Smart Innovation, Systems and Technologies 307

Lakhmi C. Jain
Roumen Kountchev
Kun Zhang
Roumiana Kountcheva *Editors*

Advances in Wireless Communications and Applications

Wireless Technology: Intelligent Network Technologies, Smart Services and Applications, Proceedings of 5th ICWCA 2021

KES International

Springer

Smart Innovation, Systems and Technologies

Volume 307

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.

More information about this series at https://link.springer.com/bookseries/8767

Lakhmi C. Jain · Roumen Kountchev ·
Kun Zhang · Roumiana Kountcheva
Editors

Advances in Wireless Communications and Applications

Wireless Technology: Intelligent Network Technologies, Smart Services and Applications, Proceedings of 5th ICWCA 2021

Springer

Editors
Lakhmi C. Jain
KES International
Shoreham-by-Sea, UK

Roumen Kountchev
Technical University of Sofia
Sofia, Bulgaria

Kun Zhang
Hainan Tropical Ocean University
Sanya, Hainan, China

Roumiana Kountcheva
TK Engineering
Sofia, Bulgaria

ISSN 2190-3018 ISSN 2190-3026 (electronic)
Smart Innovation, Systems and Technologies
ISBN 978-981-19-3485-8 ISBN 978-981-19-3486-5 (eBook)
https://doi.org/10.1007/978-981-19-3486-5

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

Preface

This book is the second volume with high-quality peer-reviewed research papers presented at the Fifth International Conference on Wireless Communications and Applications (ICWCA 2021) which was carried out in Hainan, China, during December 17–19. The volume is focused on the presentation of the newest trends and achievements in the development of intelligent evaluation methods and implementations, aimed at: Optimization of the communication network topology, optimization control for sensing terminal of power IoT platform, data fusion for abnormal network traffic, edge computing facilities in 5G power network, and also ship intelligent navigation, security of web applications, intelligent security monitoring system design, coastal water transportation and communication network based on 5G technology, network attack detection, and many others.

The aim of the book is to present the latest achievements of the authors to a wide range of readers: IT specialists, engineers, physicians, PhD students, and other specialists in the area.

Acknowledgments: The book editors express their special thanks to book chapter reviewers for their efforts and good will to help for the successful preparation of the book. Special thanks for the Honorary Chair of ICWCA'21 International conference, Prof. Lakhmi Jain, General Chairs Prof. Dr. Chong Shen, Prof. Dr. Roumen Kountchev, and Prof. Dr. Kun Zhang, and Program Chair Prof. Dr. Srikanta Patnaik.

The editors express their warmest thanks to the excellent Springer team which made this book possible.

March 2022

Lakhmi C. Jain
Roumen Kountchev
Kun Zhang
Roumiana Kountcheva

Organization

Steering Committee

General Chairs

Chong Shen	Hainan University, China
Roumen Kountchev	Technical University of Sofia, Bulgaria
Kun Zhang	Hainan Tropical Ocean University, China

Members

Xianpeng Wang	Hainan University, China
Chuan Tian	Institute of Deep Sea Science and Engineering Chinese Academy of Sciences, China
Qinyu Zhang	Harbin Institute of Technology, China
Feifei Gao	Tsinghua University, China
Qian Wang	Wuhan University, China
Peng Fei	Huazhong University Science and Technology, China
Liqiang Zheng	Shenzhen Runan Technology Development Corporation, China
Weigang Chen	Tianjin University, China

Program Committee

Program Chairs

Srikanta Patnaik	Department of Computer Science and Engineering, SOA University, Bhubaneswar, Odisha, India
S. R. Roumiana Kountcheva (Vice President)	TK Engineering, Sofia, Bulgaria

International Program Committee

Desai, U. B.	Indian Institute of Technology Hyderabad, India
Dianati, Mehrdad	University of Surrey, UK
Dumka, Ankur	University of Petroleum and Energy Studies, India
Fernando, Xavier	Ryerson University, Canada
García Villalba, Luis Javier	Universidad Complutense de Madrid (UCM), Spain
Giridhar, K.	Indian Institute of Technology, Madras, India
Gumaste, Ashwin	Indian Institute of Technology, Bombay, India
Hsu, Ching-Hsien	National Chung Cheng University, Taiwan
Jain, Raj	Washington University in St. Louis, USA
Jhunjhunwala, Ashok	Indian Institute of Technology-Madras, India
Kar, Subrat	Indian Institute of Technology Delhi, India
Karandikar, Abhay	Indian Institute of Technology Bombay, India
Kim, Jongsung	Kyungnam University, South Korea
Krithivasan, Kamala	Indian Institute of Technology Madras, India

Technical Program Committee

Hui Gao	Beijing University of Posts and Telecommunications, China
Agrawal, Dharma P.	University of Cincinnati, USA
Atiquzzaman, Mohammed	University of Oklahoma, USA
Balakrishnan, N.	Indian Institute of Science, India
Bellur, Umesh	Indian Institute of Technology Bombay, India
Bhargava, Bharat K.	Purdue University, USA
Biswas, Amitava	Cisco Systems Inc., USA
Biswas, Subir	Michigan State University, USA
Boutaba, Raouf	University of Waterloo, Canada
Chao, Han-Chieh	National Dong Hwa University, Taiwan
Chen, Hsiao-Hwa	National Cheng Kung University, Taiwan
Chen, Jiming	Zhejiang University, China
Chilamkurti, Naveen	La Trobe University, Australia
Chockalingam, A.	Indian Institute of Science, India
Desai, U. B.	Indian Institute of Technology Hyderabad, India
Dianati, Mehrdad	University of Surrey, UK
Dumka, Ankur	University of Petroleum and Energy Studies, India
Fernando, Xavier	Ryerson University, Canada
García Villalba, Luis Javier	Universidad Complutense de Madrid (UCM), Spain
Giridhar, K.	Indian Institute of Technology, Madras, India
Gumaste, Ashwin	Indian Institute of Technology, Bombay, India

