimal. When the mutation probability is too small, the genotypes in the population cannot be updated effectively, which will reduce the efficiency of population iteration and slow down the rate of obtaining the optimal solution. It can be seen that the reasonable value of crossover probability in this scheme is 0.9 (Fig. 6).

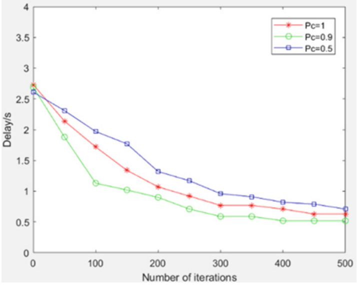


Fig. 6. Network resource utilization

Acknowledgement. This work has been supported by State Grid Corporation of China science and technology project "Research on Local Integrated Communication Network System and Endogenous Security Technologies Oriented to Urban Grid" (5700-202213221A-1-1-ZN).

References

1. Liu, Y.: Research on resource management in 5G heterogeneous networks. Beijing University of Posts and Telecommunication (2019)
2. Wu, Q.: Research on joint resource allocation algorithm for 5G heterogeneous network fusion. Shandong University of Science and Technology (2020). https://doi.org/10.27275/d.cnki.gsdku.2020.000637
3. Meng, Y., Liu, X.: Resource allocation and interference management for multi-layer wireless networks in heterogeneous cognitive networks. Wirel. Com Netw. **190** (2019)
4. Kim, S.: Cellular network bandwidth management scheme by using nash bargaining solution. IET Commun. **5**(3), 371–380 (2011)
5. Ren, J., Yu, G., Cai, Y., et al.: Latency optimization for resource allocation in mobile-edge computation offloading. IEEE Trans. Wirel. Commun. **17**(8), 5506–5519 (2018)
6. Fei, R., Huang, Renchao, et al.: Software defined networking, caching, and computing for green wireless networks. IEEE Commun. Mag. **54**(11):185–193
7. Zhang, K., Leng, S., Mao, Y.M.: Energy-efficient offloading for mobile edge computing in 5G heterogeneous networks. IEEE Access **4**(99), 5896–5907 (2017)
8. Liu, J., Mao, Y., Zhang, J., et al.: Delay-optimal computation task scheduling for mobile-edge computing systems. IEEE (2016). https://doi.org/10.1109/ISIT.2016.7541539
9. He, X.M., Xiao, X.B., Huan, H.: Application of power communication system based on heterogeneous network. Appl. IC **39**(10):41–43 (2022). https://doi.org/10.19339/j.issn.1674-2583.2022.10.015
10. Lin, M.: Research on hybrid network communication mechanism based on SDN. Chongqing University of Posts and Telecommunications (2019). https://doi.org/10.27675/d.cnki. gcydx.2019.000521
11. Hui, W.: Research and implementation of heterogeneous network video transmission protocol. Zhejiang Sci-Tech University (2022). https://doi.org/10.27786/d.cnki.gzjlg.2022.000425
12. Jixv, G., Jun, W.: Multi-dege collaborative computing unloading scheme based on genetic algorithm. Comput. Sci. **48**(1), 72–80 (2021). https://doi.org/10.11896/jsjkx.200800088

Maximum Throughput Oriented Integrated-CSC Resource Allocation Algorithm for Business with Large Bandwidth Power Communication Business

Wei Bai[1], Di Zhai[1], Cheng Zhong[2], Jiajia Tang[3](✉), and Sujie Shao[3]

[1] State Grid Smart Grid Research Institute Co, Ltd, Beijing, China
[2] State Grid Xiongan New Area Electric Power Supply Company, Hebei, China
[3] Beijing University of Posts and Telecommunications, Beijing, China
tangjiajia@bupt.edu.cn

Abstract. With the continuous and rapid development of the Internet, high-bandwidth services emerge gradually, which puts forward the requirement of high bandwidth and large traffic on the network. High-bandwidth services usually occupy a large amount of transmission bandwidth. However, due to the limited resources of a single network node in the power local wireless communication network, it cannot meet the multi-dimensional resource requirements of high-bandwidth services. Therefore, resource coordination among multiple nodes is required. To solve the above problems, this paper proposes an integrated allocation method of communication, storage and computing (CSC) resources oriented to maximizing network throughput. Firstly, an integrated allocation model of storage and computing resources oriented to maximizing throughput is established. On the basis of this model, an integrated allocation method of CSC resources aiming at minimizing delay and maximizing network throughput is proposed. Solve the resource allocation problem of large-bandwidth services in the local converged network, increase network throughput, and improve the utilization of network resources.

Keywords: Converged network · Resource allocation · Large bandwidth · Delay

1 Introduction

Multiple networking modes coexist in local converged networks, which contain a large number of different types of terminals with different service requests. With the continuous and rapid development of the Internet, high-bandwidth services such as 4 K ultra-HD, 3D, and cloud services continue to emerge, putting forward high bandwidth and large traffic requirements such as 100 Mbit/s and gigabit. The most prominent feature of the high-bandwidth service is the large amount of data transmission, which occupies a large amount of bandwidth resources. In addition, the high-bandwidth service requires high computing and storage resources, which occupies a large amount of network resources. When resources are allocated on the network together with traditional

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 295–305, 2024.
https://doi.org/10.1007/978-981-99-7161-9_23

services, how to meet the resource requirements of large-bandwidth services without affecting the resource allocation of other services has become a key issue for service resource allocation in local converged networks. However, the traditional local network cannot guarantee the service quality and diversified business needs of users due to its shortcomings such as low frequency utilization rate, resource waste and simple function [1]. In addition, due to the complex and diverse network structure, the resources of a single node or terminal in a local converged network are limited. Therefore, it is difficult for a single node to meet the differentiated resource requirements of various services at the same time. Therefore, coordinated resource allocation among multiple nodes is usually required. In view of the above problems, in order to meet the resource allocation requirements of large bandwidth services above 100 Mbps, but not affect the network to allocate resources to other services, this paper proposes an integrated storage and computing resource allocation method for large bandwidth services, which is oriented to maximizing network throughput. Based on the characteristics of large bandwidth services, a resource allocation method based on genetic annealing algorithm was designed to maximize network throughput and minimize latency for large bandwidth services. It improves network resource utilization, meets high-bandwidth service requirements, and improves network differentiation service capability.

2 Related Work

With the development of communication technology and new applications, more and more scholars at home and abroad have conducted researches on multi-dimensional resource allocation. Literature [2] proposes a multi-dimensional resource allocation method. In multi-user MEC network, through joint optimization of communication and computing resources, the closed-form expression of optimal resource allocation under special circumstances is deduced with the optimization goal of minimizing user delay. In literature [3], the author proposes an architecture that integrates network, storage and computing, combines ICN cache and computing technology, and dynamically schedules network, storage and computing resources to meet the computing service requirements in wireless networks. In literature [4], the author uses virtualization technology to share communication, computing and cache resources among users, and uses an alternate direction method to relax the problem into a convex optimization problem for solving. The authors of literature [5] jointly optimized communication resource allocation and computational migration, minimized system energy consumption under certain time-delay constraints, divided mobile devices into three types, and allocated wireless channels to mobile devices iteratively according to their priorities, thus reducing the complexity of solving the problem. Literature [6] designed an optimal computing task scheduling scheme for the MEC system. Firstly, Markov chain theory was used to analyze the average delay and average power consumption of tasks on the mobile device under the proposed scheduling strategy, and the delay minimization problem was established with the power constraint. An efficient one-dimensional search algorithm was used to derive the optimal computing migration strategy. The authors of reference [7] jointly optimized communication resources and computing resources, and adopted an iterative algorithm based on successive convex approximation to solve the constructed non-convex optimization problem with the goal of minimizing total energy consumption.

However, most of the existing multi-dimensional resource allocation algorithms only consider the allocation problem of a certain one-dimensional resource, or in the allocation problem of multi-dimensional resources, each one-dimensional resource involved is dealt with separately, and the impact of three-dimensional resources on optimization objectives is not taken into account jointly, and the complexity and dynamics of the system are ignored. Therefore, the obtained resource allocation results cannot guarantee better performance of the system [8]. In this paper, an integrated allocation method of storage and computing resources for maximum throughput is proposed, considering the cooperative allocation of communication, computing and storage resources among different nodes in local converged communication network, and considering the association relationship between three-dimensional resources to realize the integrated allocation of resources.

3 System Model

3.1 System Scenario

In this paper, resources are allocated in the local converged network for services with large bandwidth and low delay, such as 4K ultra-HD, 3D and cloud services [9]. The system scenario is shown in Fig. 1. For terminals such as video surveillance and inspection robots, the characteristics of their services are that they require a large communication bandwidth and a low delay. At the same time, they also need to ensure that resource allocation of other services is not affected. Therefore, the goal of resource allocation for high-bandwidth services is to minimize delay and maximize network throughput.

3.2 System Optimization Objectives

In this paper, the local converged network integrated storage and computing allocation model is adopted to establish the system model. The goal is to complete the request with the minimum delay in the current local converged communication network, while occupying less unnecessary system resources as far as possible to ensure the maximum system throughput. However, after a service request is generated, due to the large bandwidth occupied by large bandwidth services, if too many nodes are forwarded, although the computing and storage resources of these intermediate nodes are not occupied in the forwarding process, the communication resources of the nodes are largely occupied [10]. During this period, other requests to use the node resources cannot be answered, resulting in a waste of network resources at that time. Reduces network throughput. Therefore, in order to reduce the occupation of unnecessary network resources, we hope to minimize the number of intermediate nodes in the process of service transmission. Therefore, the number of intermediate nodes is punished in the optimization objective to ensure that resources are allocated with as few forwarding times as possible. The system optimization objectives and constraints are as follows:

$$\min f(x) = min\left(\left(\sum_{(j,k)\in P_i} T_R^{ijk}\right) + T_S^i + T_C^i + \lambda n_i\right) \tag{1}$$

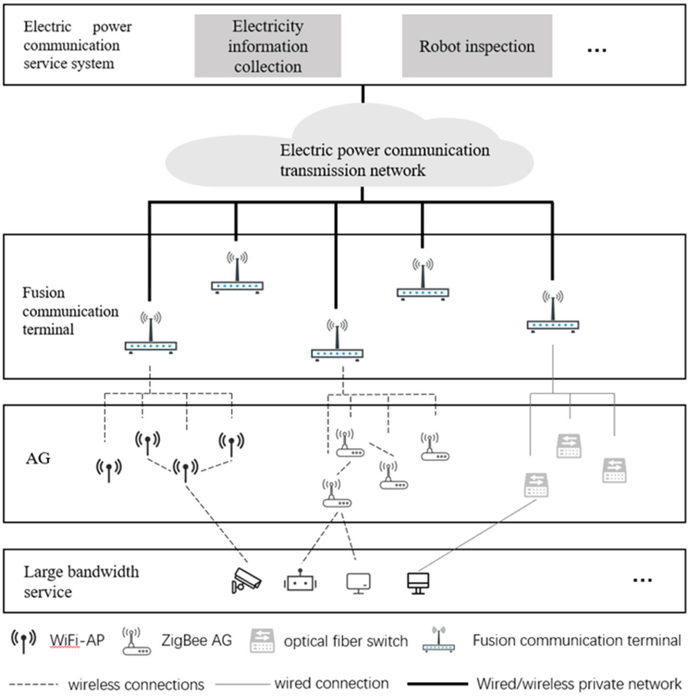

Electric power communication service system
Electricity information collection
Robot inspection
...
Electric power communication transmission network
Fusion communication terminal
AG
Large bandwidth service
...
WiFi-AP
ZigBee AG
optical fiber switch
Fusion communication terminal
wireless connections
wired connection
Wired/wireless private network

Fig. 1. System scene diagram

s.t.

$$R_i^T \le R_{ij}^N (i, j) \in P_i \tag{2}$$

$$D_i^S \le S_j^N, j = S_i \tag{3}$$

$$\left(\sum_{(j,k) \in P_i} T_R^{ijk} \right) + T_S^i + T_C^i \le \tau_i \tag{4}$$

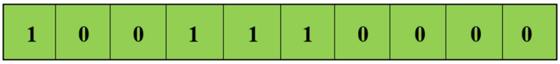
Of $\sum_{(j,k) \in P_i} T_s^{ijk}$ for business i total transmission delay in transmission between each node, P_i for business i offered by a path in the network transmission, T_S^i for business request i storage time delay, T_C^i for business I computing time delay, λ for business request i punish coefficient, the number of intermediate nodes n_i indicates the number of intermediate nodes in service request i. Restriction Condition (2) Ensure that the communication bandwidth of the path through which services are transmitted can meet the bandwidth requirements of services. Restriction Condition (3) Ensure that the storage resources of the node where services are stored can meet the storage resource requirements of services. Equation (4) Ensure that the delay for completing service requests does not exceed the maximum allowed delay specified by the service.

4 An Integrated Communication, Storage and Computing Resource Allocation Algorithm for Maximum Throughput

Traditional resource allocation algorithms have high computational complexity and slow convergence rate when solving multi-dimensional resource joint optimization problems. In order to speed up the solution, intelligent algorithms can be used for iterative optimization. Genetic algorithm has the advantages of parallelism and fast convergence, but at the same time, it is easy to fall into the local optimal and cannot guarantee the global optimal solution, so it needs to be improved. The simulated annealing algorithm can expand the search range of the algorithm, improve the diversity of solutions, and avoid falling into the problem of local optimal. But the convergence speed of simulated annealing algorithm is slow, especially when the calculation involves a large number of individuals, the efficiency is too low, and the time is too long. Therefore, in the design of integrated joint allocation method of computing and storage resources in local fusion network communication, the idea of simulated annealing algorithm is introduced on the basis of improved genetic algorithm, and the two are combined to complement each other's advantages, so as to accelerate the convergence speed and improve the solving accuracy. The core idea of this method is to accept a solution worse than the current global optimal solution as the new global optimal solution with a certain probability, rather than a full acceptance of probability 1, so as to avoid falling into the problem of local optimal solution.

4.1 Chromosome Coding

In this scheme, binary coding is adopted, and each gene represents a node in the network. 0 on the gene location means that the current service does not pass through this node, and 1 means that the current service will pass through this node. But it is worth noting that a chromosome code does not just correspond to a resource allocation scheme, because the transmission path of services is uncertain. Therefore, when initializing the population, we can directly eliminate the individuals whose all possible path combinations do not meet the business requirements (Fig. 2).



1	0	0	1	1	1	0	0	0	0

Fig. 2. Chromosome

4.2 Judge Individual Legitimacy

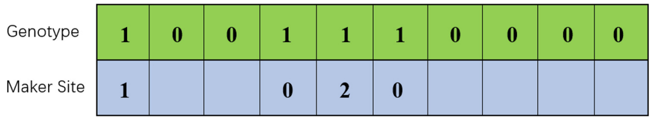
In the process of population initialization, heredity, variation and other operations, individuals with new genotypes will be generated, but not all of them meet the requirements of the current business on resources. Therefore, before adding the newly generated individuals into the population, it is necessary to judge the legitimacy of the individuals and eliminate those who do not meet the requirements. There are two aspects to determine the validity of an individual: whether there are sufficient computing and storage resources, and whether there are forwarding paths that meet service bandwidth requirements.

First, determine whether sufficient computing and storage resources exist. That is, check whether two nodes of the current genotype 1 can meet the computing and storage resource requirements. If yes, go to the next step. If no, the individual is invalid.

If a node that meets service computing and storage requirements is found, check whether a forwarding path that meets bandwidth requirements exists. Services pass through all nodes of genotype 1. Therefore, check whether the bandwidth of all network nodes can meet the current service bandwidth requirements. If the bandwidth of nodes cannot meet the current service bandwidth requirements, the individual node is invalid.

4.3 Fitness Function

In this scheme, individuals are evaluated using fitness functions, where U(x) = 1/f(x). During the calculation of individual fitness function, since there is no one-to-one correspondence between individual and resource allocation scheme, in order to simplify the calculation, the flag bit array of optimal resource allocation scheme is added to each chromosome during the calculation of fitness function, where the flag bit 0 indicates that the node only carries out business forwarding, and the flag bit 1 indicates that the node carries out business calculation. Flag bit 2 indicates the storage where services are performed on the node. According to the flag bit, you can know the optimal resource allocation scheme for the service (Fig. 3).



Genotype	1	0	0	1	1	1	0	0	0	0
Maker Site	1			0	2	0				

Fig. 3. Add marker sites to chromosomes

4.4 The Selection of Genetic Algorithms

Two individuals were selected from the original population to cross and mutate using roulette. The probability of individual selection is related to the proportion of fitness function in the sum of fitness of all individuals in the population. If the total number of individuals in the population is M, then the probability of an individual x_i being inherited to the next generation population is:

$$p(x_i) = f(x_i)/(f(x_1) + f(x_2) + \cdots + f(x_M))$$

The accumulation probability of this individual is:

$$q(x_i) = \sum_{j=1}^{i} p(x_j)$$

4.5 Algorithms

The specific solving steps of this model are as follows:

Step1: The population G, population size M and iteration number N were initialized by genetic algorithm.
Step2: Calculate the fitness value of each individual in the population $U(x) = 1/f(x)$.
Step3: Select individuals from the population to iterate into the next generation population, then cross and mutate them according to probability.
Step4: Calculate the fitness of the new population and select the optimal individual in the new population.
Step5: Judging whether the fitness of the new optimal individual is greater than that of the original optimal individual.
Step6: If yes, the current optimal solution will be updated, and the number of iterations will be increased by one.
Step7: Judge whether the maximum number of iterations has been reached. If yes, terminate the program; otherwise, perform Step3.