Hsu, Ching-Hsien	National Chung Cheng University, Taiwan
Jain, Raj	Washington University in St. Louis, USA
Jhunjhunwala, Ashok	Indian Institute of Technology-Madras, India
Kar, Subrat	Indian Institute of Technology Delhi, India
Karandikar, Abhay	Indian Institute of Technology Bombay, India
Kim, Jongsung	Kyungnam University, South Korea
Krithivasan, Kamala	Indian Institute of Technology Madras, India
Leung, Victor C. M.	The University of British Columbia, Canada
Lilien, Leszek T.	Western Michigan University, USA
Linderman, Mark H.	AFRL Information Directorate/RISE, USA
Lloret Mauri, Jaime	Polytechnic University of Valencia, Spain
Madria, Sanjay	Missouri University of Science and Technology, USA
Mahanti, Aniket	University of Auckland, New Zealand
Manjunath, D.	Indian Institute of Technology Bombay, India
Meghanathan, Natarajan	Jackson State University, USA
Mouftah, Hussein	University of Ottawa, Canada
Naït-Abdesselam, Farid	University of Paris Descartes, France
Nayak, Amiya	University of Ottawa, Canada
Obaidat, Mohammad S.	Nazarbayev University, Kazakhstan
Park, Jong Hyuk	Seoul National University of Science and Technology (SeoulTech), South Korea
Patnaik, Lalit M.	National Institute of Advanced Studies, India
Patnaik, Srikanta	SOA University and Interscience Institute of Management and Technology, Bhubaneswar, India
Rashvand, Habib F.	University of Warwick, UK
Rodrigues, Joel	University of Beira Interior, Portugal
Sadeghi, M.-R. Rafsanjani	Amirkabir University of Technology, Iran
Samanta, Debasis	Indian Institute of Technology, India
Sekaran, K. Chandra	National Institute of Technology Karnataka, India
Sharma, Vinod	Indian Institute of Science, Bangalore, India
Shu Lei	Guangdong University of Petrochemical Technology, China
Sinha, Bhabani P.	Indian Statistical Institute, India
Stojmenovic, Ivan	University of Ottawa, Canada
Tran-Gia, Phuoc	University of Wuerzburg, Germany
Traore, Issa	University of Victoria, Canada
Vaidya, Binod	University of Ottawa, Canada
Vasilakos, Athanasios	Lulea University of Technology, Sweden
Venkata Krishna, P.	SPM University, India
Verma, Dinesh	IBM TJ Watson Research Center, USA
Wang, Shiuh-Jeng	Central Police University, Taiwan
Wang, Weichao	University of North Carolina at Charlotte, USA
Wolfinger, Bernd E.	University of Hamburg, Germany

Xin Qin	University of the Faroe Islands, Faroe Islands
Zeadally, Sherali	University of Kentucky, USA
Zhang Yan	University of Oslo and Simula Research Laboratory, Norway
Biju Theruvil Sayed	Dhofar University, Sultanate of Oman
Nassim Asbai	University of Science and Technology Houari Boumediene (U.S.T.H.B), Algiers, Algerian
Steven Sheng-Uei Guan	Xi’an Jiaotong-Liverpool, China
Jan Kubíček	Technical University of Ostrava, Ostrava
Zhenguo Gao	Huaqiao University, China
Loc Nguyen	Loc Nguyen’s Academic Network, Vietnam
Fateh Mebarek-Oudina	University of 20 août 1955-Skikda, Algeria
Zahéra Mekkioui	University of Tlemcen, Algeria
Jun Tao	Jianghan University, China
Wei Wei	Xi’an University of Technology, China
Haining Yang	University of Electronic Science and Technology of China, China
Xiang Wu	China Academy of Information and Communications Technology, China
Hai Tao Wang	Nanjing Audit University, China
Xue Yong Ding	Sanya University Institute of Technology, China
Luoyun-xu	Huadian Electric Power Research Institute, China
Zhu Yao Hua	Aston University, UK
Isidoros Perikos	University of Patras, Greece
Grzegorz Sierpiński	Silesian University of Technology Faculty of Transport, Polish

Contents

About the Editors

Lakhmi C. Jain, Ph.D., Dr H.C., M.E., B.E.(Hons), Fellow (Engineers Australia), is with the Liverpool Hope University and the University of Arad. He was formerly with the University of Technology Sydney, the University of Canberra, and Bournemouth University.

Professor Jain founded the KES International for providing a professional community the opportunities for publications, knowledge exchange, cooperation, and teaming. Involving around 5,000 researchers drawn from universities and companies worldwide, KES facilitates international cooperation and generates synergy in teaching and research. KES regularly provides networking opportunities for professional community through one of the largest conferences of its kind in the area of KES.

His interests focus on the artificial intelligence paradigms and their applications in complex systems, security, e-education, and e-healthcare.

Roumen Kountchev is a professor at the Faculty of Telecommunications, Department of Radio Communications and Video Technologies at the Technical University of Sofia, Bulgaria. His scientific areas of interest are: digital signal and image processing, image compression, multimedia watermarking, video communications, pattern recognition, and neural networks. He has 400 papers published in magazines and conference proceedings; 20 books; 48 book chapters; and 20 patents. He had been the principle investigator of 52 research projects. At present, he is a member of Euro Mediterranean Academy of Arts and Sciences and the President of the Bulgarian Association for Pattern Recognition (member of IAPR). He is Editor-in-Chief of Intern. Journal of Image Processing and Vision Science. He is the editorial board member of Intern. Journal of Reasoning-based Intelligent Systems; Intern. Journal Broad Research in Artificial Intelligence and Neuroscience; KES Focus Group on Intelligent Decision Technologies; Egyptian Computer Science Journal; Intern. Journal of Bio-Medical Informatics and e-Health, and Intern. Journal Intelligent Decision Technologies; Intern. Journal of Bio-Medical Informatics and e-Health. He is Member of the Institute of Data Science and Artificial Intelligence and Intern. Engineering and Technology

Institute. He has been a plenary speaker at more than 30 international scientific conferences and symposia.