The flow chart of the algorithm is shown as follows (Fig. 4).

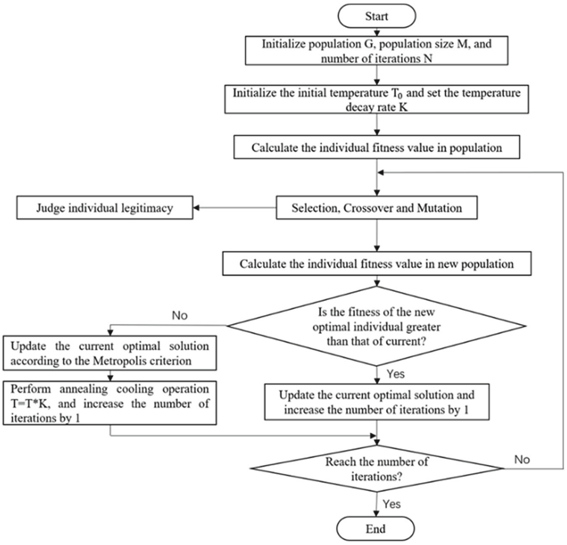

Start
Initialize population G, population size M, and number of iterations N
Initialize the initial temperature T_0 and set the temperature decay rate K
Calculate the individual fitness value in population
Judge individual legitimacy
Selection, Crossover and Mutation
Calculate the individual fitness value in new population
No
Is the fitness of the new optimal individual greater than that of current?
Update the current optimal solution according to the Metropolis criterion
Yes
Perform annealing cooling operation T=T*K, and increase the number of iterations by 1
Update the current optimal solution and increase the number of iterations by 1
Reach the number of iterations?
No
Yes
End

Fig. 4. Algorithm flow chart

5 Simulation

In order to verify the performance of this scheme, the software MATLAB R2020b is used to simulate the operation of the algorithm, in which the main data parameters are as follows (Table 1).

Table 1. Simulation parameters

Parameter meaning	Value
Communication bandwidth of Wireless mesh, WiFi network R_1, R_2/Mbps	200
Communication bandwidth of 5G network R_3/Mbps	1000
Communication bandwidth between different networks R_4/Mbps	100
CPU frequency of a network node f/GHz	1–4
Storage resources of a network node D/GB	2–256
Population size M	100
Maximum number of iterations I	500
Probability of crossover P_c	0.9
Probability of mutation P_m	0.1
Initial temperature T_0	1000
Cooling rate K	0.95

The figure below shows the average service delay of this scheme (MT-GSA) and the other two schemes under different service quantities. It can be seen from the figure that the average processing delay of the scheme proposed in this paper increases smoothly and slowly with the increase of large bandwidth service requests. In the internal resource allocation scheme of the local network, service requests can only use the limited resources of the local network nodes, and high-bandwidth services usually occupy a lot of resources. As the number of service requests increases, the resources of small local network devices are exhausted, and the average processing delay increases significantly and the growth rate increases gradually. However, in the random resource allocation scheme, since the resources of different nodes are randomly allocated, services need to be transmitted between these nodes, occupying a large number of unnecessary resources. Although there is a certain probability of responding to services with a small delay, due to unreasonable resource allocation, as the number of services increases, the remaining resources become less and less, which makes it difficult to meet subsequent service requests. As a result, the service processing delay increases rapidly. It can be seen that this scheme can efficiently implement resource allocation for large bandwidth services with small delay (Fig. 5).

The following figure shows the average processing latency of other services when large-bandwidth services exist together with other services on the network. In this scenario, it is assumed that every other type of service generated will also generate a large-bandwidth service request waiting to be processed, that is, when n other types of services exist in the network, n high-bandwidth services will also exist. There are 2n services waiting to be processed on the network. As can be seen from the figure, with the increase of the total number of services in the network, the average processing delay of other types of services shows a slow rising trend. However, as the number of services on the network increases, the other two resource allocation methods fail to allocate resources for services within a specified time. As a result, requests are blocked

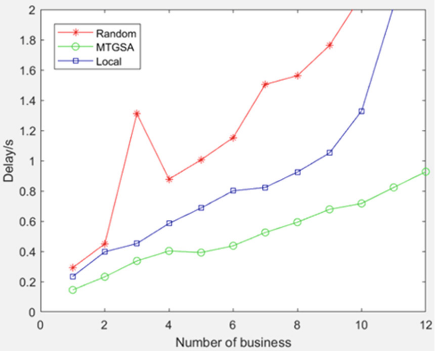


Fig. 5. Average latency of large-bandwidth services

and network throughput decreases. It can be seen that this solution can allocate service resources with low latency, maximize network throughput, and meet resource allocation requirements of more services at the same time (Fig. 6).

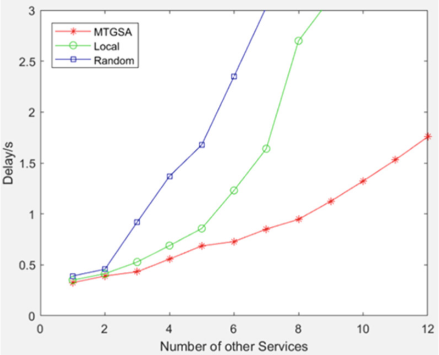


Fig. 6. Average latency of other services

The following figure shows the bandwidth resource utilization of this scheme and the other two schemes in different numbers of services. The following figure shows that as the number of service requests increases, the utilization of bandwidth resources in the network also increases. In the scheme proposed in this paper, the resource utilization increases gently with the increase of the number of services. It shows that the scheme proposed in this paper can efficiently utilize the idle bandwidth resources in the network, while the other two resource allocation schemes cannot be properly allocated with the increase of the number of services, and the service resource demand cannot be met, resulting in no further increase of resource utilization. It also shows that this scheme can achieve the maximum network throughput of service resource allocation. It can be seen that this scheme can efficiently utilize network resources and maximize network throughput (Fig. 7).

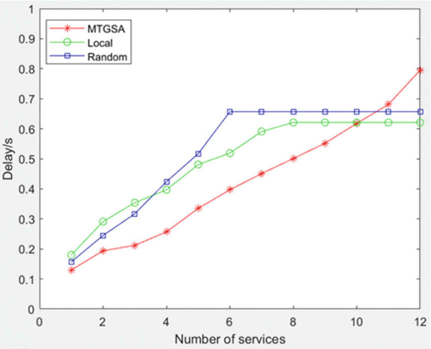


Fig. 7. Bandwidth resource utilization

The following figure shows the delay of a service allocation scheme under different iterations of this scheme and the other two intelligent solving algorithms. As can be seen from the figure below, with the increase of the number of iterations, the three schemes can get the optimal resource allocation scheme after reaching the specified number of iterations. The scheme proposed in this paper can get a better allocation scheme at a faster speed. Although the solution using only genetic algorithm is faster than this scheme, the delay of the optimal allocation scheme obtained is higher than that of this scheme, which reflects that although the genetic algorithm has faster iteration speed, it is easy to fall into the local optimal solution. Although the scheme using only the simulated annealing algorithm can get the optimal solution, it has a certain probability to jump out of the current optimal solution, so the iteration speed is slower and it takes longer time to calculate and solve. It also shows that among the two solving methods, the genetic algorithm is more suitable for fast iteration, while the simulated annealing algorithm is more suitable for small adjustment near the current optimal solution. It reflects the rationality of genetic—simulated annealing algorithm. It can be seen that this scheme can solve the problem quickly in a short time and obtain the resource allocation strategy with the shortest delay, which verifies the correctness and effectiveness of the scheme proposed in this paper (Fig. 8).

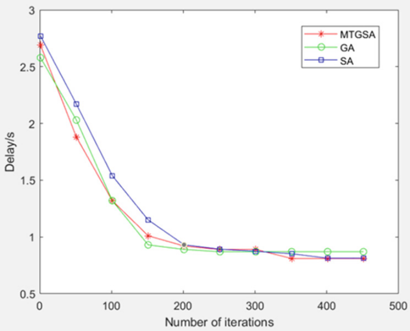


Fig. 8. Different algorithms solve the iterative process

Acknowledgement. This work has been supported by State Grid Corporation of China science and technology project "Research on Local Integrated Communication Network System and Endogenous Security Technologies Oriented to Urban Grid" (5700-202213221A-1-1-ZN).

References

1. Liu, Y.: Research on resource management in 5G heterogeneous networks. Beijing University of Posts and Telecommunication (2019)
2. Wu, Q.: Research on joint resource allocation algorithm for 5G heterogeneous network fusion. Shandong University of Science and Technology (2020). https://doi.org/10.27275/d.cnki.gsdku.2020.000637
3. Meng, Y., Liu, X.: Resource allocation and interference management for multi-layer wireless networks in heterogeneous cognitive networks. Wirel. Com Netw. **190** (2019)
4. Ren, J., Yu, G., Cai, Y., et al.: Latency optimization for resource allocation in mobile-edge computation offloading. IEEE Trans. Wireless Commun. **17**(8), 5506–5519 (2018)
5. Fei, R, Huang, Renchao, et al.: Software defined networking, caching, and computing for green wireless networks. IEEE Commun. Mag. **54**(11):185–193 (2016)
6. Zhou, Y., Yu, F.R., Chen, J., et al.: Resource allocation for information-centric virtualized heterogeneous networks with in-network caching and mobile edge computing. IEEE Trans. Veh. Technol. 1–1 (2017)
7. Zhang, K., Leng, S., Mao, Y.M.: Energy-efficient offloading for mobile edge computing in 5G heterogeneous networks. IEEE Access **4**(99), 5896–5907 (2017)
8. Liu, J., Mao, Y., Zhang, J., et al.: Delay-optimal computation task scheduling for mobile-edge computing systems. IEEE (2016). https://doi.org/10.1109/ISIT.2016.7541539
9. Sardellitti, S., Scutari, G., Barbarossa, S.: Joint optimization of radio and computational resources for multicell mobile cloud computing. In: International Workshop on Signal Processing Advances in Wireless Communications. IEEE (2014)
10. Chen, Q.: Research on key technologies of integrated networking, storage and computing. Beijing University of Posts and Telecommunication (2018)

Fault Diagnosis Mechanism of Virtual Network Service Based on Network Characteristics

Yan Wang[1], Jingze Li[1], Ziyi Zhu[1], Detai Pan[1], and Peng Lin[2](✉)

[1] Hainan Power Grid Communication Branch HaiNan, HaiKou 570203, China
[2] Beijing VectInfo Technologies Co., Ltd., Beijing 100088, People's Republic of China
linpeng@vectinfo.com

Abstract. Efficient fault management method in network virtualization environment has become an important research content. In order to solve the problem of low fault management efficiency caused by large number of power terminals and high network noise, this paper designs a virtual network service fault management model based on network characteristics. The model is constructed based on network features such as network mapping relationship, corresponding relationship between faults and symptoms. The model includes five modules: underlying network, virtual network, network alarm collection center, network mapping management center, and network fault diagnosis center. Based on this model, this paper proposes a virtual network service fault diagnosis mechanism. The mechanism includes six steps: alarm information collection, alarm preprocessing, network mapping, binary Bayesian model, fault diagnosis model optimization, and fault location. Through performance analysis, it is verified that the fault management model and diagnosis mechanism proposed in this paper have good performance and application value.

Keywords: Network virtualization · Virtual network · Underlying layer network · Fault diagnosis · Fault management

1 First Section

With the rapid development and application of 5G technology, the types and number of new applications such as the Internet of Things and smart home have increased rapidly. These new applications require the rapid increase of power communication network resources, which puts forward higher requirements for power companies to build power communication network. In order to meet the network demand and reduce the investment in network construction, network virtualization technology has been adopted by more and more network operators [1]. In the network virtualization environment, the traditional infrastructure is divided into the underlying network and virtual network. The underlying network and virtual network have their respective responsibilities and focus on their own businesses, which has greatly improved the efficiency and resource utilization of network construction. However, in the network virtualization environment, the underlying network and virtual network are constructed and operated by different

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 306–314, 2024.
https://doi.org/10.1007/978-981-99-7161-9_24

organizations or companies, resulting in the low efficiency of network service fault diagnosis [2]. Therefore, efficient fault management method in network virtualization environment has become an important research content.

To solve this problem, literature [3] takes key tasks and tasks with high real-time requirements as the research object, proposes intelligent fault recovery mechanism, and improves the quality of network service. Literature [4] takes the network characteristics such as cell location and fault frequency in the mobile communication network as model parameters, and constructs an automatic fault diagnosis algorithm based on machine learning. Literature [5] extracts alarm feature data from alarm information and proposes a communication network fault analysis algorithm based on alarm feature. Literature [6] combines link fault prediction technology with network tomography technology to improve the performance of network link packet loss inference algorithm. Literature [7] takes key links as the research object, and gives priority to inferring the packet loss of key links in dynamic network environment, ensuring the reliability of key services. Through the analysis of existing research, we can see that many research results have been achieved in network fault diagnosis. However, under the background of the vigorous development of the power Internet of Things and smart home, the number of power terminals and the number of business types have increased rapidly, resulting in complex fault management models and large network noise during fault diagnosis, which has posed a great challenge to existing research. In order to solve the problem of low efficiency of fault management caused by large number of power terminals and large network noise, this paper designs a virtual network service fault management model based on network characteristics, and proposes a virtual network service fault diagnosis mechanism based on this model. Through performance analysis, it is verified that the fault management model and diagnosis mechanism proposed in this paper have good performance and application value.

2 Fault Management Model

According to the characteristics of the network in the network virtualization environment, this paper designs a virtual network service fault management model, as shown in Fig. 1. The model includes five modules: the underlying network, virtual network, network alarm collection center, network mapping management center, and network fault diagnosis center.

The underlying network module and virtual network module belong to the network resource layer. The underlying network is responsible for building the underlying nodes and links. The virtual network can quickly build a virtual network by renting the underlying nodes and links, so as to carry various power services. The network alarm collection center is responsible for collecting alarm information from the underlying network and virtual network to provide data support for the network fault diagnosis center to quickly infer network faults. Because the underlying network and virtual network contain different network elements and realize different functions, the network alarm collection center needs to collect alarm information according to the characteristics of the network.

For the underlying network, the network alarm collection center can collect equipment alarm and link alarm. Device alarm refers to the alarm information generated by

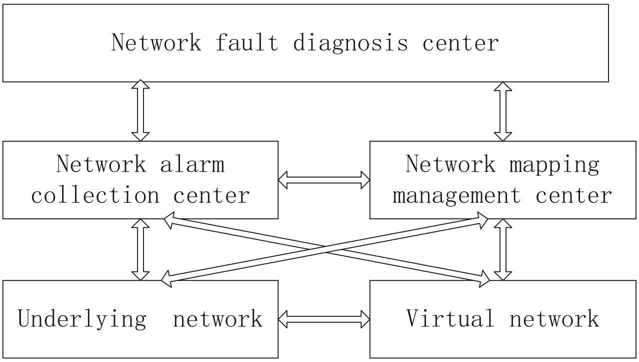

Network fault diagnosis center
Network alarm collection center
Network mapping management center
Underlying network
Virtual network

Fig. 1. Fault management model.

the phenomenon that the performance index of the device is lower than the threshold or the port is abnormal. Link alarm refers to the alarm information generated by the high packet loss rate or link disconnection. For virtual networks, the network alarm center can collect software alarms. Software alarm refers to the alarm information generated by the jamming and unavailability of services on the virtual network.

The network mapping management center is responsible for the resource allocation relationship management of the underlying network and virtual network. Because the alarm information of the underlying network and virtual network collected by the network alarm collection center is different. In order to locate and diagnose the virtual network service fault, it is necessary to associate the alarm information of the underlying network with the alarm information of the virtual network, so as to further infer the source of the fault. In order to achieve this goal, the network mapping management center constructs the mapping management between the bottom node and the virtual node, and the mapping relationship between the bottom link and the virtual link according to the mapping relationship between the bottom network and the virtual network, so as to associate the alarm information of the virtual network service with the alarm information of the underlying network.

The network fault diagnosis center infers the cause of the fault according to the alarm information and resource mapping relationship. This paper mainly addresses the management and location of virtual network service faults. Therefore, the fault diagnosis center first analyzes the virtual network service alarm information, then builds a fault diagnosis model according to the mapping relationship between the underlying network and the virtual network, and finally uses the fault inference model to diagnose the fault. See the next section for specific fault diagnosis process.

3 Virtual Network Service Fault Diagnosis Mechanism

Based on the module composition and cooperation relationship of the fault management model, this paper designs a fault diagnosis mechanism for virtual network services. The mechanism includes six steps: alarm information collection, alarm preprocessing, establishment of network mapping relationship, establishment of binary Bayesian model, optimization of fault diagnosis model, and fault location (Fig. 2).

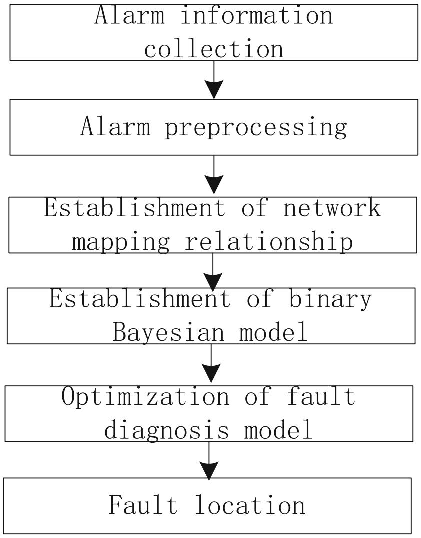

Alarm information collection
Alarm preprocessing
Establishment of network mapping relationship
Establishment of binary Bayesian model
Optimization of fault diagnosis model
Fault location

Fig. 2. Fault diagnosis mechanism of virtual network service.

In the alarm information collection step, the network alarm collection center collects the underlying network alarm information and virtual network service alarm information within each time period T. In terms of the underlying network alarm information, the topology of the underlying network is represented by $G = (N, E)$, where $n_i \in N$ represents the underlying network node information and $e_j \in E$ represents the underlying link information. In terms of virtual network alarm information, the topology of virtual network is represented by $G^V = (N^V, E^V)$, where $n_i^V \in N^V$ represents virtual network node information and $e_j^V \in E^V$ represents virtual link information. In terms of virtual network service description, end-to-end virtual network service is taken as the research object. For example, end-to-end services are represented by S_{ij}^v. Where, virtual nodes n_i^v and n_j^v are the starting and ending nodes of the service respectively.

In the alarm pre-processing step, the network alarm collection center needs to pre-process the collected alarm information to improve the efficiency and accuracy of fault diagnosis. Among them, the pre-processing of the low-level network alarm information refers to clearing the alarms that will not affect the upper-level business. For example, dynamic migration or expansion of underlying resources. The pre-processing of virtual network alarm information refers to clearing the alarms generated by virtual network or virtual network layer services. For example, the alarm information caused by its own software fault.

According to many years of network operation and maintenance experience, alarm data is an important prerequisite for fault diagnosis. If the alarm data collected by the network management system is timely, comprehensive and accurate, it will effectively improve the performance of the fault diagnosis system.

In the aspect of timely acquisition of alarm data, this paper proposes an alarm data acquisition strategy based on network characteristics. Generally speaking, different network equipment alarms have different effects on the availability and reliability of virtual network services. For example, if there are many virtual network devices on the underlying network, the alarms of such underlying network devices will generate more virtual network service exceptions. In order to avoid this situation, set different exception information trigger thresholds for network devices according to their characteristics. Based on this idea, the parameters triggered by the alarm of important underlying network equipment can be adjusted lower to prevent the occurrence of major fault events. Through the analysis of network equipment characteristics and virtual network service resource management strategies, the following network characteristics of the underlying network equipment are used as an important evaluation basis for triggering abnormal alarms. These network features mainly include the number of virtual network resources, resource utilization, and network centrality of resources. The number of virtual network resources carried can reflect the degree of loss caused by the current underlying network failure. When the number of virtual network resources carried by the underlying device is large, the threshold for triggering the alarm is small. The resource utilization rate of the underlying network equipment and the network centrality of the resources are analyzed from the perspective of the correlation of the network equipment. When the resource utilization rate of the underlying network equipment is too high, the probability of network equipment failure is high. When the underlying network equipment belongs to the central resource of the network, the network equipment is more likely to jointly provide virtual network services for other network equipment. Therefore, when the virtual network resources carried on the underlying network are determined, the resource utilization rate and network centrality of the underlying network equipment are the key factors that trigger the alarm.

In terms of comprehensive guarantee of alarm data acquisition, big data storage technology is preferred to save alarm data and relevant parameters in recent years. With the rapid development of computer technology, the software technology and hardware equipment of data storage are rapidly maturing. In terms of software technology for alarm data storage, distributed big data storage technology is preferred to meet the requirements of large capacity and high reliability. In terms of hardware equipment for alarm data storage, disk array equipment is preferred for storage, which can achieve high reliability and scalability at the hardware level. In terms of accuracy assurance of alarm data acquisition, data cleaning, normalization, active detection and other technologies are mainly adopted. Incomplete and duplicate invalid data needs to be deleted in the data cleaning stage. Considering that data cleaning will reduce alarm data and affect the performance of network fault location algorithm. In this paper, active detection technology is used as a supplementary technology for alarm data acquisition. Active detection technology can effectively collect specific network operation data according to the requirements of the fault management platform, and further improve the performance of fault diagnosis.

In the step of establishing network mapping relationship, the network mapping management center associates the alarm information of the underlying network with the alarm information of the virtual network according to the resource allocation relationship between the underlying network and the virtual network. First, the network mapping management center builds the corresponding underlying network model according to the underlying network alarm, and generates the underlying node set and link set that may fail. Secondly, the network mapping management center builds the corresponding virtual network model according to the virtual network alarm, and generates the virtual node set and virtual link set that may fail. Finally, the network mapping management center associates the underlying network alarm information with the virtual network alarm information according to the mapping relationship between the virtual network and the underlying network.

The mapping relationship between low-level network G alarm information and virtual network G^V alarm information is represented by $G^V \downarrow G$. Accordingly, the relationship between underlying node n_i and virtual node n_i^v is represented by $n_i^v \downarrow n_i$, and the relationship between bottom path p_j^s and virtual link e_j^v is represented by $e_j^v \downarrow p_j^s$. The underlying path p_j^s refers to an end-to-end underlying path carrying virtual link e_j^v, which is composed of one or more underlying links.

In the process of building the dichotomy Bayesian model, it includes three sub-processes: building the dichotomy Bayesian model of virtual network service and virtual network, building the dichotomy Bayesian model of virtual network and underlying network, and merging the two Bayesian models. When building a dichotomy Bayesian model, it is necessary to build three steps: the upper node, the lower node, and the connection between the upper and lower nodes. The upper node represents the symptom node, the lower node represents the fault node, and the connection between the upper and lower nodes represents the probability that the upper node is true when the lower node is true. The symptom set composed of m symptom nodes is represented by $S_o = \{s_1, s_2, ..., s_m\}$, and the value of symptom s is 1 or 0. The suspected fault set composed of n suspected faults f is represented by $F = \{f_1, f_2, ..., f_n\}$, and the value of fault f is 1 or 0. The connection between the upper and lower nodes is indicated by $P(s_j|f_i)$. Due to the presence of noise in the network, the probability value generally belongs to the [0,1].

Based on this analysis, in the dichotomy Bayesian model of virtual network service and virtual network, the upper node refers to the alarm information of virtual network service, and the lower node refers to the alarm information of virtual network resources. In the dichotomy Bayesian model of the virtual network and the underlying network, the upper node refers to the alarm information of the virtual network resources, and the lower node refers to the alarm information of the underlying network resources. In the sub-process of merging two Bayesian models, the strategy of node association merging and probability multiplication is adopted. Node association merging refers to the virtual network in the dichotomy Bayesian model of virtual network service and virtual network, and the underlying network resources in the dichotomy Bayesian model of virtual network and underlying network, which are directly merged according to the mapping relationship. Probability multiplication refers to the direct multiplication of the probability value of the node and the probability value of the connection when the nodes are connected, which represents the probability value after the occurrence of two events.

In the step of optimizing the fault diagnosis model, the fault diagnosis center needs to optimize the binary Bayesian model established in the previous step. Because of the large scale of the network and the large number and types of virtual network services, the established dichotomy Bayesian model will have problems of large scale and complex relationship. In this step, the method of fault set filtering is used to optimize the binary

Bayesian model. Among them, the method of fault set filtering is to simplify the fault set according to the ability of fault interpretation. When the fault can explain more symptoms, the fault is considered as a valid fault. When the fault cannot explain the symptoms or the ability to explain the symptoms is weak, the fault is regarded as invalid and can be deleted from the fault set, thus simplifying the binary Bayesian model.

The simplified fault set can simplify the fault diagnosis model, but also lead to the loss of some real faults. In order to avoid the problem of reducing the performance of fault diagnosis due to the loss of real faults, it is necessary to confirm the alarm data after simplifying the fault set. Alarm data confirmation means that each alarm must be associated with at least one fault. The method of alarm data confirmation is to judge whether at least one fault can be associated with it from the perspective of alarm. If an alarm is found to have no corresponding fault, you need to select from the deleted fault set and add its associated fault to the simplified fault set. After adding alarm data confirmation, it can effectively reduce the false alarm rate of fault diagnosis algorithm and improve the performance of fault diagnosis algorithm.

In the fault location step, according to the simplified dichotomy Bayesian model, the number of symptoms that can be explained for each fault is first calculated, and the fault with the largest number of symptoms that can be explained is regarded as the confirmed fault. Iterative execution until all symptoms are explained. Through this method, the implementation efficiency is high. After the fault diagnosis results are sent to the maintenance personnel, the maintenance personnel can quickly identify and maintain the fault information based on the operation and maintenance experience and network detection technology.

According to the operation and maintenance experience, the iterative algorithm is used to calculate the fault interpretation ability and confirm the fault one by one, which can significantly improve the accuracy of fault location. However, it takes a long time to adopt iterative algorithm and calculate the interpretation ability of fault. For the time-sensitive fault diagnosis problem, this fault location method will lead to the reduction of network service quality. In order to solve the problem of time-sensitive virtual network service fault location, this paper proposes to use the technology of knowledge map to solve it. Because the knowledge map technology can use the strategy of association graph to associate the anomaly of virtual network service with the result of fault location, which greatly improves the efficiency of network fault location.

In order to apply the knowledge map to the time-sensitive virtual network service fault diagnosis problem, it is necessary to perform five steps: exception symptom extraction and fault association, knowledge map database creation, virtual network service exception symptom capture, exception symptom and fault matching, and return result optimization. In the process of knowledge map database creation, this paper uses the graphic database Node4j to create. The creation process mainly includes database field design, data attribute association, data attribute graphical optimization and other processes. The purpose of the return result optimization step is to process the knowledge in the knowledge map in natural language, so that the operation and maintenance personnel can understand the operation results of the system and quickly apply it to the operation and maintenance work. Therefore, this paper associates the faults and alarms confirmed by the operation and maintenance personnel and stores them into the knowledge map, which can significantly improve the efficiency of fault location, and solve the problem of long fault location time of time-sensitive virtual network services.

4 Performance Analysis

The performance analysis includes the feasibility of fault management model and the performance of fault diagnosis mechanism.

The feasibility of fault management model can be divided into two aspects: the feasibility of model construction and the feasibility of model fault management capability. In terms of the feasibility of the model construction, the five modules included in the model can be realized from the technical and functional levels, and are necessary functions. Among them, the underlying network and virtual network, as the managed objects, are the necessary functional modules. The three modules of network alarm collection center, network mapping management center and network fault diagnosis center provide necessary elements and functions for fault management from three aspects of alarm collection, resource mapping and fault diagnosis. As for the feasibility analysis of the model's fault management capability, the model effectively realizes the five fault diagnosis processes of alarm collection, alarm optimization, fault diagnosis model construction and optimization, and fault location through the cooperation of five modules. It has strong environmental adaptability and can better achieve the fault management capability.

In terms of the performance of the fault diagnosis mechanism, the accuracy and complexity of the fault diagnosis mechanism can be analyzed. In terms of the accuracy of the fault diagnosis mechanism, the fault diagnosis mechanism in this paper can construct and combine the model from three aspects: the dichotomy Bayesian model of the virtual network service and the virtual network, the dichotomy Bayesian model of the virtual network and the underlying network, and the combination of the two Bayesian models, so as to ensure the integrity and accuracy of the fault diagnosis data and provide relatively complete data for the fault diagnosis mechanism. The accuracy of fault diagnosis mechanism is guaranteed. In terms of the complexity of fault diagnosis mechanism, this paper adopts two processes of alarm information optimization and fault model optimization to effectively reduce the complexity of fault diagnosis model. In addition, when optimizing the model, the complexity of fault diagnosis algorithm is better reduced on the premise that all abnormal symptoms can be located and the complexity of fault is reduced.

It can be seen from the above analysis that the fault management model and diagnosis mechanism proposed in this paper can better realize the fault management of virtual network service, and has better accuracy and lower complexity in the performance of fault diagnosis.

5 Conclusion

In order to improve the utilization of network resources and reduce the cost of network construction, network virtualization technology has become a key technology of network construction. In order to improve the service quality of virtual network, efficient fault management methods in network virtualization environment have become an important research content. In order to solve the problem of low efficiency of fault management caused by large number of power terminals and large network noise, this paper designs a virtual network service fault management model based on network characteristics, and proposes a virtual network service fault diagnosis mechanism based on this model. Through performance analysis, it is verified that the fault management model and diagnosis mechanism proposed in this paper have good performance and application value. With the increase of the number of underlying network providers, the virtual network service fault management is facing problems such as the increase of the number of network participants and the difficulty of obtaining network management data. In the next work, based on the research results of this paper, we will further study the fault management model and fault diagnosis mechanism under the environment of multiple network providers.

Acknowledgments. This work is supported by science and technology project from Hainan Power Grid Communication Branch: "Automatic Operation Decision System Based on Intelligent Fault Location and Identification".

References

1. Afolabi, I., Taleb, T., Frangoudis, P.A., et al.: Network slicing-based customization of 5G mobile services. IEEE Netw. **33**(5), 134–141 (2019)
2. Wen, R., Feng, G., Tang, J., et al.: On robustness of network slicing for next-generation mobile networks. IEEE Trans. Commun. **67**(1), 430–444 (2018)
3. Zheng, J., Xu, H., Zhu, X., et al.: Sentinel: failure recovery in centralized traffic engineering. IEEE/ACM Trans. Netw. **27**(5), 1859–1872 (2019)
4. Chen, K.M., Chang, T.H., Wang, K.C., et al.: Machine learning based automatic diagnosis in mobile communication networks. IEEE Trans. Veh. Technol. **68**(10), 10081–10093 (2019)
5. Ji, X., Shi, X., Han, J., et al.: The alarm feature analysis algorithm for communication network. In: Proceedings of the 9th International Conference on Computer Engineering and Networks, pp. 255–265. Springer, Singapore (2021)
6. Li, H., Gao, Y., Dong, W., et al.: Taming both predictable and unpredictable link failures for network tomography. In: Proceedings of the ACM Turing 50th Celebration Conference-China, pp. 1–10 (2017)
7. Li, H., Gao, Y., Dong, W., et al.: Preferential link tomography in dynamic networks. IEEE/ACM Trans. Netw. **27**(5), 1801–1814 (2019)

Large-Scale Deterministic Network Time Sensitive Traffic Scheduling Mechanism with Joint Routing and Queuing

Yi Cao[1], Junhong Weng[1], Qiong Xu[1], and Peng Lin[2](✉)

[1] Shenzhen Power Supply Co., Ltd, Beijing 518000, China
[2] Beijing Vectinfo Technologies Co., Ltd, Beijing 100088, China
1846248750@qq.com

Abstract. Aiming at the deterministic delay problem of time-sensitive traffic in large-scale deterministic networks, a joint routing and queue scheduling mechanism for time-sensitive network traffic is proposed. In order to solve the defects of the current scheduling mechanism, the scheduling mechanism proposed in this paper designs the real-time online scheduling model of joint routing and circular forwarding queue through the system architecture of the circular queue forwarding (CQF) mechanism based on the distributed SDN architecture and time sensitive network (TSN). Based on the DDQN algorithm, the model comprehensively considers the network status such as node queue, link capacity, feasible path, congestion information, and other traffic factors such as different levels of bounded delay requirements to achieve optimal scheduling of time-sensitive flows, aiming to improve the scheduling success rate and reduce delay and packet loss. By comparing this mechanism with the shortest path algorithm based on CQF mechanism and the DRL path selection algorithm based on CQF mechanism, the simulation results show that the proposed mechanism can flexibly adjust the transmission scale of traffic according to the resource usage of the network in the large-scale scheduling scenario, effectively improve the scheduling performance, and reduce the overall end-to-end delay.

Keywords: Deterministic Network · Deep Reinforcement Learning · Route Selection

1 Introduction

With the advent of the 5G era, many emerging businesses appear, forcing the network to upgrade in terms of delay and jitter. IEEE 802 Working group and Deterministic network (DetNet) working group of IETF have proposed the concept of time-sensitive network (TSN) to guarantee deterministic delay at physical layer and link layer, and guarantee network layer (L3) and higher level of wide area deterministic network technology [1].

TSN uses network-wide clock synchronization, time-aware shaper (TAS), and cyclic queuing and forwarding (CQF). It realizes the common network transmission of time-sensitive flows and non-real-time flows within the LAN [2]. The DetNet Working group

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 315–327, 2024.
https://doi.org/10.1007/978-981-99-7161-9_25

proposes a cycle specified queuing and forwarding (CSQF) mechanism. Based on CQF, CSQF relaxes synchronization constraints and allows packets to be routed and scheduled using segment routing, with multiple additional queues caching data. Based on the above two mechanisms, a large number of studies have emerged on scheduling mechanisms for deterministic delay problems.

Literature [3] proposes an integer linear programming (ILP) for routing and scheduling, which takes end-to-end delay and scheduling success rate as indicators, accelerates the solution through ILP solver, and reduces the size of the problem by deleting link-independent mapping conditions. The gate control list (GCL) is generated based on the ILP computational formula, and resources are optimally allocated to time-triggered traffic by calculating global scheduling. Literature [4] proposes a topology pruning strategy and a flow grouping strategy based on spectrum clustering to avoid the impact of the sharp increase in network topology size and traffic size on the scheduling response speed and improve the scheduling calculation efficiency. Literature [5] proposes a heuristic scheduling algorithm based on genetic algorithm based on the joint constraint of routing and scheduling of time-sensitive flows as a gene, which generates static global scheduling, thus improving the scheduling performance, transmission efficiency and network resource utilization of time-delay sensitive flows.