Kun Zhang, Ph.D., is Master's Supervisor. He is Professor at Hainan Tropical Ocean University. He is Visiting Professor of the State Key Laboratory of Marine Resources Utilization in the South China Sea, Hainan University, and Guest Master's Supervisor at Tianjin Science and Technology University. He is Visiting Scholar at the Harbin Institute of Technology; he has high-level talents in Hainan Province, "Top Talents," and "Nanhai Masters" youth project talents in Hainan Province; he is a candidate in the third level of Hainan Province "515" Engineering and a senior member of Chinese Computer Society (CCF) and China Electronics Association (CIE); he is the member of ACM and IEEE, Hainan Province Science and Technology Expert, Guangdong Province Science and Technology Expert, Sanya City Information Construction Expert, and Sanya City Contracted Theoretical Expert; he is the host of Key Laboratory of visual computer in Sanya. More than 160 papers have been published so far, including 20 SCI indexes published in IEEE Journal of Selected Topics in Signal Processing (JSTSP), Digital Signal Processing, IEEE Access, Cluster Computing, International Journal of Distributed Sensor Networks, etc.

Roumiana Kountcheva got her M.Sc. and Ph.D. at the Technical University of Sofia, Bulgaria, in 1992. Presently, she is Vice President of TK Engineering, Sofia. She had postgraduate trainings in Fujitsu and Fanuc, Japan. Her main scientific interests are in image processing, image compression, digital watermarking, pattern recognition, image tensor representation, neural networks, CNC, and programmable controllers. She has more than 180 publications, among which: 34 journal papers, 21 book chapters, and 5 patents. She was the PI and Co-PI of 48 scientific research projects. She was the plenary speaker at 16 international scientific conferences and scientific events. She edited several books published in the Springer SIST series and is a member of international organizations: Bulgarian Association for Pattern Recognition, International Research Institute for Economics and Management (IRIEM), the Institute of Data Science and Artificial Intelligence (IDSAI), and is Honorary Member of the Editorial Board of the non-profit peer-reviewed open access IJBST Journal Group.

Equipment Terminals Optimization Control Method for Sensing Terminal of Power IoT Platform

Boxiang Shang[1](✉) and Xiaoyan Guo[2]

[1] State Grid Tianjin Electric Power Company, 39 Wujing Road, Hebei District, Tianjin, China
sbxsl123@163.com

[2] Information and Communication Company, State Grid Tianjin Electric Power Company, 153 Kunwei Road, Hebei District, Tianjin, China

Abstract. Nowadays, with the massive terminal access, which leads to data congestion and energy imbalance problems in power grids, regions have implemented equipment terminals shedding or power restriction measures due to technical and national strategic reasons, congestion or energy shortage, which bring certain negative impacts on regional economic development despite the simple rotation strategy to ensure resource equity. In this paper, we propose a equipment terminals optimization control method for the sensing terminal of the smart IOT platform, which uses adaptive scheduling methods and operational constraints to achieve minimal power loss in order to overcome overall data congestion, power-energy shortage and resource waste. Through the experimental simulation, the method can effectively optimize the scheduling of the imperial platform sensation equipment, reduce power energy loss, and ensure business service needs. It guarantees source-end data integration and business online in real time to improve safe grid operation, enterprise lean management and customer quality service.

Keywords: Smart grid · Load optimization · IoT platform

1 Introduction

With the advancement of digital reform, most of the traditional power grids today are being transformed and upgraded into smart grids, which are the belonging and business integration of power grids and two-way communication network systems [1–3]. Demand-side management (DSM) is an important to realize electric energy management in smart grid [4]. The DSM is to encourage electric devices to reduce electricity consumption during peak periods to make the regional electric equipment terminals curve appear flat [5]. The existing access to the IoT platform sensing terminal devices have low device data integration efficiency, high power consumption, and high cost due to deployment requirements, which brings great inconvenience to the regional energy deployment [6]. Therefore, there is an urgent need to propose a power equipment terminal scheduling method to make the regional grid terminal equipment terminals shift

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 1–9, 2022.
https://doi.org/10.1007/978-981-19-3486-5_1

with time so that the devices can better match the power demand and supply without expanding the power loss [7, 8].

In this paper, we proposed an optimization model for equipment terminals scheduling of sensing terminals in the smart IoT platform, which can optimize equipment terminals scheduling according to different tips. The model could be adapted to other preferences in the power equipment or smart grid. At the same time, it takes into account the balanced situation of both incentives, distributed renewable energy systems (DRES), and fully coordinates the combination of development (cost, peak equipment terminals, and customer usability) to solve the equipment terminals problem in perspectives [9]. Therefore, this model can extend to be applied to smart grid in other geographic areas and communities. In this paper, the model is applied to the smart IOT platform sensing terminal to realize the grid equipment terminals scheduling in intelligent management [10].

2 Related Work

This paper focuses on the power consumption and equipment terminals scheduling problems on the demand side of the IoT platform. Renewable energy losses in smart grids are achieved with the help of optimization methods.

The literature [11] introduces the IoT architecture and clarifies the positioning and important role of the IoT platform, analyzes each functional component of the IoT platform, and points out the direction of the convergence development of the IoT platform software. The literature [12] proposes a hybrid optimized load balancing algorithm for the load balancing scheduling problem, which makes full use of the advantages of both artificial bee colony and ant colony optimization algorithms and applies the percolation technique to load balancing. The migration efficiency and performance are improved. The literature [13] addresses the optimization problem of satellite terminal load topology and establishes a topology model. Then, the load balancing network topology optimization method is proposed based on the navigation constellation model, which improves the load balancing performance. The literature [14] addresses the characteristics of electric vehicle power consumption rate affected by the load size, and constructs a band vehicle path optimization model to optimize on the vehicle sensing load and drive unit, yielding significant advantages. In the literature [15], facing the load problem of transformers in distribution networks, a spatio-temporal balancing optimization method is proposed to effectively reduce the network loss and improve the node voltage quality of distribution clusters by flexibly adjusting the node voltage of distributed power optimization distribution clusters.

This paper proposes an equipment terminal scheduling optimization model that combines the terminal types addressed by the IoT platform with an optimized scheduling approach to optimize equipment terminals scheduling. The model uses adaptive scheduling methods and operational constraints to minimize power losses, combines power consumption records of different sensing terminals for fast analysis and decision making, optimizes device control allocation and integration with the cloud-based terminal architecture of the IoT platform, and achieves intelligent management of network equipment terminals scheduling.

3 Perception Terminal Multi-service Equipment Terminals Optimization Method

3.1 Multi-service Scheduling Optimization Architecture

According to the access types of sensing terminals in the IOT platform, this paper designs a smart grid middleware containing an equipment terminal scheduling module to realize equipment terminals scheduling. Where each sensing terminal k (k1…, K) define a set of devices and was applied in energy. There exists a huge number of access terminals including smart meters and other devices in each region, which are connected through a centralized scheduler (CS).

The model algorithm by the CS to issue instructions, terminal bill costs and peak equipment terminals are generated and communicated to the grid master control business middle office. The CS optimizes the equipment terminals meters of each terminal based on the business demand analysis taking into account development, feeds back the equipment terminals schedule to customer's smart meter. Figure 1 represents the equipment terminals optimization control method.

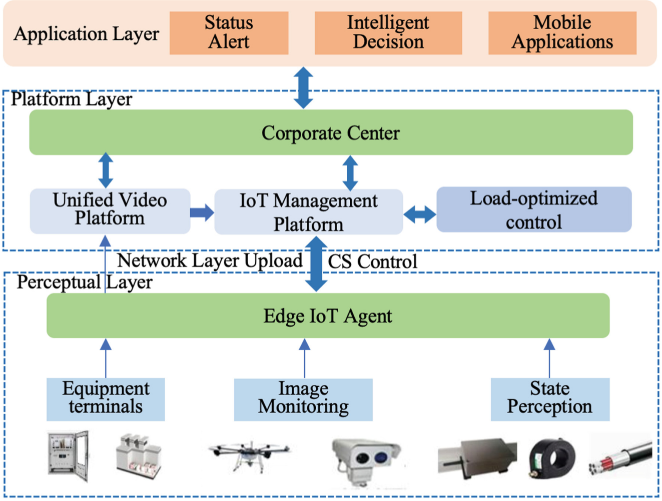


Fig. 1. Sense terminal equipment terminals scheduling optimization architecture

3.2 End-Equipment Terminals Presets

First a set of K sensing terminals in the region is defined in categories, each with a flexible set of equipment terminals/devices M_k in time range T, the start time of the equipment terminals/devices is determined. Each sensing terminal is flexibly supplied, where $i = 1,\ldots,M_k$, has a duration. In the process of accessing the sensing layer of the IOT platform, each sensing terminal establishes a statistical assessment of power consumption, and the power output of each device at each time period t can be calculated. Therefore, each transferable equipment terminals $S_{i,\ k}$ as the time point in time range $[r_{i,k} - X_{i,k}, r_{i,k} + X_{i,k}]$; Deploy the terminal in time $[L_{i,k}, U_{i,k}]$, the start time of each equipment terminals as Eq. 1 and Eq. 2:

$$\tilde{L}_{i,k} = \max(r_{i,k} - X_{i,k})\ \forall i, k \tag{1}$$

$$\tilde{U}_{i,k} = \min(T - d_{i,k} + r_{i,k} + X_{i,k})\ \forall i, k \tag{2}$$

3.3 Multi-service Equipment Terminals Optimization Methods

As shown in Fig. 2, the overall process of equipment terminals optimization for the perception layer devices of the IoT platform, the optimization criteria are obtained through the processing of data combined with business requirements. By obtaining the multi-constraint weights, and then realizing the adjustment of power loss and online time of equipment terminals devices, the business adjustment of sensing terminal devices is realized (as shown in Fig. 2).

Where, k represents the terminal data of the terminal device of the IoT platform, s represents the energy standard calculation rule, d represents the device priority weighting in the adjustment feedback process, e represents the energy loss of the device, and t represents the feedback scheme of the final device access.

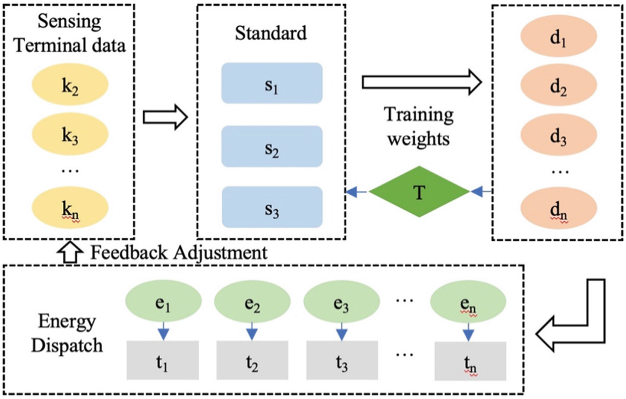


Fig. 2. Flow chart of equipment terminals optimization algorithm

Adaptive Equipment Terminals Constraint. How to decrease equipment terminals peak is the important of DSM, thereby improving the sustainability of the grid. The peak equipment terminals can be expressed as Eq. 3.

$$PL = \max_{t \in [1, T]} \left(N(t) + \sum_{k=1}^{K} \sum_{i=1}^{M_k} e_{i,k}(t) \right) \tag{3}$$

This is used as a criterion for scheduling in order to develop an equipment terminal plan that minimizes peak equipment terminals as Eq. 4.

$$\min_{u} s1 = PL \tag{4}$$

For energy cost calculation is solved based on electrical energy losses, the energy cost $SC(t)$ of the planned equipment terminals in any time period t. $c(t)$ represents the calculated function of the total duration t in the evaluation time, can be carried out as Eq. 5:

$$SC(t) = SG(t) \cdot c(t), \forall t \tag{5}$$

The cost of energy demanded by the sensing terminal at each time period is represented by $NC(t)$ and can be expressed by Eq. 6.

$$NC(t) = \begin{cases} (SC(t) - PVG(t)) \cdot c(t),\ SC(t) - PVG(t) > 0 \\ 0,\ SC(t) - PVG(t) \geq 0 \end{cases}, \forall t \tag{6}$$

The dispatch time is calculated as Eq. 7.

$$TNC = \sum_{t=1}^{T} NC(t) \tag{7}$$

The minimization of perceived end-use energy losses can be expressed as Eq. 8.

$$\min_{u} s2 = TNC \tag{8}$$

The deviation of the equipment terminals plan from the terminal power adjustment can be defined based on the business demand for sensing terminal uptime and power consumption. It is mainly measured from the perspective of time or power. The smaller the deviation of the equipment terminals from the preferred start-up time, the more effectively the sensing terminal can meet the grid operation and maintenance business requirements. The higher the demand can be to achieve the adjustment of regional power loss.