Literature [6] proposes that most of the traditional model-based network resource allocation methods only aim at the optimal solution of the network snapshot and cannot solve the problem of how to adjust or recalculate the resource allocation to adapt to the highly time-varying communication network. It proposes to introduce the deep reinforcement learning (DRL) method to learn how to control the communication network according to human experience, rather than the precise and mathematically solvable system model (such as queuing model), so as to enhance the applicability in the complex network with random and unpredictable behavior. Literature [7] deals with the online flow allocation problem based on the method of deep reinforcement learning, which relies on the asynchronous traffic shaper of the underlying TSN network and the ATS performance model to check the feasibility of the actions sent by the agent, predefine the number of hops, and give the action vector composed of the ATS priority of each hop and the proportion of the total delay. Literature [8] proposes that the next hop node can be selected in a node state to reach the next hop node to obtain a new state. It is very suitable to use the deep reinforcement learning method to model, so that the transmission path is not directly allocated for the data flow in advance, and the DRL model of the data packet can flexibly forward according to the perceived dynamic changes of the network during the transmission process and its own delay requirements.

In contrast, the scheduling mechanism based on DRL can adapt to the complex network topology and real-time traffic scheduling, but the static global path of its output cannot control the flow according to the change of future network status faster, so as to avoid the resource contention problem caused by the subsequent traffic changes in the transmission process. In order to solve the above problems, this paper studies the scheduling problem of time-sensitive flows in large-scale deterministic networks. The specific contributions are as follows.

A system architecture of joint routing and queuing is proposed. Based on the SDN architecture and the CQF mechanism of TSN, the forwarding direction of the flow is constrained to reach the destination node through the reachable path. After that, the scheduling action granularity is refined, from selecting the complete path to selecting the next hop node, so that the flexible forwarding of time-sensitive flow can be realized according to the real-time environment information.

The problem optimization model of routing queue joint scheduling is established. Based on the Double Deep Q-network (DDQN) algorithm, the flow information and the queue capacity and link capacity of the current node collected by the SDN controller, as well as the cache information composition state of the neighboring nodes, and the internal delay of the flow at the previous node and the congestion information related to the queue processing in the current super cycle when the flow arrives at the node constitute the reward value, Thus, network resources are fully utilized to reduce the packet loss rate and delay of time-sensitive flows.

2 System Architecture

For large-scale time-sensitive flow networks, this section designs a scheduling mechanism of joint routing and periodic cyclic priority queue starting from the system architecture. The system architecture is shown in Fig. 1.

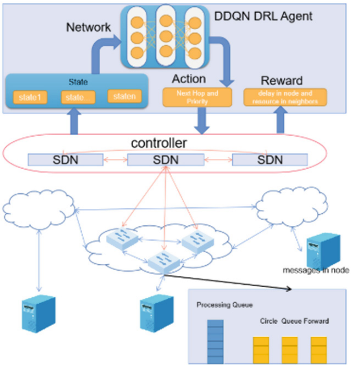


Fig. 1. System architecture diagram

Because the scale of nodes is too complex and huge in the real large-scale network, and the processing capacity of the centralized control platform is limited, the cost of collecting a complete global view in real time is too high, which limits the network size that can be applied.

Therefore, based on the distributed SDN architecture, the scheduling mechanism divides the large-scale time-sensitive flow network into corresponding transmission domains under the control of multiple SDN controllers.

The partition method of the transmission domain can refer to the topology partition algorithm based on the minimum f-balanced edge cut proposed in literature [10], or the controller deployment algorithm based on the correlation degree, or other relevant documents on the distributed SDN deployment, and the partition deployment can be carried out under the premise of balancing the effect and cost.

Each SDN controller is responsible for collecting the nodal information and link information of the local area network corresponding to the transport layer and processing the scheduling of end-to-end time-sensitive flows in the region.

In addition, because the DRL model has a long learning process in an unknown dynamic environment, it cannot meet the strict requirements of the system for delay.

Therefore, the DRL model trains the learning strategy offline, and then makes online decisions in a short execution time according to the trained model.

The problem of cross-domain transmission between SDN controllers is solved through the Border Gateway Protocol (BGP).

The SDN controller will specify the transmission node corresponding to the next transmission domain as the temporary destination node for transmission.

Under the same SDN controller, each programmable switch, as a transmission node, needs to maintain the queue to be processed and the multi-level priority queue based on the CQF mechanism of TSN, monitor the node queue, link capacity and other environmental conditions, and record the initial arrival time of each flow, and calculate the nodal delay.

In each transmission cycle, the node will first allocate the recorded data flow in the flow table to the transmission queue, and then upload the recorded delay data, the snapshot of the current environment state and the remaining flow information of the queue to the SDN controller for scheduling.

Each SDN controller is trained with a deep reinforcement learning model based on the DDQN algorithm, which can train the optimization model through the collected delay data as the reward of the environment feedback and output the scheduling action including routing and priority queue for the node's data packets to be processed through the pre-calculated constraints and environment status.

Finally, the SDN controller will send the flow table of the scheduling action to the programmable switch.

The switch allocates the flow to the priority queue of the corresponding routing port according to the flow table and transmits the packet of the flow to the next hop in the next cycle.

3 System Model

3.1 Problem Model

For the system architecture shown in Fig. 1, the network topology set is divided into M transmission domains in total, so the network topology set is $G = \{G^f = \{V^f, E^f\} | f \in M\}$. We can model the network topology corresponding to each SDN controller into the corresponding undirected graph G^f. Where $V^f = \{v_0^f, ..., v_n^f\}$ represents the collection of N^f switching nodes in the SDN controller, and $E^f = \{e_{ij}^f | i, j \in N, i \neq j\}$ represents the collection of physical links. In addition, $A^f = R_{nxn}$ represents the adjacency matrix of G^f, that is, the connection between the internal exchange node i and node j, when $e_{ij}^f \in E^f$, $a_{ij}^f = 1$, when $e_{ij}^f \notin E^f$, $a_{ij}^f = 1$, let the weight BW_{ij}^f of the side e_{ij}^f represent the bandwidth limit of the link.

At the same time, each switch node i is required to have K ports, $P_i^f = \{p_{i,0}^f, \ldots p_{i,0}^f\}$. At the same time, record the neighbor switching node $Neighbor_i^f = \{nbr_{i,0}^f, \ldots nbr_{i,0}^f\}$ corresponding to node i port. If there is no neighbor node, set it to—1. In addition, node i needs to maintain two kinds of virtual queues, one is the queue to be processed $queue_{proc}^{f,i}$, which collects all the stream data frames of all ports for scheduling.

The other is the pMax priority queues $queue_{proc}^{f,i} = \{q_{pr}^{f,i,p} | pr \in pMax, p \in K\}$ used by each port p of node i for periodic cyclic transmission.

Among them, the queue to be processed, $queue_{proc}^{f,i}$ will be scheduled for processing according to the priority of data frames in the queue from high to low. The scheduling method is to first find the set flow table, schedule the flow that finds the matching item to the corresponding priority queue of the corresponding port, or the flow table cannot find the corresponding information, and finally forward all the unmatched flow information and the environment status to the SDN controller for decision, and then issue the flow table according to the decision for processing. Priority queue $queue_{trans}^{f,i,p}$ determines the current sending queue according to the order of priority, and the data frames in the same queue are sent according to the FCFS principle. In order to avoid congestion, the maximum queue length $procNum$ is uniformly set for queue to be processed, $queue_{proc}^{f,i}$, and the maximum value of the sum of the queue length of priority queues, $\sum_p^K queue_{trans}^{f,i,p} = \sum_p^K \sum_{pr}^{pMax} q_{pr}^{f,i,p}$, is uniformly set to $transNum$. Assume that the equal length over cycle duration of all nodes is C, and the unit is s. All priority queues in each cycle are sent circularly, and the transmission rate of each link is v_{trans}, and the unit is bps. In order to unify the different transmission cycle periods of time sensitive flows, make the transmission set over cycle C equal to the least common multiple of all time sensitive flows, as shown in formula (1).

$$C = LCM\left(period_i\right) \tag{1}$$

In order to ensure that the flow with successful bandwidth reservation can send the subsequent data frames successfully, for the minimum data frame length of 64B, the maximum value of the sum of the queue length of each priority $queue_{trans}^{f,i,p}$ of each node port p is shown in formula (2).

$$transNum = C/(64 * 8/v_{trans}) = 512C/v_{trans} \tag{2}$$

Related to this, the pending queue $queue_{proc}^{f,i}$, which is scheduled to the priority queue of each port, needs to cache all data frames of each node port for processing by the SDN controller in the worst case, so the maximum queue length is shown in formula (3).

$$procNum = K * transNum \tag{3}$$

There are FT transport tasks on the entire transport layer, which are represented as a set $FL = \{flow_0, \ldots, flow_{ft-1}\}$.

Each task can be abstracted as a flow, which is represented as a tuple $flow_i = \{id_i, n_{src,i}, n_{dst,i}, idx_{start,i}, idx_{end,i}, pr_i, d_i, t_i, bw_i, period_i, done_i\}$.

Where $n_{src,i}$ and $n_{dst,i} \in V^f = \{v_0^f, \ldots, v_n^f\}$ are the source node and destination node addresses of $flow_i$ respectively, and the value range is the address of any node in M

transmission domains.id_i indicates that the ID of the flow in a transmission domain G^f is convenient for matching the flow table, and $idx_{start,i}$, $idx_{end,i}$ indicate the subscript of the start and end nodes of the flow in a transmission domain G^f, which is convenient for the corresponding SDN controller to find the corresponding reachable path set.

$pr_i, d_i, t_i, bw_i, period_i, done_i$ represents the transmission priority of the flow, the maximum delay allowed for transmission, the transmission start time, the bandwidth required for transmission, the transmission period, and the symbol of the end of transmission. Each priority will correspond to a delay upper limit.

And when $done_i$ is 1, it means that the transmission is over, and the occupied bandwidth is released.

And before starting the transmission task, each SDN controller needs to solve the reachable path set $Path^{f,pr}_{start,end}, f \in M, pr \in pMax, start, end \in N^f$ for any starting and ending points $idx_{start,i}$, $idx_{end,i}$ of the $flow_i$ with different priorities in the transmission domain G^f. Where, $start, end$ denote the start and end subscripts, and the average delay of any $path^{f,pr}_{start,end} \in Path^{f,pr}_{start,end}$ should not be greater than the maximum delay of the corresponding priority.

After that, based on $Path^{f,pr}_{start,end}$, each node calculates the next hop nodes set, $rn^{f,pr,cur}_{start,end}$ that can make the flow reach $n_{dst,i}$ in time. Where cur represents the subscript of the current node. The set of all reachable path nodes is $RN^{f,pr}_{start,end} = \{rn^{f,pr,cur}_{start,end}, f \in M, pr \in pMax, start, end \in N^f\}$.

The goal of the scheduling mechanism in this paper through joint routing and queuing operations is to make full use of the fine-grained forwarding actions of network resources and comprehensively consider the priority and delay constraints of traffic, reasonably schedule low-priority traffic without affecting the delay certainty of high-priority time-sensitive flow, and avoid the occurrence of timeout, so as to minimize the weighted delay of FT transmission tasks with multi-priority traffic, Its objective function is shown in formula (4).

$$\frac{\sum_i^{ft} pr_i * Delay_i}{\sum_i^{ft} pr_i} \tag{4}$$

where, $Delay_i$ refers to the end-to-end delay of $flow_i$.

3.2 Mathematical Constraints

Transmission Delay Constraint. Obviously, each node should ensure that the time delay experienced by $flow_i$ does not exceed its specified maximum time delay, as shown in formula (5).

$$t_{now} - flow_i.t_i \le flow_i.d_i \tag{5}$$

Reservation Bandwidth Constraint. For any node a and b in any transmission domain, the bandwidth BW^f_{ab} of the link e^f_{ab} between the nodes a and b should not be less than the sum of the reserved bandwidth of several flows on it, as shown in formula (6).

$$BW^f_{ab} \ge \sum flow.bw \tag{6}$$

Reachable Path Node Set Constraint. Obviously, the scheduling mechanism of simply selecting the next hop node for $flow_i$ at each node cannot guarantee that the next hop must make the $flow_i$ close to the direction of $n_{dst,i}$, and may also deviate. Therefore, an explicit routing strategy is necessary.

Because the scheduling mechanism in this paper subdivides the large-scale transmission network into M smaller transmission domains, which reduces the calculation scale, the SDN controller of each transmission domain can quickly and efficiently solve the reachable path set $Path^{f,pr}_{start,end}, f \in M, pr \in pMax$ at any start and end of the transmission domain of each priority and the reachable path node set $RN^{f,pr}_{start,end} = \{rn^{f,pr,cur}_{start,end}, f \in M, pr \in pMax, start, end \in N^f\}$. At the same time, in order to prevent link loopback, the reachable path set should not contain nodes that have passed the flow.

Finally, the DRL model on the SDN controller outputs action $act^{f,x}_{i,t}$ for $flow_i$ at node x. The k-th routing port $p^f_{x,k}$ should meet the constraint shown in formula (7).

$$p^f_{x,k} \in rn^{f,pr,cur}_{start,end} \tag{7}$$

The routing port $p^f_{x,k}$ is the corresponding port of the reachable path node that meets the starting and ending point of $start$, end and priority of pr.

4 Algorithm Design

4.1 Algorithm Three Elements

State. In this scheduling mechanism, the state refers to the flow request information and network information in the network parsed by the data analysis agent. For each time slot T, the SDN controller in the corresponding region will collect the relevant network status and the flow request information uploaded by the node. In order to prevent the flow from being over centrally scheduled to a node, which causes the packet loss rate to rise, the status factor should consider the priority queues capacity of K corresponding ports of node i, and the processing queue capacity of K neighbor nodes, as shown in formula (8) and (9).

$$Qu^{f,i}_{trans} = \left\{queue^{f,i,p}_{trans} | p \in K\right\} \tag{8}$$

$$Qu^{f,i}_{proc} = \left\{queue^{f,nbr^{f,i}_p}_{proc} | p \in K\right\} \tag{9}$$

And the links capacity of node i corresponding to neighbor nodes at time t, as shown in formula (10).

$$EBW^{f,i}_t = \left\{ebw^{f,i}_{t,nbr^{f,i}_p} | p \in K\right\} \tag{10}$$

To sum up, the state representation of *flow*$_j$ on node i at time t is shown in formula (11).

$$S_{j,t}^{f,i} = \left\{pr_j, bw_j, Qu_{proc}^{f,i}, EBW_t^{f,i}, Qu_{proc}^{f,i}, rn_{start,end}^{f,pr,i}\right\} \tag{11}$$

where pr_j, bw_j are the priority of *flow*$_j$ and the reserved transmission bandwidth. $rn_{start,end}^{f,pr,i}$ is to find all the neighbor nodes of the current node i in the reachable path set of the corresponding *flow*$_j$, remove the nodes that have experienced, avoid the loopback of the link, and restrict the ports that may be forwarded, so that the *flow*$_j$ can reach the specified target node.

Action. In this scheduling mechanism, the scheduling action is more fine-grained, from selecting a path across a large-scale network to selecting the priority queue and the next hop node to send, so that it can feel the fluctuations of the network in the environment, use network resources as much as possible, and reduce the overall delay increase caused by network congestion, etc.

Therefore, the action of *flow*$_j$ on node i represents $act_{j,t}^{f,i}$ as shown in formula (12) Where, $p_{x,k}^{f}$,pr_y respectively represent the x-th port of node i and the y-th priority queue sent periodically by the port.

$$act_{j,t}^{f,i} = \left\{p_{x,k}^{f}, pr_y | x \in K, y \in pMax\right\} \tag{12}$$

Reward. The design of the reward value of the environment is the evaluation of the benefits obtained from the selected actions. Where, the penalty value is the reward when the restriction in Sect. 3.3 above is not valid, as shown in formula (13).

$$PV_t = pr_j * \left[w_1 * (t_{now} - t_i) + w_2 * \left(bw_j - ebw_{t,nbr_x^{f,i}}^{f,i}\right) + w_3 * Z\right] \tag{13}$$

where, $w_1 = w_2 = w_3 = -1$, when the corresponding constraint is not tenable, and 0 when it is tenable. Z is a positive integer, which is used to indicate the penalty for selecting a non-reachable path node.

The reward value mainly considers two aspects: first, reduce the weighted delay of the flow at the current node to avoid timeout; secondly, it is necessary to make full use of network resources to reduce the increase of delay caused by network congestion, so when it arrives at the next hop node, the packet congestion information that has been processed or will be processed before itself will be used as a supplement to the reward value.

Therefore, the positive return is shown in formula (14). Where, β,μ are the corresponding weight values.