Therefore, the power required by the sensing terminal k can be calculated as Eq. 9.

$$SL_k^{uc}(t) = N_k(t) + \sum\nolimits_{i=1}^{M_k} e_{i,k}(t),\ \forall t, k \tag{9}$$

The squared deviation of the preferred plan can be measured as Eq. 10.

$$D_k = \sum\nolimits_{t=1}^{T} (Q_k(t) - SL_k^{uc}(t))^2, \forall k \tag{10}$$

where $Q_k(t)$ is the total power of the equipment terminals rescheduled by the sensing terminal, based on which the objective optimization function is established as the objective function of the equipment terminals scheduling model to realize the control of energy loss as Eq. 11 and Eq. 12.

$$D = \sum\nolimits_{k=1}^{K} D_k \tag{11}$$

$$\min_{u} s3 = D \tag{12}$$

Equipment Terminals Optimization Model. In addition, most existing models have incentives, such as TOU tariffs, that do not allow effective integration of DRES and most existing models set an objective function. Therefore, this paper considers the application limitations of existing models and develops different combinations of dispatch criteria. Based on this, an equipment terminal scheduling model is proposed.

The scheduling model is developed for the type of perceptual layer terminal access.

$$\min s = w_1 s1 + w_2 s2 + w_3 s3 \tag{13}$$

For the purpose of device terminal scheduling, we optimize the model with constraints on the peak value of the device terminal (s_1), the power loss (s_2), and the terminal service (s_3). The device terminal scheduling is optimized according to the needs of different business scenarios, and the scheduling scheme is obtained by weighting. The optimization scheme of the scheduling model in time T is shown in Eq. 14.

$$\sum_{t=1}^{T} e_{i,k}(t) = d_{i,k} \cdot p_{i,k}, \ \ \forall i, k \tag{14}$$

The formula indicates that the equipment terminals i of the sensing terminal k can be scheduled to be identified in a continuous time period starting from $t = v$ up to $v + d_{ik} - 1$ as Eq. 15. And the load-optimized scheduling algorithm is designed in Table 1.

$$\sum_{t=v}^{v+d_{i,k}-1} e_{i,k}(t) = d_{i,k}, p_{i,k}, \ \ \forall i, k; v \in [\tilde{L}_{i,k}, \tilde{U}_{i,k}] \tag{15}$$

4 Experimental Simulation

4.1 Model Business Performance Evaluation

To judge the effectiveness assessment of the model in terms of business requirements, the experimental part is oriented to the evaluation of the working effect of six types of sensing terminals under an urban transmission scenario business. The uninterrupted and normal operation and maintenance of the original business is achieved with less power cost loss.

Table 1. Load-optimized scheduling algorithm.

Algorithm 1 Load-optimized scheduling

```
Input: terminal data K, development S, service weights D
Output: Power consumption E, terminal deployment T
Calculate the minimized peak equipment terminals min(s1)
Minimum cost of end-use energy loss min(s2)
Calculate the terminal service constraint s3
Generate the total power consumption E
    while E not in T:
        if K is in 1, 2 or 3 then:
            Calculate the weighted W (w1, w2, w3)
            Calculate the total power consumption E
            End-equipment terminals execution K
    end if
end while
return Power consumption E, terminal deployment K
```

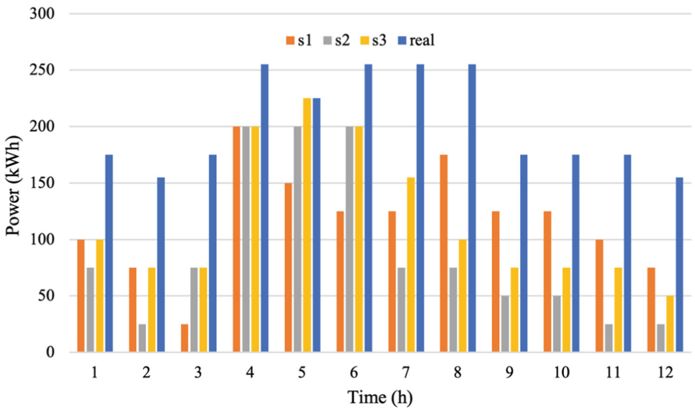


Fig. 3. Time-series diagram of model business performance evaluation

As shown in Fig. 3, the results of power loss monitoring of four smart IoT platform terminal equipment terminals in the test area over a 12-h period, it can be concluded from the figure that the actual power loss is up to 20% excess loss with time series analysis compared to the three individual intermodulation models. Therefore, the implementation of the model can produce greater efficiency in business maintenance and energy resource saving.

4.2 Business Scenario Validation

To demonstrate the wide applicability of the proposed equipment terminals scheduling model, this paper collects real equipment terminals data of power-using equipment according to several business scenarios in an urban area and conducts a case study. The experiment includes a case study of two scenarios: substation equipment, and office area terminal equipment. The figure shows the power consumption analysis of the equipment terminals scheduling of the scenario under the condition that the business requirements of the scenario are satisfied (see Fig. 4).

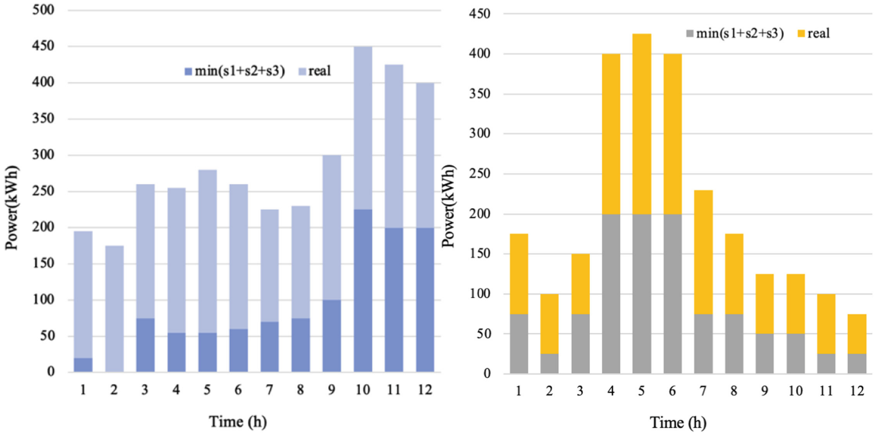


Fig. 4. Model business scenario power consumption timing diagram

5 Conclusion

In this paper, an equipment terminals optimization control method is proposed in combination with the perception layer access terminal of the smart IOT platform, which combines the consumption of different device terminal records for fast analysis and decision making, effectively minimizing power loss and meeting the business requirements of actual scenarios. Through experimental verification, the model can reduce the power energy loss of existing sensing terminals by 20%, while having portability for different scenarios, and can achieve effective mitigation of overall power data congestion and energy loss. While maintaining the normal operation and maintenance of the power system, it achieves the effective promotion of the digital transformation of the power grid.

References

1. Araujo, V., et al.: Performance evaluation of FIWARE: A cloud-based IoT platform for smart cities. J. Parallel Distrib. Comput. 132, 250–261 (2019)

2. Foukalas, F.: Cognitive IoT platform for fog computing industrial applications. Comput. Electr. Eng. **87**, 113–115 (2020)
3. Shang, L., et al.: Allocation of computing resources at the grid edge based on software-defined networks. Power Syst. Prot. Control **49**(20), 136–143 (2021)
4. Barabadi, B., Yaghmaee, M.H.: A new pricing mechanism for optimal load scheduling in smart grid. IEEE Syst. J. **13**, 1737–1746 (2019)
5. Huang, Y.Q., et al.: Power IoT data transmission scheme: current status and outlook based on 5G technology. J. Electr. Eng. Technol. **36**(17), 3581–3593 (2021)
6. Wu, K., He, et al.: Research on secure communication protocols for power IoT. Inf. Netw. Secur. **21**(09), 8–15 (2021)
7. Dai, X.Z., et al.: Operational model and method of distributed energy trading based on decentralized decision making by Internet of Things. Renew. Energy **39**(08), 1130–1136 (2021)
8. Liu, J.G., Tan, Y.H., Deng, Y.: An end-side cloud collaboration model for power information physical systems. J. Power Syst. Autom., 101–102 (2020)
9. Wang, X.L., Li, X., Qin, X.L.: Distributed state-aware source-network load-storage cooperative scheduling under the power Internet of Things. Comput. Sci. **48**(02), 23–32 (2021)
10. Sun, Y.Y., et al.: Power IoT cloud master station computing load model and optimal resource allocation. Power Autom. Equip. **41**(04), 177–183 (2021)
11. Wang, H., Chen, Y.: IOT platform software to build an intelligent interconnection hub for enterprises. Chemical Progress **35**(S2), 51–55 (2016)
12. Hou, X.Y., Cheng, F., Liu, D.C.: A load balancing algorithm based on a hybrid percolating artificial bee colony and ant colony optimization. Comput. Appl. Res. **38**(02), 440–443 (2021)
13. Jia, W.S., Wang, Q., Li, L.M., Yue, J.: Research on load balancing based navigation time-division network chain building optimization technology. Spacecraft Eng. **28**(05), 39–45 (2019)
14. Huang, J.H., Liu, F.X.: Electric vehicle charging strategy and path optimization problem under dynamic load. Comput. Integr. Manuf. Syst., 1–23 (2021)
15. Huang, K., Zhai, G.X., Han, J.L., Zhao, Z.H., Tang, X.L., Sun, P.F.: Research on load balancing optimization method for distribution network transformer clusters. J. Power Syst. Autom. **33**(07), 113–119 (2021)

Comprehensive Evaluation of Intelligent Obstacle Avoidance Function by Changing Lanes of Vehicle Based on an Improved Evaluation Index System

Qi Zhan[1], Wei Zhou[1], Wenliang Li[1], Xuewen Zhang[1,2(✉)], and Xiao Qin[1]

[1] Research Institute of Highway Ministry of Transport, Beijing 100088, China
345562132@qq.com
[2] Southeast University, Nanjing 210000, China

Abstract. In order to make a comprehensive evaluation of the vehicle intelligent obstacle avoidance function by changing lanes, the evaluation index system was improved from the aspects of whether the function is available and how well the function performs. Then, the combination weights of each index were determined by improved G1 method (improved order relation analysis method) and CRITIC method (Criteria Importance Though Intercrieria Correlation method), followed by comprehensive quantitative evaluation by fuzzy comprehensive evaluation method. Finally, the method was applied to the comprehensive evaluation of the vehicle intelligent obstacle avoidance function by changing lanes of three intelligent commercial vehicles. The total scores of the three test vehicles were 92.7, 97.1 and 49.0, and the evaluation grades were excellent, excellent and fail, respectively. The results obtained by this method corresponded to the performance of the vehicles in the test. The results show that the improved evaluation index system is more comprehensive and can determine whether the vehicle has the intelligent obstacle avoidance function and evaluate its performance.

Keywords: Unmanned vehicles · Avoiding obstacles · Changing lanes · Improved evaluation index system · Improved G1 · CRITIC · Fuzzy comprehensive evaluation

1 Introduction

After unmanned vehicles have been developed and verified, a more complete system is formed and its functions are perfected, then it needs to be tested and evaluated in order to obtain the performance of the vehicle, so as to help developers find the shortcomings or defects of the functions and improve them in a targeted manner [1]. The intelligent obstacle avoidance function, as one of the core functions of safe driving of unmanned vehicles, plays a crucial role in ensuring the safety of occupants, reducing traffic accidents and improving traffic efficiency. According to the avoidance action, the non-stop obstacle avoidance is divided into two scenarios, lane change obstacle avoidance and

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 10–21, 2022.
https://doi.org/10.1007/978-981-19-3486-5_2

lane borrowing obstacle avoidance. Lane change refers to the vehicle changing lane to avoid obstacles, and lane borrowing refers to the vehicle borrowing part of the adjacent lane, fine-tuning the driving direction to avoid obstacles. This paper firstly focuses on the intelligent obstacle avoidance by changing lanes.