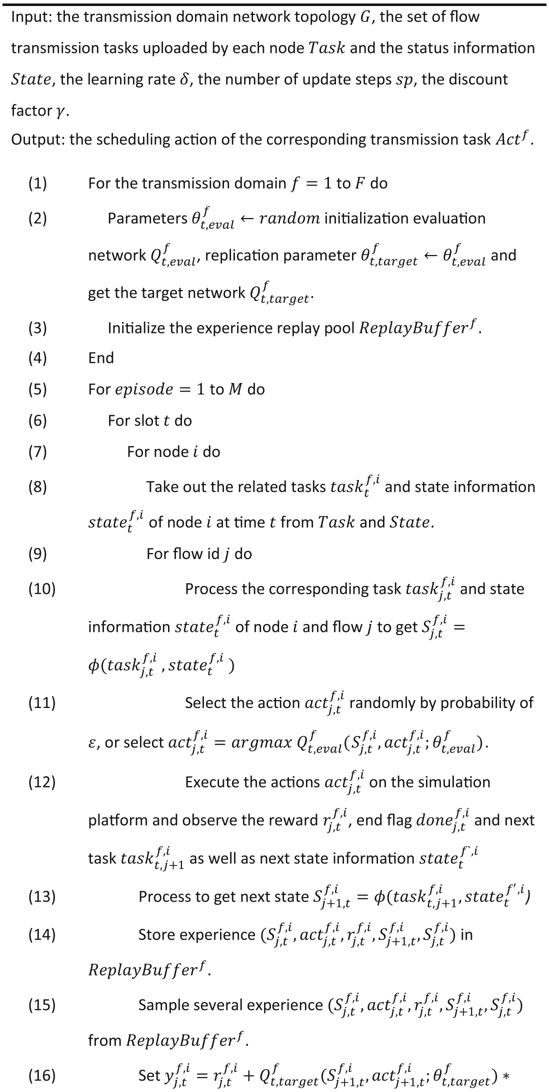
$$RV_t = \beta * pr_j * (C - D_{node,j}) + \mu * (procNum - queue_{proc}^{f,nbr_p^{f,i}} - \sum_{p}^{K} queue_{trans}^{f,nbr_x^{f,i},p}) \tag{14}$$

Therefore, the reward function of *flow*$_j$ on node i at time t is shown in formula (15).

$$r_{j,t}^{f,i} = \alpha * PV_t + (1-\alpha) * RV_t \tag{15}$$

where, if penalty value is not zero, then α is 1, and the end flag of *flow*$_j$,*done*$_j$ is 1. Or the weighted delay of the current node and the congestion information of the next-hop neighbor node $nbr_x^{f,i}$ jointly constitute $r_{j,t}^{f,i}$. When the next hop is the destination node, μ is considered as 0.

4.2 Joint Routing and Queuing Scheduling Algorithm Based on DDQN



Input: the transmission domain network topology G, the set of flow transmission tasks uploaded by each node $Task$ and the status information $State$, the learning rate δ, the number of update steps sp, the discount factor γ.

Output: the scheduling action of the corresponding transmission task Act^f.

```
For the transmission domain $f = 1$ to $F$ do
    Parameters $\theta_{t,eval}^f \leftarrow random$ initialization evaluation network $Q_{t,eval}^f$, replication parameter $\theta_{t,target}^f \leftarrow \theta_{t,eval}^f$ and get the target network $Q_{t,target}^f$.
    Initialize the experience replay pool $ReplayBuffer^f$.
End
For $episode = 1$ to $M$ do
    For slot $t$ do
        For node $i$ do
            Take out the related tasks $task_t^{f,i}$ and state information $state_t^{f,i}$ of node $i$ at time $t$ from $Task$ and $State$.
            For flow id $j$ do
                Process the corresponding task $task_{j,t}^{f,i}$ and state information $state_t^{f,i}$ of node $i$ and flow $j$ to get $S_{j,t}^{f,i} = \phi(task_{j,t}^{f,i}, state_t^{f,i})$
                Select the action $act_{j,t}^{f,i}$ randomly by probability of $\varepsilon$, or select $act_{j,t}^{f,i} = argmax\ Q_{t,eval}^f(S_{j,t}^{f,i}, act_{j,t}^{f,i}; \theta_{t,eval}^f)$.
                Execute the actions $act_{j,t}^{f,i}$ on the simulation platform and observe the reward $r_{j,t}^{f,i}$, end flag $done_{j,t}^{f,i}$ and next task $task_{t,j+1}^{f,i}$ as well as next state information $state_t^{f',i}$
            Process to get next state $S_{j+1,t}^{f,i} = \phi(task_{t,j+1}^{f,i}, state_t^{f',i})$
            Store experience $(S_{j,t}^{f,i}, act_{j,t}^{f,i}, r_{j,t}^{f,i}, S_{j+1,t}^{f,i}, S_{j,t}^{f,i})$ in $ReplayBuffer^f$.
            Sample several experience $(S_{j,t}^{f,i}, act_{j,t}^{f,i}, r_{j,t}^{f,i}, S_{j+1,t}^{f,i}, S_{j,t}^{f,i})$ from $ReplayBuffer^f$.
            Set $y_{j,t}^{f,i} = r_{j,t}^{f,i} + Q_{t,target}^f(S_{j+1,t}^{f,i}, act_{j+1,t}^{f,i}; \theta_{t,target}^f) *$
```

```
                $done_{j t}^{f i})$
                Use loss function $L(\theta_{t,eval}^{f}) = E[(y_{j,t}^{f,i} - Q_{t,eval}^{f}(S_{j,t}^{f,i}, act_{j,t}^{f,i}; \theta_{t,eval}^{f}))^2]$ to update evaluation network :
                $\theta_{t,eval}^{f} \leftarrow \theta_{t,eval}^{f} + \delta \nabla_{\theta_{t,eval}^{f}} L(\theta_{t,eval}^{f})$
                Update target network $Q_{t,target}^{f} \leftarrow Q_{t,eval}^{f}$ per $sp$ steps.
            End
        End
    End
End
```

5 Simulation Experiment

5.1 Experimental Environment

This paper uses Python 3.9 networks module package to generate network topology and uses Python to build DRL model and conduct training. Considering the complexity of the integrated network environment, this paper randomly generates a large-scale network scenario with 100 nodes. Among them, 10 nodes are selected as terminals, which are the start and end nodes of flow transmission, and the remaining nodes are transmission nodes. The capacity of each link is set to 10 Mbit/s, and the link delay is 1 ~ 10 ms. Each node port has three CQF mechanisms with different priority queues for deterministic traffic transmission. The capacity of each queue is 1Mbit, and the cycle of cyclic forwarding is C = 10 ms. According to the characteristics of time-sensitive flows, this paper generates time-sensitive flows with random sources and destination nodes. All flows are generated continuously. The generation time and bandwidth requirements are subject to Poisson distribution. The maximum delay allowed is related to the shortest path under the corresponding priority of the start-stop node. In this paper, 1000 streams with three different priorities and periods are deployed in the network, which are 2 ms, 5 ms and 10 ms respectively. At the same time, the simulation time is set to be 100 s, aiming at simulating the network environment of high strength receiving and sending streams.

5.2 Results and Analysis

In order to evaluate the performance of the designed scheduling mechanism, this paper collects the flow information and all node information as the state by combining it (RPJH-CQF, ReachablePath-Jam-Hop-CQF), the shortest path scheduling mechanism based on CQF mechanism (SP-CQF, ShortestPath-CQF), and the CQF mechanism, Compare the scheduling mechanism of path selection (KSP-CQF, KShortestPath-DRL-CQF) through DRL model. The indicators of scheduling performance evaluation are scheduling success rate and average weighted delay.

The Impact of Traffic Size on Scheduling Performance. Figure 2 shows the change of scheduling success rate of several strategies as the network traffic size increases.

As can be seen from the figure, with the increase of the number of flows, the intensity of resource competition intensifies, and the success rate of each strategy gradually decreases. However, the scheduling success rate of RPJH-CQF strategy is higher than that of other strategies. This is mainly because the algorithm forwards the flow to the appropriate neighbor nodes according to the real-time link capacity and the congestion degree of neighboring nodes, thus improving the scheduling success rate.

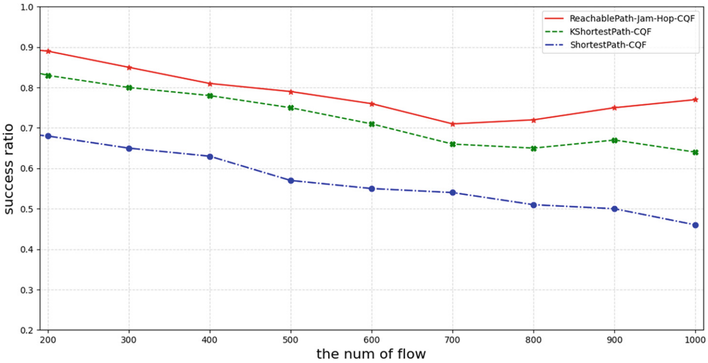


Fig. 2. The change of scheduling success rate with the number of flows

On the other hand, Fig. 3 shows the proportion of the actual average weighted delay of each strategy to the theoretical average weighted delay. Among them, RPJH-CQF strategy has a more stable proportion than other strategies. This is because according to the real-time network status, the flow data frame is flexibly forwarded among nodes that meet the constraints of feasible node set, thus reducing the average weighted delay. However, after the KSP-CQF strategy and SP-CQF strategy select the path, the stream data frame can only be forwarded to the specified node, resulting in excessive concentration of some node data packets, and thus the weighted delay is too large.

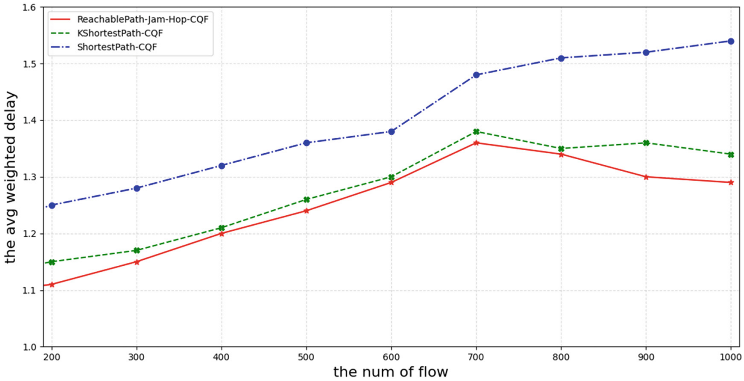


Fig. 3. Variation of the ratio of actual average weighted delay to theoretical delay with the number of time-sensitive flows

The Impact of Network size on Scheduling Performance. In order to explore the impact of different network sizes on scheduling strategies, this paper randomly generates two networks of different sizes, including 50,100, and the number of time-sensitive flows is 1000. Figure 4 shows the change of scheduling success rate of several strategies as the network size increases. It can be seen from the figure that when the number of flows remains unchanged, the performance of each strategy will improve with the increase of the number of network nodes. RPJH-CQF strategy optimization is obvious. When the number of network topologies is small, due to the constraints of feasible paths, the transmission paths between flows overlap more, which leads to some link overloads and large internal delay of corresponding nodes; When the network size increases and feasible paths increase, for the RPJH-CQF strategy, the next hop can be selected from more suitable feasible path nodes, thus effectively alleviating the above situation.

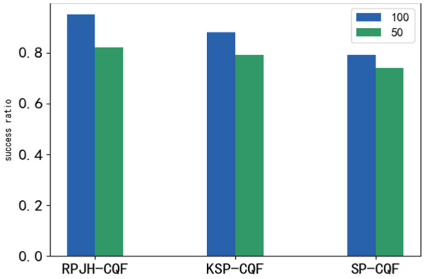


Fig. 4. The change of scheduling success rate under different network scales

As shown in Fig. 5, with the increase of network size, more alternative paths and nodes can bring better performance, so the packet loss rate of various scheduling mechanisms has decreased slightly, among which, RPJH-CQF has a lower packet loss rate. This is due to the RPJH-CQF policy, which relaxed the path constraints of the flow, so that the flow of packets can experience more route hops in an acceptable degree, so as to effectively utilize the resources of the surrounding nodes and avoid the overflow caused by the concentration of packets on a certain node.

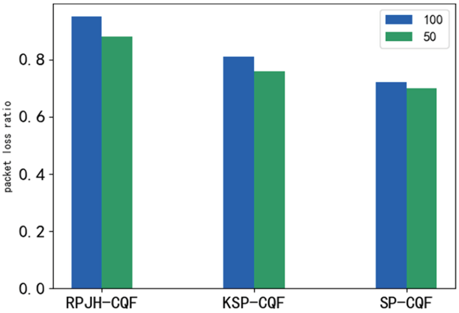


Fig. 5. The change of packet loss rate under different network scales

6 Conclusion

According to the relevant technical concepts of TSN, aiming at the deterministic delay problem of time-sensitive traffic in large-scale deterministic networks, this paper proposes a scheduling mechanism for joint routing and queuing of time-sensitive network flows to ensure the delay certainty and scheduling success rate of time-sensitive flows. The mechanism proposed in this paper is to schedule and select the priority of the next hop node and the sending queue, and realize flexible and reliable hop-by-hop forwarding of time-sensitive flows through the constraints of the feasible path node set; At the same time, considering the internal delay of the current node and the congestion information in front of the next hop node as the reward value, the neural network is trained, so that the scheduling mechanism can make full use of network resources to reduce the packet loss rate and delay of time-sensitive flows. The simulation results show that, in the large-scale time-sensitive network scenario, the scheduling mechanism of the joint routing and queue in this paper can reduce the weighted delay and packet loss rate while ensuring a certain scheduling success rate.

Acknowledgement. This work was supported by the Science and Technology Project of China Southern Power Grid (No.090000KK52210155).

References

1. Huang, T., Wang, S., Huang, Y., Zheng, Y., Liu, J., Liu, Y.: Survey on deterministic networks. J. Commun. **40**(6), 160–176 (2019)
2. Grossman, E.: Deterministic networking use cases. RFC Editor (2019)
3. Schweissguth, E., et al.: ILP-based joint routing and scheduling for time-triggered networks (2017)
4. Qiu, X., Huang, X., Li, W., Li, W., Guo, S.: Packet Scheduling mechanism for large-scale time-sensitive networks. J. Commun. **41**(11), 124–131 (2020)
5. Pahlevan, M., Obermaisser, R.: Genetic algorithm for scheduling time-triggered traffic in time-sensitive networks. In: 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), Turin, pp. 337–344 (2018)
6. Xu, Z., Tang, J., Meng, J., et al.: Experience-driven networking: A deep reinforcement learning based approach. In: IEEE INFOCOM 2018-IEEE Conference on Computer Communications. IEEE, pp. 1871–1879 (2018)
7. Prados-Garzon, J., Taleb, T., Bagaa, M.: LEARNET: reinforcement learning based flow scheduling for asynchronous deterministic networks. In: ICC 2020–2020 IEEE International Conference on Communications (ICC). IEEE, pp. 1–6 (2020)
8. Zhang, P.: Design and Implementation of Deterministic Network Data Forwarding Model Based on Deep Reinforcement Learning. Beijing University of Posts and Telecommunications (2020)
9. Wu, J.: For a Static Snapshot of Dynamic Network Characterization Method Research. Heilongjiang University (2022)
10. You, L., Xi, X., Hongjie, W., Zhang, N.: Multi-controller deployment method for SDN based on topology division. Comput. Appl. Res. **34**(11), 3388–3393 (2017)

Generation Method of Dynamic Alarm Baseline for Cloud Server Based on XGBoost and Tolerability

Dequan Gao[1](✉), Yaozhong Dong[1], Jiwei Li[1], Bao Feng[2], Linfeng Zhang[1], Meng Yang[1], Rui Feng[1], and Junfei Yao[2]

[1] State Grid Information and Telecommunication Brach, Beijing 100761, China
gaodeq@163.com

[2] NARI Group Corporation, Nanjing 211106, China

Abstract. In order to solve the problem that massive server alarm management of cloud data centers in electric power enterprises cannot adapt to the personalized operation of cloud business and lean equipment management, we propose a dynamic baseline generation method for cloud server alarms based on XGBoost and alarm tolerability. Firstly, based on the historical data of each server operation indicators, we apply XGBoost algorithm to predict the operation status value of a performance indicator in a certain period range in the future. Then, by comprehensively considering multi-dimensional factors such as the importance of operation time interval, the levels of business systems, the number of historical alarms, and the number of users as constraint parameters, we quantitatively calculate different alarm tolerability ranges and generate the initial curve of alarm baseline. Finally, we use the Savitzky-Golay filter method to smooth the threshold of initial alarm baseline curve and dynamically generate post-processed alarm baselines for different servers. Through case analysis of the cloud servers operation data, this method can effectively learn the historical operation data of different servers and obtain the alarm threshold under their tolerability constraints, dynamically adapt to generate hierarchical alarm baseline of massive servers, and improve the efficiency of large-scale cloud server monitoring alarms.

Keywords: Cloud Data Center · Cloud Server Alarm Management · Dynamic Baseline · Alarm Tolerability · XGBoost · Baseline Threshold Smoothing

1 Introduction

Cloud data center is the key information infrastructure during the digital transformation and development of Chinese power grid enterprises. Massive cloud server equipment carries various business application systems, data and platform software, such as production control and operation management information of enterprises, and their stable and reliable operation is critical. With the construction and development of new power systems and energy internet, the scale of cloud server equipment deployed is becoming larger and larger, and the new business application systems supporting cloud service

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 328–338, 2024.
https://doi.org/10.1007/978-981-99-7161-9_26

modes are becoming more and more complex. Meanwhile, with the massive adoption of micro-service architecture for business systems, their requirements for operation and maintenance capabilities are also increasing. Different business application systems usually have different user group behavior, operation cycle mode and adaptive diversified resource allocation management. Therefore, in order to ensure the reliable and stable operation of diversified power grid business systems at different levels, large-scale server resources (including virtual resources) at the infrastructure level urgently need to provide maintenance capabilities of personalized and lean operation.