The premise of comprehensive evaluation is the selection of evaluation indexes, which should follow the principles of systematicity, feasibility, and science. In terms of overall vehicle intelligence evaluation, Sun [2] constructed an evaluation index system from safety, intelligence, and smoothness to make a comprehensive quantitative evaluation of the intelligent behavior of unmanned vehicles. Li [3] analyzed the test content of Future Challenges, and constructed an evaluation index system from safety, systemic, smoothness and speed to make a comprehensive intelligent quantitative evaluation of the autonomous vehicles. In terms of single capability or behavior evaluation, Fang [4] combined the test items of Future Challenges to evaluate the vehicle turnaround behavior. Zhang [5] constructed an evaluation index system of intelligent vehicle target detection capability in terms of both target classification and recognition capability. Most of the current studies on the evaluation indexes of unmanned vehicle intelligence focus on the overall performance of the vehicle [6], and there are few studies on the evaluation of a single function, and there are problems of incomplete evaluation. The evaluation of a single function should be evaluated in terms of whether the function is available and how well it performs.

The evaluation index system of intelligent obstacle avoidance by changing lanes has been constructed in the previous period, but it is more applicable to the evaluation of vehicles with intelligent obstacle avoidance function, which has the problem of incomplete evaluation. In order to comprehensively evaluate the intelligent obstacle avoidance function by changing lanes of vehicles, the evaluation index system is modified from two perspectives of whether the vehicles have this function and the performance of this function. Based on the improved evaluation index system, the combination weights are obtained by improved G1 method [7] and CRITIC method [8], and the evaluation model is established to make a comprehensive evaluation of the vehicle intelligent obstacle avoidance function by changing lances, which provides a basis for the further development of its function.

2 Comprehensive Evaluation

2.1 Improved Evaluation Index System

The test conditions of the vehicle intelligent function of obstacle avoidance by changing lanes in the closed field are divided into straight road test condition and curved road test condition.

Straight Road Test Condition. The test road is at least a one-way two-lane long straight road. The test vehicle travels at a certain speed along the road that meets the requirements of the test road. When the vehicle recognizes the obstacle in front of this lane and determines that the adjacent lane meets the lane change condition, it performs lane change to avoid the obstacle. The schematic diagram of this test condition is shown in Fig. 1.

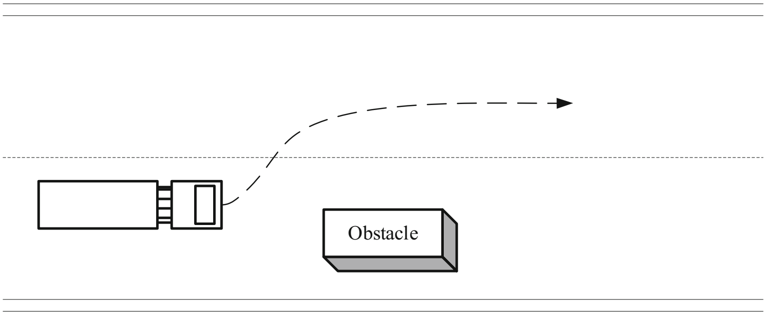


Fig. 1. Diagram of intelligent obstacle avoidance by changing lanes test conditions in the straight path.

Curve Road Test Condition. The test road is at least a one-way two-car curve with a radius of curvature of 500 m. The test vehicle travels at a certain speed along the road that meets the requirements of the test road. When the vehicle recognizes the obstacle in front of this lane and determines that the adjacent lane meets the lane change condition, it performs lane change to avoid the obstacle. This test condition is divided into the same direction as the curve lane change obstacle avoidance and reverse lane change obstacle avoidance with the curve. Take the left curve as an example, the same direction is pointing to the left lane change to avoid obstacles, as shown in Fig. 2(a), and the reverse direction is pointing to the right lane change to avoid obstacles, as shown in Fig. 2(b).

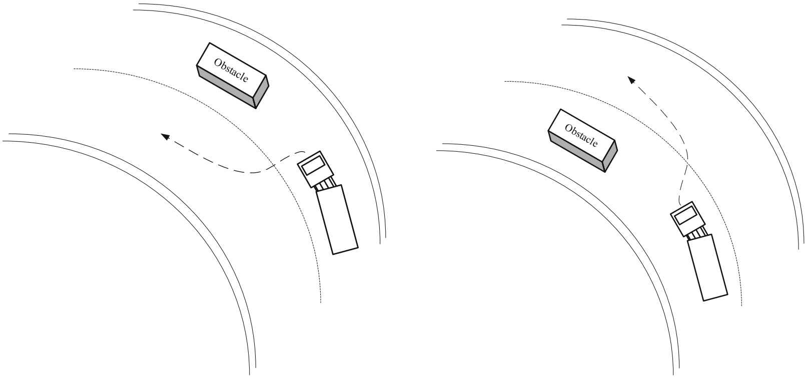


Fig. 2. Diagram of intelligent obstacle avoidance by changing lanes test conditions on curves. (a) Left curve, change lanes to the left to avoid obstacles (b) Left curve, change lanes to the right to avoid obstacles

The process of obstacle avoidance by changing lanes refers to the process from when the turn signal is turned on to when the vehicle completes the lane change to avoid the obstacle and the turn signal is off. The preparation stage refers to the stage from when the turn signal is turned on to when the outside of the front wheels touches the inner edge of the lane line. The execution stage refers to the stage from when the outside of the front wheels touches the inner edge of the lane line to when the rear wheels of the vehicle completely cross the lane line. The completion means that the vehicle enters the target lane, completes the lane change action to safely avoid obstacles, and drives steadily in the current lane.

Based on the above test conditions, specific parameters were selected from different stages, including smoothness, maximum lateral acceleration, average lateral acceleration, preparation time, and full time. Maximum lateral acceleration and average lateral acceleration evaluate smoothness and lateral control. The full time evaluates the efficiency and longitudinal control. The smoothness of avoidance by changing lanes means that there is no obvious interval delay in the process, and the lane change action is continuous.