In the operation and maintenance scenarios of information communication equipment (such as cloud server, SDH equipment), power equipment (such as generator, transformer), information system software (such as e-commerce platform, cloud platform, database), alarm management is an important research field of intelligent operation and maintenance technology. Advanced baseline early warning technologies are applied to achieve efficient alarm management. For example, for server monitoring scenarios, probability and probability distribution algorithms are applied to alarm management to generate baselines, thus to realize dynamic alarm management of servers and other devices [1]. In terms of the operation status monitoring and alarm identification for other important equipment, some researchers have adopted the multivariate state estimation method. For example, Liu et al. [2] used the multivariate state estimation method to realize the early warning of the fault for the wind turbine in the electric field. Li et al. and Sun et al. [3, 4] respectively applied the multivariate state estimation technology (MSET) to the non-independent variable early warning model of the wind turbine and the abnormal judgment of variables in the reactor coolant system of nuclear power plant. The above research mainly uses the fixed threshold mode to pre-judge the single characteristic parameter to evaluate the equipment operation status. However, a single feature parameter has the problem that it cannot reflect its complex state information as a whole. In the field of communication operation and maintenance, Chen and Gong [5] adopted neural network for alarm data in telecom network management, and proposed an expert system of alarm correlation analysis for alarm analysis of performance indicators. For the power equipment condition monitoring and alarm scenarios, Lu et al. [6] constructed an alarm threshold model of condition monitoring data for power transmission and transformation equipment to solve the problem of low sensitivity of power transmission and transformation information. The above methods have uncertainty for setting baseline threshold, and there is a problem that the threshold is too large or too small. Secondly, the time range and update frequency of historical operation data will affect threshold, which may cause false alarms or missed alarms. In addition, the generation process of alarm baseline has not fully explored key performance indicator (KPI) periodic pattern of server alarm and the related attributes and operation constraints, so it is difficult to achieve accurate personalized warning.

Nowadays, for the monitoring and operation of cloud servers, many electric power enterprises usually adopt the traditional server management mode in their actual operation and maintenance work. Operation and maintenance personnel manually check the recent historical KPI status curve of a server (for example, the previous week or month), and then configure the server threshold for one week. This mode cannot meet the personalized and lean maintenance requirements of massive servers, and does not take into account the constraints such as the differences in the service systems and their business importance level. Therefore, according to the intelligent development trend of cloud server maintenance, it is necessary to make full use of KPI data and machine learning methods to solve the problem of generating dynamic alarms baseline for large-scale server device management.

This paper focuses on the key methods for generating dynamic baselines for server alarms. In Sect. 2, we briefly summarize and analyze the front-line operation and maintenance requirements of generating dynamic baseline. In Sect. 3, we propose a generating method of server dynamic alarm baseline based on XGBoost [7] and tolerability. This method integrates the constraints of the important operation characteristics of business system during dynamic threshold calculation, and smooth the threshold of baseline curve with a filtering algorithm. In Sect. 4, we show the results corresponding to a real word data illustration. Finally, Sect. 5 shows the main conclusion and future works.

2 Alarm Baseline Management of Cloud Server

Cloud server operation and maintenance involves normalized patrol monitoring, equipment parameter configuration, policy management, performance tuning, etc. Alarm management mainly involves threshold configuration of key operating indicators of the server (such as disk IO, network throughput, CPU and memory usage, etc.). Different threshold levels will trigger different alarms. For different KPI, their threshold configurations are also different.

The threshold configuration of alarm baseline has two modes: fixed threshold and dynamic threshold, as shown in Fig. 1. The fixed threshold mode is more suitable for the situation where the continuous change range of server KPI status data is small and regular, but different thresholds need to be set for different servers according to their specific situation. The dynamic threshold mode is suitable for the situation where the status data of the key performance indicators of the server is relatively uncertain. The dynamic threshold can dynamically adapt to the actual operation of server equipment and improve the accuracy and effectiveness of tolerability value.

The dynamic baseline of server alarm [8] is composed of dynamic alarm thresholds of a series of operation indicators within a period, and is a kind of time series data. To realize the dynamic of personalized baseline, it is necessary to solve the dynamic calculation and configuration of alarm threshold under different servers and different operating indicators. During the process of alarm baseline calculation, on the one hand, it is necessary to fully exploit and utilize the periodic mode characteristics in the historical data of operation indicators. Its performance state curve often has the patterns of day, week and month, and the state curve fluctuates greatly in different periods. Therefore, the traditional alarm mode based on fixed threshold cannot reflect the dynamic characteristics. On the other hand, the alarm tolerability range of different servers should have personalized characteristics, because they carry different levels of business systems with different requirements for operation reliability.

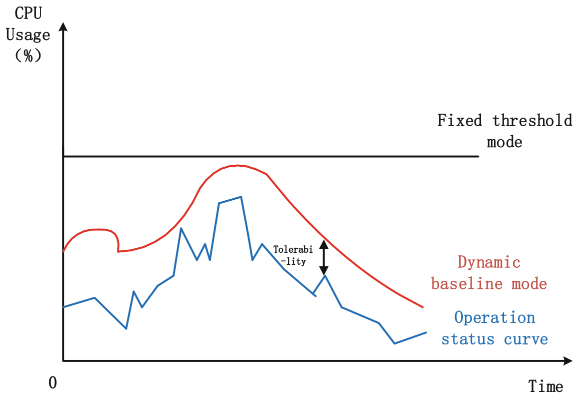


Fig. 1. Alarm baseline management mode

3 Intelligent Generation Method of Dynamic Alarm Baseline

3.1 Dynamic Baseline Calculation Process

Firstly, we collect the performance status data and historical alarm data from big data sources, such as business system and server operation log, and preprocess these original sample data. The processed KPI data samples are trained by the XGBoost algorithm in the form of key-value pairs to generate a state prediction model. Secondly, according to the historical data of different KPI, the future status data of the operation indicators in a certain time range are predicted. Then, according to the operation requirements of different business systems importance, the average number of users and the average number of alarms in different periods and other constraint parameters, the alarm tolerability is separately calculated to obtain the basic tolerability value for a period in the future. Finally, we use the filtering algorithm to process initial alarm baseline, and generate smoothed dynamic baseline. The generation process of alarm baseline is shown in Fig. 2.

3.2 KPI Status Prediction Based on XGBoost

Firstly, we select valid historical operation data, including operation KPI data, alarm data, and user data. Then, we preprocess the original sample data and detect abnormal sample data based on the found faults, holidays, major operation support events, and other situations. Finally, we clean and exclude abnormal data, and retain typical data that reflects the change modes of server operation status.

During the prediction generation, we input the processed sample data into the XGBoost-based KPI prediction model in the form of key-value pairs (<time point, performance data (CPU utilization), holiday identification (marked with 0, 1)>). We set the number of decision trees to k [9–12]. According to the output results of different f_k, we assume that the XGBoost-based performance state prediction model has k decision

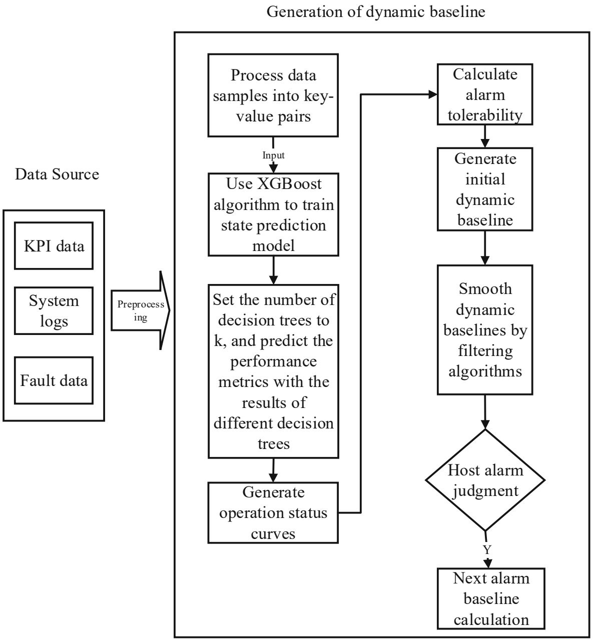

Generation of dynamic baseline
Data Source
KPI data
System logs
Fault data
Preprocessing
Process data samples into key-value pairs
Input
Use XGBoost algorithm to train state prediction model
Set the number of decision trees to k, and predict the performance metrics with the results of different decision trees
Generate operation status curves
Calculate alarm tolerability
Generate initial dynamic baseline
Smooth dynamic baselines by filtering algorithms
Host alarm judgment
Y
Next alarm baseline calculation

Fig. 2. Generation Process of dynamic baseline

tree, the formula for predicting server performance indicators is expressed as follows.

$$\hat{y}_i = \sum_{k=1}^{K} f_k(x_i), f_k \in \mathcal{F} \tag{1}$$

Its objective function is expressed as follows.

$$Obj^{(t)} = Loss\left(\hat{y}_i^{(t-1)}, y_i + f_t(x_i)\right) + \Omega(f_t) \tag{2}$$

$$\Omega(f_t) = \gamma M + \frac{1}{2}\lambda\|w\|^2 \tag{3}$$

where the *Loss* represents the loss function of the relationship between the real value and the predicted value, $\Omega(f_t)$ is a regular item, which is used to prevent over-fitting. M represents the number of leaves, w represents the weight of leaves, γ and λ are super parameters for tuning, and $\hat{y}_i^{(t)} = \hat{y}_i^{(t-1)} + f_t(x_i)$.

After training the KPI prediction model, according to the time limit requirements of the server alarm management, we input the time point of the future period into the model, and calculate the KPI status data within a certain time range in the future.

3.3 Alarm Tolerability Calculation

For cloud server operation and maintenance management, server alarm level will be determined and set according to the historical indicators status of equipment and the different tolerability ranges of alarm baseline. Therefore, the settings value of different indicator levels are often different. In this paper, we assume the alarm level is three-level mode, and the corresponding alarm coefficients are set as $L1$, $L2$, $L3$. The alarm coefficient indicates the range within which the threshold of different alarm levels can be floated upwards, usually determined by the experience and knowledge of operation experts.

Alarm tolerance refers to the tolerance level that exceeds the reasonable operating range of server KPI. For the requirements of server personalized operation and maintenance, alarm tolerability calculation mainly considers such factors as business service level, actual server operation performance and historical alarm conditions. Therefore, for the alarm tolerability T, the number of users and alarms (including the number of faults), business service level and other important factors of the corresponding business system in different periods are used as constraints to build a tolerability calculation model under multi-dimensional quantitative constraints. The formula is as follows:

$$\begin{aligned} T &= f(user, warning) \\ &= W_{user}\cos(R_{user}\pi/2) + W_{warning}\cos\left(R_{warning}\pi/2\right) \end{aligned} \tag{4}$$

W_{user} and $W_{\mathrm{wa}rning}$ respectively represent the weight of the number of users and the number of alarms on the alarm baseline, $W_{user} + W_{\mathrm{wa}rning} = 1$. Figure 3 shows the relationship between R_{user} and T.

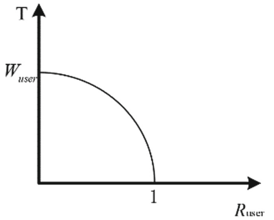


Fig. 3. The relationship between R_{user} and T

In this paper, cosine function (cos) is used to solve the problem that the tolerability shows a continuous downward trend with the increase of R_{user} and $R_{warning}$, which limits the output range and outputs in the form of curve.

$$R_{user} = \frac{n_{user}}{N_{user}} \tag{5}$$

$$R_{warning} = \frac{n_{warning}}{N_{warning}} \tag{6}$$

Here, n_{user} represents the average number of users in different operating hours, N_{user} represents the maximum number of users in each hour of 24-hourday, $n_{warning}$ represents the average number of alarms in different operating hours, and $N_{warning}$ represents the maximum number of alarms in each hour of 24-hour-day.

Furthermore, the calculation formula of initial alarm dynamic baseline is as follows,

$$Line_{alarm} = y_{pred} + LiT \tag{7}$$

Here, R_{user} and $R_{warning}$ are calculated based on hourly samples, and y_{pred} is predicted based on samples sampled every two minutes, so T takes the same value every hour.

3.4 Smooth Baseline Threshold

For the smoothing of initial alarm dynamic baseline, we use Savitzky-Golay filtering algorithm to process dynamic threshold, and calculate the weighted average value of the center point in the window about its surrounding points by polynomial least squares fitting of the threshold data in the moving window X_i^*.

$$X_i^* = \frac{\sum\limits_{j=-r}^{r} X_{i+j} W_j}{\sum\limits_{j=-r}^{r} W_j} \tag{8}$$

The X_i and X_i^* are the data before and after smoothing, W_j is the weight factor in the smoothing of the moving window, representing the importance of data in the moving window, and r is the number of input data pairs.

4 Experimental Analysis

We use the CPU operation status data of the real-world servers in actual cloud data center and the number of users, alarms and other information, including the running time, CPU usage, and average number of users and the average number of alarms in each period in the previous month. The CPU utilization dataset is the operation status data from 0:00 on October 20, 2020 to 0:00 on October 30, 2020, and the data collection frequency is once every two minutes. Each dataset are randomly divided into training set, verification set and test set according to the ratio of 8:1:1 for the model training, verification and test.

In the data experiment, we adopt Python programming language and scikit-larn algorithm library. The training and prediction of the model are performed on GeForce RTX 2080 Ti 11G graphics card.

Firstly, we use the XGBoost-based prediction model to calculate the server KPI performance state. We compare the prediction model based on XGBoost-based method with the multiple perceptron method [13] and the random forest algorithm [14]. Figure 4 shows the calculation results of the three algorithm models on the CPU utilization index. The CPU utilization broken line predicted by XGBoost-based algorithm is closest to the true performance value of the performance state, and the gap between the other two algorithms and the true value of the performance state is large.

Furthermore, Table 1 shows the comparison results of the three different methods in terms of prediction accuracy and loss value. As a result, the XGBoost-based prediction

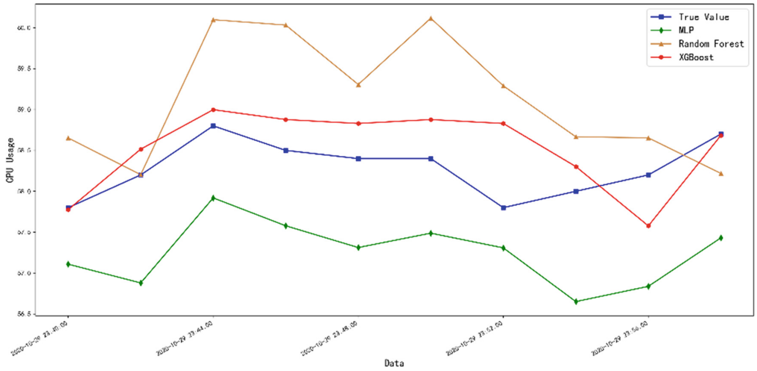


Fig. 4. Comparison of the prediction result between XGBoost model and the other two algorithms

Table 1. Comparison of the prediction effect of XGBoost model and the other two algorithms

Algorithm name	Accuracy (%)	Loss	Training time (s)
Multiple perceptron	71.41	0.033	10
Random forest	70.71	0.033	32
XGBoost	75.04	0.025	5

model is better than the multiple perceptron and random forest in terms of accuracy, loss value and calculation efficiency.

Secondly, in the calculation of alarm tolerability, we take the number of online users and the number of alarms as the key constraints. According to the practical experience of operation and maintenance, the server daily operation periods are divided into three intervals: 0–7, 7–19, 19–24, and the key interval of 7–19 is divided by hour.

Table 2 shows the average number of users in each interval and the average number of alarms in each interval in the previous month for case calculation (Table 3).

The W_{user} and W_{warning} are set to 0.3 and 0.7 respectively, and k is set to 5. When the CPU share is 20%, we set Li to 0.45. When the CPU share is 50%, we set Li to 0.35, and when the CPU share is 60%, we set Li to 0.25.

Table 2. Average number of users in each interval and average number of alarms in the previous month

Serial number	Operation interval	Average user number	Average number of alarms
1	0:00–7:00	0	0
2	7:00–8:00	35	2
3	8:00–9:00	190	6
4	9:00–10:00	557	29
5	10:00–11:00	670	36
6	11:00–12:00	512	12
7	12:00–13:00	421	7
8	13:00–14:00	480	4
9	14:00–15:00	780	11
10	15:00–16:00	865	39
11	16:00–17:00	823	15
12	17:00–18:00	468	5
13	18:00–19:00	79	2
14	19:00–24:00	0	0

Finally, we use Savitzky-Golay filtering algorithm [15] to smooth the threshold fluctuation in the initial alarm baseline, and obtain the effective alarm dynamic baseline in different intervals and under different conditions, as shown in Fig. 5.

The proposed method can dynamically calculate the tolerability value of each time interval to generate a dynamic alarm baseline. Indeed, it solves the problem that the time span of selected historical data and the update frequency of model data will affect the setting of the alarm threshold, which causes false alarms or missed alarms of early warning signals.

Table 3. Tolerability value in each interval

Serial number	Operation period	Tolerability (%)
1	0:00–7:00	7.61
2	7:00–8:00	4.28
3	8:00–9:00	5.01
4	9:00–10:00	3.76
5	10:00–11:00	2.61
6	11:00–12:00	6.79
7	12:00–13:00	3.97
8	13:00–14:00	2.76
9	14:00–15:00	2.46
10	15:00–16:00	3.96
11	16:00–17:00	3.67
12	17:00–18:00	4.32
13	18:00–19:00	5.24
14	19:00–24:00	7.31

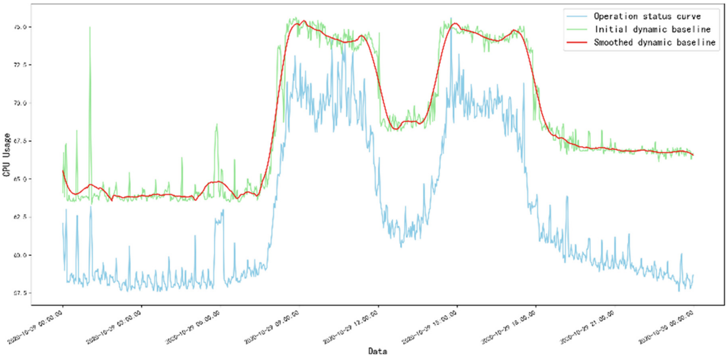


Fig. 5. Operation status curves and dynamic alarm baseline before and after smoothing

5 Conclusion

With the large-scale deployment of enterprise business systems to the cloud, cloud server operation and maintenance is one of the core services for cloud data center equipment life-cycle management. In order to meet the requirements of massive server personalized and lean management, our paper proposes a dynamic baseline generation method of server alarms based on XGBoost and tolerability. The method uses the performance prediction model based on XGBoost to predict the KPI value in the future period.

Then, through the multi-dimensional feature constraint of alarm tolerance, the baseline threshold under different alarm scenarios is dynamically calculated and adjusted. Finally, combined with the Savitzky-Golay filtering method, the server alarm baselines are dynamically generated. From the case results, our approach can generate three-level alarm prompts according to different business scenarios, realize hierarchical alarms of server status and improve the efficiency and accuracy of server alarm management. In the future, we will study the construction methods of multimodal operation knowledge graph for server fault handling.

Acknowledgment. This work was supported by Foundation of State Grid Information & Telecommunication Brach science and technology program "Research and application of key scenario technologies for intelligent operation of power information and communication (NO: 52993919000G)".

References

1. Gu, L., Duan, J., Duan, J., et al.: Research and implementation of dynamic baseline alarm management in host monitoring system. Shanxi Electric Power **3**, 40–44 (2017)
2. Liu, T., Liu, J., Lu, Y., et al.: Early fault warning of power plant fans based on MSET and the deviation degree. J. Chin. Soc. Power Eng. **36**(6), 454–460 (2016)
3. Li, D., Chang, Y., Zhao, J., et al.: Fault alarm of wind generator based on MSET method. North China Electric Power **12**, 43–48 (2016)
4. Sun, Y., Peng, M.: MSET&SPRT-based abnormal condition monitoring technology for nuclear power plants. Nuclear Power Eng. **3**, 57–61 (2015)
5. Chen, G., Gong, Q.: Application of neural networks and dynamic baseline algorithms in network management data processing and analysis. Shandong Commun. Technol. (2), 15–20+25 (2013)
6. Lu, M., Cheng, L., Jin, X.: Establishment of threshold warning model for condition monitoring data of power transmission and transformation equipment. Electron. Des. Eng. **28**(19), 5 (2020)
7. Yang, Y., Zhang, X., Yang, L.: Data-driven power system small-signal stability assessment and correction control model based on XGBoost. Energy Rep. **8**(S5), 710–717 (2022)
8. Fred, W., Richard, D., Alwyn, H.: Dynamic baselines for the detection of water quality impacts the case of shale gas development. Environ. Sci. Process. Impacts (2021)
9. Li, D., Yang, Q., Lu, X.: SDN network intrusion classification detection model based on decision tree. Comput. Eng. Des. **43**(8), 2146–2152 (2022)
10. Tang, L., Li, F.: Research on forecasting model of internet of vehicles security situation based on decision tree. Comput. Sci. **48**(S1), 514–517 (2021)
11. Wang, Y., Qian, Y., Liu, G.: Ordinal decision tree algorithm based on fuzzy advantage complementary mutual information. J. Comput. Appl. **41**(10), 2785–2792 (2021)
12. Du, Z., Li, Y., Zhang, D., et al.: Corn variable-rate seeding decision based on gradient boosting decision tree model. Comput. Electron. Agric. **198** (2022)
13. Xia, G., Tang, Q., Zhang, X.: Improved multi-layer perceptron applied to customer churn prediction. Comput. Eng. Appl. **56**(14), 257–263 (2020)
14. Wang, T., Liu, J., Zhu, S., et al.: Transient stability assessment and emergency control strategy based on random forest in power system. Power Syst. Technol. **44**(12), 4694–4701 (2020)
15. Yang, Y., Wu, L., Jian, M., et al.: Video stabilization algorithm based on savitzky-golay filtering and l1 norm optimization. J. Signal Process. **36**(11), 1829–1837 (2020)

Cloud-Edge Collaborative Computing Offloading Method for IoT Terminals

Shen Guo[1], Peng Wang[1], Jichuan Zhang[1], Jiaying Lin[1], Shuaitao Bai[1], Haoyang Sun[1], and Shi Wang[2](✉)

[1] Power Research Institute, Beijing 100192, China
[2] Beijing Vectinfo Technologies Co., Beijing 100082, China
928460190@qq.com

Abstract. With the booming IoT industry in recent years, smart devices are carrying more computationally intensive tasks. In the scenario of using drones for smart device inspection in the energy internet, it is often necessary to inspect towers, wires and their surrounding artificial and natural environments along transmission lines over long distances and take a lot of images and videos for inspection. However, the Unmanned Aerial Vehicle (UAV) has weak computing power and relies on a small capacity battery for operation, which cannot take on too many computing tasks; and the geographical location and task requirements of the UAV change from time to time, which easily leads to uneven load on the edge server nodes, increasing equipment energy consumption and reducing network performance. To solve the above problems, this paper investigates the cloud-edge collaborative task offloading mechanism based on deep reinforcement learning. This paper first constructs a three-layer system model of UAV-base station-cloud server for the intelligent inspection scenario and establishes a mathematical model with system power consumption as the optimization target and service processing delay and load balance among base stations as the constraints based on different demands in the actual scenario. Then, the deep reinforcement learning algorithm optimized by proximal policy optimization (PPO) is used for simulation to solve the offloading decision matrix in a given time and network environment, and the performance of the model is verified. The simulation results show that the algorithm in this paper can reduce the energy consumption of the system while ensuring the delay and load balance.

Keywords: Edge Computing · Computation Offloading · Deep Reinforcement Learning · Proximal Policy Optimization

1 Introduction

With the development of smart grid, the number of large-capacity and long-distance EHV/UHV transmission lines has increased significantly, and the load density of distribution system has also increased significantly. The safe operation of power lines is the key technology to ensure safe and reliable power supply. Due to the wide geospatial distribution of equipment, the traditional manual inspection is dangerous and hard work,

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 339–352, 2024.
https://doi.org/10.1007/978-981-99-7161-9_27

and UAV inspection gradually becomes an effective solution for the intelligent inspection of power equipment. Compared with traditional manual inspection, UAV inspection is less affected by external factors such as geographic environment and weather, and has the advantages of low cost, high automation, short cycle time, high mobility, high efficiency and convenient supervision [1].

Since the intelligent identification and detection of images is a computationally intensive task, and the power reserve, storage space and processing capacity of the UAV itself are insufficient to support such tasks, a cloud-based intelligent inspection system for transmission lines was born. The drone transmits image data to a remote cloud server for screening, which greatly enhances the degree of automation. However, this solution has the following two problems: first, the distance from the network belonging to the transmission tower perimeter to the cloud is generally long, and the transmission delay is large and the connection is not stable enough to meet the real-time needs of users [2]; second, the original data of the inspection task itself is an image, and the data volume is large, and the transmission to the cloud will consume a lot of network resources or even cause congestion.

For the above problems, Moving Edge Computing (MEC) can be a proven solution. Compared with mobile cloud computing, mobile edge computing model has great advantages. First, instead of communicating directly with the geographically distant cloud, the terminal device communicates directly with the edge server, which can effectively reduce the latency and broaden the application scenario of latency-sensitive applications [3]. At the same time, mobile edge computing itself also has some advantages of mobile cloud computing, for example, it can significantly reduce the average energy consumption of user devices and extend the usage cycle.

In recent years, increasing attention has been paid to the study of UAV task offloading. The literature [4] used the Q-Learning reinforcement learning algorithm for computational task offloading, which achieves an appropriate balance between equipment energy consumption and task processing latency. However, Q-Learning uses a value function to guide individual behavior, which requires training to obtain a reliable Q-Table value matrix with more demanding conditions and is only applicable to situations where the state space and action space are small or highly discrete and is not well suited for more complex UAV task offloading scenarios. The literature [5] uses convex optimization with reinforcement learning and Lyapunov optimization methods, which have good results for scenarios with tight or scarce computational resources. However, this study only focused on the energy consumption optimization of the device and ignored the latency factor, which tends to produce large fluctuations in the processing time of computational tasks and reduces the real-time and reliability of user experience. The literature [6] uses deep reinforcement learning algorithms to reduce the communication power consumption of drone clusters, and uses an optimized and improved deep reinforcement learning algorithm for energy consumption control based on the Actor-Critic algorithm, with the help of two independent neural networks to realize the algorithm, and improve the communication reliability of the UAV cluster while optimizing power consumption.

Considering the limitations of the existing work, this paper conducts a research on the design of computational offloading method for the application scenario of UAV intelligent inspection among cloud-edge cooperative IoT, to achieve the minimization of system energy consumption under the condition of guaranteeing the delay demand and the load balance of base stations. The main contributions of this research are as follows.

1. For the actual scenario of transmission line inspection tasks, a three-layer system model of UAV-base station-cloud server is constructed, and the energy consumption and delay conditions of each link of computing task generation, transmission and completion are modeled. Based on this, an optimization problem model with system power consumption as the optimization objective and service processing delay and load balancing among base stations as the constraints is established
2. The above optimization problem model is transformed into a Markovian decision process with defined states, actions and rewards, and a computational task offloading algorithm based on proximal policy optimization (PPO) is designed. Simulation results show that the algorithm in this paper can reduce the system energy consumption with guaranteed delay and load balancing.

The rest of this paper is organized as follows: Part II presents the system model and the optimization problem model. Based on the above model, a PPO-based task offloading algorithm is designed in the third part of this paper. The fourth part simulates the above algorithm and analyzes the simulation results. The last part summarizes the work of this paper.

2 System Model

2.1 Network Model

For the practical application scenario of UAV inspection of transmission line, this paper constructs a three-tier system model, consisting of UAV, base station and cloud server, as shown in Fig. 1. Their names and functions are as follows:

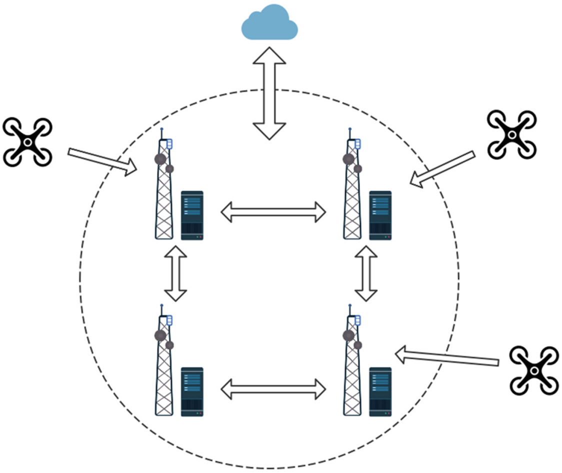


Fig. 1. Cloud-Edge Collaborative Computing Model

1. User Terminal Layer: Contain user devices, exemplified by unmanned aerial vehicles (UAVs) in this system. At initialization, UAVs will connect decide to connect to a base station according to its geographic location and network quality. During patrol inspection, UAVs will take images of production equipment and upload them for detection. The generation of detection tasks obeys Poisson distribution. In realistic scenarios, UAVs are likely to change their locations at any time, which results in the delay, transmission power and transmission rate between adjacent base stations being affected to a certain extent. For ease of calculation, our model simplifies the behavior of a UAV by randomly selecting its initial location and connecting itself to a base station, without subsequent movement.

   The UAV does not carry any computing tasks but unloads them to the base station unconditionally. This paper mainly considers the upstream data containing image and video information from the UAV to the base station but ignores the downstream data from the base station to the UAV, including control information, task meta-information and positioning information.
2. Base Station Layer: Contain base stations and supporting computing and network resources. Base stations are connected to each other, which incurs transmission costs when transmitting data. Base stations can receive computing tasks offloaded by user terminals and exchange tasks with other base stations. By collecting information about themself and calculating their current performance, base stations can learn to make offloading decisions and store historical experience data. With the accumulation of business data processed by base stations, the offloading decision will be optimized step by step.
3. Cloud Server Layer: Contain Sufficient computing resources. Each base station can offload tasks to the cloud server, enabling tasks to be processed at a faster speed, which consumes more transmission resources. It is worth noting that the end point of the task should be the base station instead of cloud servers. If the task is sent to a cloud server, the result of it should be returned to one of base stations.

The entire time span of the system is divided into a limited number of time slots. At the beginning of each time slot, obeying the Poisson distribution, the UAV generate a task that contains two parameters, the task size and the delay requirement, and offload the task to base stations. It is assumed that each generated task can be uploaded to the base station in the current time slot. After receiving all the tasks from UAVs, the base station selects the action to offload the task to itself, another base station or the cloud server. At the end of the current time slot, the base station calculates and processes the task queue, and then proceeds to the next time slot.

Due to the limited computing power of base stations, it is possible that the task queue is not computed after the end of the current time slot. There are two possible ways to handle tasks that have already been executed but have not yet been completed when processor resource is exhausted in the current slot: First, treat them as completed tasks and pop them out of the task queue directly; Second, keep the current state as a clipped task. The first scheme makes the processing easier and keeps the size of a single task within a certain range in the implementation so that the task size is not too large for a single base station. In the simulation, the second scheme is selected because it is more suitable for application scenario. When slot switching, the base station checks the remaining task queue and subtracts the remaining time of the task from the length of the slot in order. The remaining time going to zero means that the task exceeds the user's delay requirements and should be given a large penalty (Table 1).

Table 1. Parameters of the Model.

Notation	Description
α_k^t	Total number of tasks owned by base station K before offloading in time slot T, namely the sum of the remaining tasks at the end of the last time slot and the tasks offloaded by the UAV at the beginning of the current time slot
δ_{km}^t	The number of tasks offloaded from base station K to base station M. In particular, the amount of computation offloaded from the base station K to the cloud server is δ_{k0}^t, the amount of computation processed by itself is δ_{kk}^t
β_k^t	Total number of tasks owned by base station k after offloading in time slot T
μ_k	Computing power of base station K
W	Transmission bandwidth of a single base station
P_{r0}	Basic operating power of a single UAV
P_{b0}	Basic operating power of a single base station
P_{c-min}	No-load power of a single base station processor
P_{c-max}	Full-load power of a single base station processor
r_k^t	Average transmission rate of base station K in time slot t
h_0	Coefficient of the channel
σ^2	Noise power of the channel
P_{kc}^t	Computing power of base station K in time slot t
P_{km}^t	Transmission power of base station K in time slot t
r_{qos}	Minimum transmission rate of QoS

2.2 Energy Consumption Model

All energy consumption is divided into the following parts:

(1) The operating energy consumption of the UAV. This item includes the basic consumption to support the flight of mechanical equipment and the operation of electronic components. To simplify the calculation, the model assumes that the UAV will not move after the initialization of the position. The operating energy consumption fluctuates near a fixed value for a long time, which is regarded as the fixed value P_{r0} in the model.

(2) The operating energy consumption of the base station. This item includes the basic consumption of the reception and transmission of the signal and equipment other

than processor. Similarly, the power consumption of the base station fluctuates near a fixed value for a long time, which is regarded as P_{b0} in the model.

(3) The computational consumption of the processor. According to the correlation analysis [7], the computational energy consumption is roughly linearly related to the processor utilization. Based on the no-load power and full-load power of the CPU, we can obtain

$$P_{kc}^{t} = P_{c-min} + \frac{\beta_k^t}{\mu_k}(P_{c-max} - P_{c-min}) \tag{1}$$

(4) The energy consumption of transmission during task offloading. It includes the consumption of UAVs offloading tasks to base stations, base stations offloading tasks to other base stations, and base stations offloading tasks to the cloud. In this model, because the relative position between the UAV and base station and the transmission power of each equipment during data transmission remains unchanged, and the distance factor is not considered, according to Shannon's second law, we have

$$r_k^t = Wlog_2\left(1 + \frac{P_{km}^t h_0}{\sigma^2}\right) \tag{2}$$

where W is the channel bandwidth, h_0 is the channel gain between the UAV and the base station, and σ^2 is the noise power.

After deformation, we have

$$P_{km}^{t} = \left(2^{r_k^t/W} - 1\right)\sigma^2/h_0 \tag{3}$$

It is worth noting that in the actual scenario of UAV task offloading, data will not be transferred in every time slot. For example, the UAV does not take any images or videos when moving from one tower to another to perform tower inspection At this time, if the control data is ignored and the task data is considered, r_k^t should be zero. However, in the above system model, because the task generation of UAV follows Poisson distribution and is properly trimmed, the probability of r_k^t equaling to 0 is not large.

To sum up, for the energy consumption of base station K in time slot t E_k^t, we have

$$E_k^t = t\left(P_{r0} + P_{b0} + P_{kc}^t + P_{km}^t\right) \tag{4}$$

2.3 Time Delay Model

Delays in the process of task offloading and transmission can be roughly divided into the following parts:

(1) Propagation delay: We assume that the linear distance between two wireless devices (UAV to base station and base station to base station) is x and the speed of light is c. Then we can obtain the propagation delay as

$$D_{kx}^t = \frac{x}{c} \tag{5}$$

Since the distance between the devices in this study is relatively close, the propagation delay has orders of magnitude that is smaller than other items, so the propagation delay is ignored.

(2) Transmission delay: Assuming that the packet size is d, the transmission delay can be obtained as

$$D_{kd}^{t} = \frac{d}{W} \tag{6}$$

(3) The queuing delay from UAV to base station: As mentioned above, the tasks generated by drones obey the Poisson distribution, and each drone is only connected to one base station, so the task offloading process can be described using the M/M/1 queuing model. Suppose the QoS delay requirement of the user terminal is r_{qos}, then the queuing delay can be obtained by:

$$D_{km}^{t} = \frac{1}{r_{qos}}\left(1 + \frac{\overline{\alpha_k^t}/r_{qos}}{2\left(1-\overline{\alpha_k^t}/r_{qos}\right)}\right) \tag{7}$$

(4) Congestion delay from base station to base station and cloud: When the base station transfers tasks to other base stations and cloud servers, it is a point-to-point transmission, so certain congestion is unavoidable. Suppose the delay is when there is no congestion, and the congestion delay can be obtained by using the M/M/1 queuing model

$$D_{kg}^{t} = \frac{\tau}{1-\tau\Sigma_{i=1}^{N}\left(\alpha_i^t-\delta_{ii}^t-\delta_{i0}^t\right)} \tag{8}$$

(5) Queuing delay for task calculation at the base station: Each base station has a task sequence to be processed, and takes out tasks from the head in turn for calculation. The M/M/1 queuing model can be used to calculate the queuing delay

$$D_{kc}^{t} = \frac{1}{\mu_k - \beta_k^t} \tag{9}$$

(6) The queuing delay for offloading the task to the cloud server and then transferring the result back: As mentioned above, if the base station offloads the task to the cloud server for a second time, the result needs to be transmitted back to the base station, and this transmission process can also be described using the M/M/1 queuing model. Assuming that the backhaul speed is ρ times the transfer speed between base stations, the backhaul queuing delay can be obtained using the M/M/1 queuing model

$$D_{kb}^{t} = \frac{\tau/\rho}{1-\tau\Sigma_{i=1}^{N}\delta_{i0}^t/\rho} \tag{10}$$

2.4 Formulation of Problem

The objective of this paper is to find the task offloading scheme that minimizes the energy consumption of the UAV-base station-cloud server task processing system while ensuring the delay and load balancing constraints. That is, to find the

$$min \lim_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} \sum_{k=1}^{N} E_k\left(\alpha_k^t, \beta_k^t, \mathcal{M}\right) \tag{11}$$

$$M = M_0, M_1 \ldots M_{T-1} \tag{12}$$

Which make,

$$D_k^t\left(\alpha_k^t, \mathcal{P}_k^t\right) \leq D_{\max}\ \forall t \tag{13}$$

$$\lim_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} \overline{E_k^t} \leq E_{max} \tag{14}$$

$$\sqrt{\sum_{k=1}^{N} \overline{(\beta_k^t - \beta^t)}^2 / N} \leq \sigma_{\max}\ \forall t \tag{15}$$

When the minimum energy consumption is obtained, the target output, i.e., the decision sequence $\mathcal{M}$, is obtained simultaneously. The length of the decision sequence is T, and each element M is a one-dimensional array of length the number of base stations, where.

$$M_{tk} = \begin{cases} 0, & \text{represents base station } k \text{ to process tasks locally} \\ 1, & \text{represents base station } k \text{ offloads tasks to other base stations} \\ 2, & \text{represents base station } k \text{ offloads takss to the cloud} \end{cases} \tag{16}$$

The condition (3-13) restricts the time delay to be a QoS requirement. That is, at each time slot, the time spent by s task processing cannot exceed the time limit requested by the user.

Condition (3-14) restricts the average energy consumption of the system during long-term operation.

Condition (3-15) limits the standard deviation of the task volume of each base station at each time slot after offloading to meet the load balancing requirement.

3 Design and Implementation of Algorithm

Task offloading in edge networks usually involves a large number of terminal devices and edge servers. When traditional heuristic algorithms deal with task offloading decision-making problems, they often get local optimal solutions because they do not have the ability to learn. Therefore, this paper designs a computing task offloading algorithm based on PPO. The entire power inspection application scenario includes three parts: environment, individual and action. Individuals interact with the environment, starting from a state, choosing actions according to their own strategy distribution, and getting rewards. The environment is composed of physical equipment in the power scene that is inspected to provide individuals with environmental status information. Individuals can take different actions according to their state, calculate the corresponding rewards, and feed them back to the individual. Then, perform the uninstall operation.

The main body of the algorithm training is the base station MEC, which acquires tasks from the UAV and uses its own task queue to calculate the time slot state, then selects the offloading action based on the state, performs the offloading and obtains feedback. The base station adjusts the unloading strategy by the obtained feedback and goes to the next time slot to repeat the above actions.

The individual state space S is a matrix of size 1 × 2, which represents the amount of task and the delay requirements of the current time slot:

$$S_{t,i} = \left(D_{t,i}, T_{t,i}\right) \tag{17}$$

The size of the individual action space A is 3, which represents different unloading positions of the task, expressed as:

$$A_{t,i} = \left(x_{t,i}^{local}, x_{t,i}^{mec}, x_{t,i}^{cloud}\right) \in \{[1,0,0],[0,1,0],[0,0,1]\} \tag{18}$$

The offloading of vector $A_{t,i}$ is the offloading decision made by the base station i in the time slot t. When the value is [1, 0, 0], it means that the task is processed locally, and when the value is [0, 1, 0], it means Unload to other base stations, [0, 0, 1] represents uninstall to cloud server.

As mentioned above, this research is based on PPO near-end strategy optimization for algorithm design. The objective function of PPO is:

$$maxE\left[\frac{\pi(s_t,a_t)}{\pi_{old}(s_t,a_t)}\hat{A}_{\pi_{old}}(s_t,a_t)\right] \tag{19}$$

where π_{old} is the probability that the policy function before the update takes action a_t in the state s_t; and π is the probability that the policy function takes action a_t in the state s_t after the update; $\hat{A}_{\pi_{old}}(s_t,a_t)$ is estimation of the advantage function. In order to ensure that the new strategy is not too different from the old strategy, the value of $\frac{\pi(s_t,a_t)}{\pi_{old}(s_t,a_t)}$ should be constrained to be around 1 [8]. Here, the floating range is set to $[1-\in, 1+\in]$, so the objective function can be rewritten as:

$$E\left[min\left(\frac{\pi(s_t,a_t)}{\pi_{old}(s_t,a_t)}\hat{A}_{\pi_{old}}(s_t,a_t), clip\left(\frac{\pi(s_t,a_t)}{\pi_{old}(s_t,a_t)}, 1-\in, 1+\in\right)\right)\right] \tag{20}$$

The computation of the offloading algorithm can be expressed as follows:

```
Input: the parameters of UAV, base station and cloud server, the distribution of UAV tasks over time
Output: offloading strategy
Steps:
Initialize the drone, base station and cloud server
Random initialization strategy $\pi$ and $\pi_{old}$
for each episode in 1, N do
    for each epsilon in 1, M do
        Update the status of drones, base stations and cloud servers
        Choose action according to status
        Execute the action and calculate the reward value, update the critic network
        Go to the next state
        Temporarily store the previous status, actions and rewards
        if reach the update step size do
            Update the actor network with all temporary states, actions and rewards
            Update strategy function
        end if
    end for
end for
Return to the offloading strategy
```

In each execution cycle, the individual performs multiple iterations and updates the state and the resulting actions. Every few iterations will use the accumulated data to trigger a strategy update. Assuming that the total number of cycles is m and the number of iterations in each cycle is n, it is easy to get that the time complexity of this algorithm is $O(mn)$.

4 Simulations

The execution environment of this simulation program is Python 3.6.0 and TensorFlow 1.14.0. In this paper, we assume that the inspection scenario is a 50km × 50km square area with 20 UAVs and 16 base stations working simultaneously, and the UAVs generate tasks according to the Poisson process with arrival rates ranging from 0 to 10 tasks per second. The data size of a unit task is 0.2 Mb. The data size of a task is a multiple of the unit task. Thus, for a typical 100 Mb Ethernet LAN, the expected transmission time delay per unit task is $\tau = 200$ ms. The channel bandwidth is 20 M. The average value of the channel gain h_0 distribution is $\mathrm{g0}(1/100)^4$, where $\mathrm{g0} = -30\,\mathrm{dB}$ is the path loss constant of 1m. Assume that the noise power is $\sigma^2 = 10^{-10}$ W/Hz.

The first is the average energy consumption of the base station, which is the optimization target of the problem. We can consider the optimization effective when the average energy consumption can gradually decrease with the increase of training iterations and converge to a smaller value; the second is the average delay of the task processing, which is a hard constraint and leads to a high penalty for task timeout during the simulation. Under the same task generation distribution, it is assumed that the decrease in power consumption will lead to the increase in delay, and vice versa, the decrease in delay will cause the increase in power consumption, then it can be presumed that the optimization for power consumption under ideal conditions will lead to the average delay gradually approaching the upper bound of the set delay [9]; the third is the standard deviation of the task load of each base station, which is similar to the delay indicator and is a hard constraint, but in the simulation The third is the standard deviation of the task load of each base station, which is similar to the delay index and is a hard constraint, but in the simulation process, only a more relaxed limit is given considering the actual offloading effect.

The following will compare the execution results of the PPO algorithm with the randomized algorithm.

Firstly, we analyze the average energy consumption of the base station. As shown in Fig. 2, the horizontal axis of the coordinate system represents the number of iteration rounds and the vertical axis represents the average energy consumption of the base station. It can be seen that, as the main performance index of the algorithm, this algorithm can make significant optimization of energy consumption. At the beginning, the average energy consumption of the improved algorithm is significantly higher than that of the randomized algorithm; at the 200th iterations, the improved average energy consumption starts to be lower than that of the randomized-based algorithm; and the average energy consumption converges around the 250th iteration. In this sample, the improved algorithm saves about 9% of the average energy expenditure relative to the random unloading algorithm.

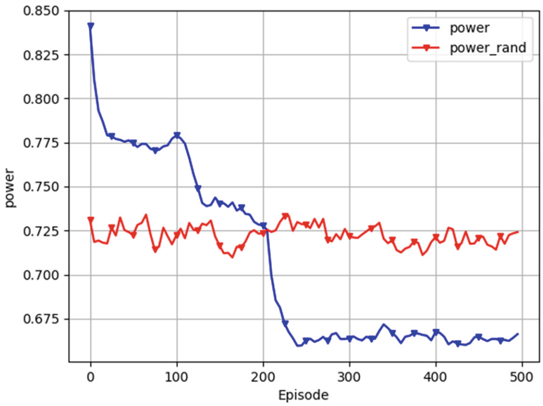


Fig. 2. The Average Energy Consumption of Base Stations

Analyze the average time delay of user tasks. As shown in Fig. 3, the algorithm sacrifices some of the time delay to improve the energy consumption at the beginning of the iteration because of the strong constraint imposed on the task demand time delay in the improved algorithm. As the average time delay gradually increases and encounters a penalty, it stabilizes at a level slightly below the time delay constraint. Even so, in this sample the improved algorithm achieves a time delay savings of about 55% relative to the random offloading algorithm.

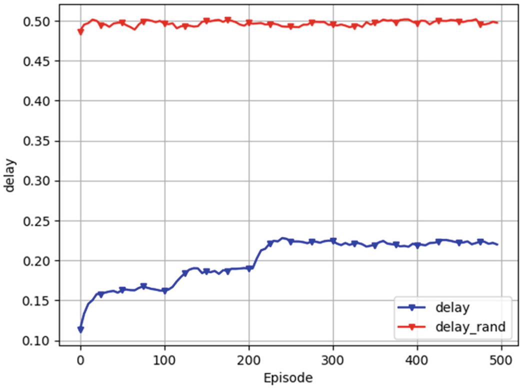


Fig. 3. Average Task Processing Latency

Figure 4 compares the load balancing of the two algorithms. In this study, the load balancing is quantified using the standard deviation of the amount of tasks carried by each base station after offloading for each time slot. As the number of iterations increases, the load balancing metric tends to level off, but does not reveal a large difference from the load balancing of the random algorithm. The conjecture is that the given time delay constraint is tighter and the constraint for load balancing is weaker, so it becomes the cost of optimizing the average energy consumption.

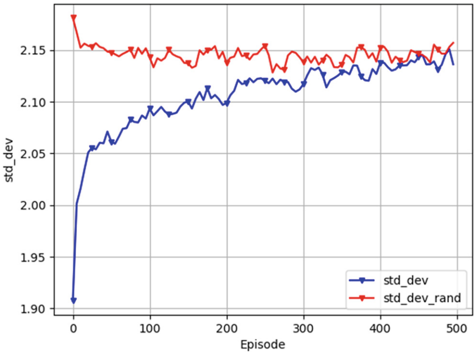


Fig. 4. Standard Deviation of Base Station Load

5 Conclusion

In order to make full use of UAVs for transmission line inspection, the system energy consumption is reduced and the inspection efficiency is improved under the condition of guaranteeing the time delay demand and the load balance of base stations. In this paper, we study the cloud-side collaborative task offloading mechanism based on deep reinforcement learning. Firstly, a three-layer system model of UAV-base station-cloud server is constructed for the intelligent inspection scenario, and an optimization problem model with system power consumption as the optimization target and service processing time delay and load balancing among base stations as the constraints is established based on the different requirements in the actual scenario. Then, a deep reinforcement learning algorithm for near-end policy optimization is simulated to solve the offloading decision matrix for a given time and network environment with the processing time of the task and the standard deviation of the load between each base station as constraints. The simulation analysis shows that the near-segment policy optimization algorithm used in this paper can reduce the system energy consumption by about 9% compared to the random offloading algorithm with a given time delay constraint and base station load balancing requirement guaranteed.

Acknowledgement. This work is supported by the Research on Digitization and Intelligent Application of Low-Voltage Power Distribution Equipment (Contract NO: SGSDDK00PDJS2000375).

References

1. Du, Y., Yang, K., Wang, K., Zhang, G., Zhao, Y., Chen, D.: Joint resources and workflow scheduling in UAV-enabled wirelessly-powered MEC for IoT systems. IEEE Trans. Veh. Technol. **68**(10), 10187–10200 (2019)
2. Zhao, W., Xu, M., Cheng, X., Zhao, Z.: An Insulator in transmission lines recognition and fault detection model based on improved faster RCNN. IEEE Trans. Instrum. Meas. **70**, 1–8 (2021)
3. Nie, Y., Zhao, J., Gao, F., Yu, F.R.: Semi-distributed resource management in UAV-aided MEC systems: a multi-agent federated reinforcement learning approach. IEEE Trans. Veh. Technol. https://doi.org/10.1109/TVT.2021.3118446
4. Liu, X., Yu, J., Wang, J., Gao, Y.: Resource allocation with edge computing in IoT networks via machine learning. IEEE Internet Things J. **7**(4), 3415–3426 (2020)
5. Pan, S., Chen, Y.: Energy-optimal scheduling of mobile cloud computing based on a modified Lyapunov optimization method. IEEE Trans. Green Commun. Netw. **3**(1), 227–235 (2019)
6. Liu, C.H., Chen, Z., Tang, J., Xu, J., Piao, C.: Energy-efficient UAV control for effective and fair communication coverage: a deep reinforcement learning approach. IEEE J. Sel. Areas Commun. **36**(9), 2059–2070 (2018)
7. Fan, X., Weber, W.D., Barroso, L.A.: Power provisioning for a warehouse-sized computer. ACM SIGARCH Comput. Architect. News **35**(2), 13–23 (2007)
8. Guan, Y., Ren, Y., Li, S.E., Sun, Q., Luo, L., Li, K.: Centralized cooperation for connected and automated vehicles at intersections by proximal policy optimization. IEEE Trans. Veh. Technol. **69**(11), 12597–12608 (2020)
9. Liu, C., Bennis, M., Debbah, M., Poor, H.V.: Dynamic task offloading and resource allocation for ultra-reliable low-latency edge computing. IEEE Trans. Commun. **67**(6), 4132–4150 (2019)
10. Zhan, W., et al.: Deep-reinforcement-learning-based offloading scheduling for vehicular edge computing. IEEE Internet Things J. **7**(6), 5449–5465 (2020)

11. Xu, S., et al.: RJCC: reinforcement-learning-based joint communicational-and-computational resource allocation mechanism for smart city IoT. IEEE Internet Things J. **7**(9), 8059–8076 (2020)
12. Guo, K., Quek, T.Q.S.: On the asynchrony of computation offloading in multi-user MEC systems. IEEE Trans. Commun. **68**(12), 7746–7761 (2020)
13. Li, Q., Wang, S., Zhou, A., Ma, X., Yang, F., Liu, A.X.: QoS driven task offloading with statistical guarantee in mobile edge computing. IEEE Trans Mobile Comput. https://doi.org/10.1109/TMC.2020.3004225

Index

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 353–354, 2024.
https://doi.org/10.1007/978-981-99-7161-9