The weights of the indicators under the three test conditions were obtained by questionnaire and actual measurement data of two intelligent commercial vehicles as shown in Table 1. The indicators in descending order of importance are maximum lateral acceleration, full time, preparation time, average lateral acceleration, and smoothness, in which the weight of smoothness is the smallest and is less than 0.15 in all three working conditions. Therefore, two indicators are added to evaluate the process and completion status of obstacle avoidance, namely, whether collision occurs with obstacles and whether the line is pressed after lane change. If it happens, the corresponding indicator will be recorded as 0 points, otherwise the corresponding indicator will be recorded as full points.

Table 1. The weights of the original evaluation index system.

	Weights of straight road	Weights of changing lanes in the same direction as the curve	Weights of changing lanes in the reverse direction as the curve
Smoothness	0.148	0.143	0.148
Maximum lateral acceleration	0.246	0.269	0.269
Average lateral acceleration	0.182	0.185	0.186
Preparation time	0.198	0.197	0.189
Full time	0.226	0.204	0.208

The improved evaluation index system of vehicle intelligent function of obstacle avoidance by changing lanes is shown in Table 2. The evaluation index system includes two primary indexes, which are straight road test condition and curve road test condition. The curve road test condition is divided into changing lanes in the same and reverse direction as the curve. Under each level index, there are 5 secondary indexes including whether collision with obstacles occurs, whether the line is pressed after lane change, maximum lateral acceleration, average lateral acceleration, preparation time, and full time.

Table 2. Evaluation index system of vehicle intelligent function of obstacle avoidance by changing lanes.

Target level	Element level A		Indicator level B
Vehicle intelligent function of obstacle avoidance by changing lanes	Straight road test condition (A1)		Whether collision with obstacles occurs (B11)
			Whether the line is pressed after lane change (B12)
			Maximum lateral acceleration (B13)
			Average lateral acceleration (B14)
			Preparation time (B15)
			Full time (B16)
	Curve road test condition (A2)	Changing lanes in the same direction as the curve (A21)	Whether collision with obstacles occurs (B211)
			Whether the line is pressed after lane change (B212)
			Maximum lateral acceleration (B213)
			Average lateral acceleration (B214)
			Preparation time (B215)
			Full time (B216)
		Changing lanes in the reverse direction as the curve (A22)	Whether collision with obstacles occurs (B221)
			Whether the line is pressed after lane change (B222)
			Maximum lateral acceleration (B223)

(*continued*)

Table 2. (*continued*)

Target level	Element level A		Indicator level B
			Average lateral acceleration (B224)
			Preparation time (B225)
			Full time (B226)

2.2 Fuzzy Comprehensive Evaluation Method Based on Combination Assignment

Improved G1. Improved G1 method specifically consists of the following steps.

Determining the Sequential Relationship Between Indicators. Experts are invited to score the importance of each indicator, and the scoring criteria are referred to Table 3. According to the importance scores given by the experts, the indicator sets at each level are reordered. If the score of indicator X_i is higher than that of indicator X_j, then it means that indicator X_i is more important than indicator X_j, and it is recorded as $X_i > X_j$, and the sequential relationship is obtained accordingly.

Table 3. Expert scoring criteria.

Importance	Score
Particularly important	9–10
Relatively important	6–8
Generally important	4–5
Unimportant	1–3

Ratio of Importance of Adjacent Indicators. Taking the scoring of an expert as an example, the ratio of the importance scores of adjacent indicators is used as the ratio of the weights of two indicators, as shown in Eq. (1).

$$r_k = \frac{x_{k-1}}{x_k} = \frac{w_{s(k-1)}}{w_{sk}} (k = m, m-1, \cdots, 2) \tag{1}$$

where, m is the number of indicators at the corresponding level, x_k is the score of the importance of indicator X_k by an expert, r_k is the ratio of the weights of adjacent indicators, and w_{sk} is the subjective weight of indicator X_k based on the score of an expert.

Calculating Subjective Weights. The formula for calculating the subjective weight w_{sk} based on this expert scoring is shown in Eq. (2).

$$w_{sk} = \left(1 + \sum_{k=2}^{m} \prod_{k=2}^{m} r_k\right)^{-1} \tag{2}$$

The subjective weights of the other indicators can be obtained according to the recurrence relationship, as shown in Eq. (3).

$$w_{\mathrm{s}(k-1)} = r_k w_{sk} (k = m, m-1, \cdots, 2) \tag{3}$$

Finally, the subjective weights of each index based on that expert are obtained, and then the scoring weights of all experts are averaged to obtain the final weights $w_{sk} = \{w_{s1}, w_{s2}, w_{s3}, \cdots, w_{sm}\}$.

CRITIC. CRITIC method specifically consists of the following steps.

Dimensionless Treatment. Equation (4) is used for positive indicators with higher indicator values, and Eq. (5) is used for negative indicators with lower indicator values.

$$x_{ik} = \frac{X_{ik} - \min(X_k)}{\max(X_k) - \min(X_k)} \tag{4}$$

$$x_{ik} = \frac{\max(X_k) - X_{ik}}{\max(X_k) - \min(X_k)} \tag{5}$$

where, X_{ik} is the *i*-th original measured data of index X_k, x_{ik} is the dimensionless processed data.

Calculating the Standard Deviation of Each Indicators

$$\sigma_k = \sqrt{\frac{1}{n-1} \sum_{i=1}^{n} (x_{ik} - \overline{x}_k)^2} \tag{6}$$

where, $\overline{x}_k$ is the mean of the measured data of index $X_{k,}$ n is the number of measured data of index X_k, and σ_k is the standard deviation of measured data of index X_k.

Constructing the Correlation Coefficient Matrix. The linear correlation coefficient r_{kj} between indicator X_k and indicator X_j is calculated as shown in Eq. (7).

$$r_{kj} = \frac{\sum\limits_{k=1}^{m} (x_k - \overline{x}_k)(x_j - \overline{x}_j)}{\sqrt{\sum\limits_{k=1}^{m} (x_k - \overline{x}_k)^2 \sum\limits_{j=1}^{m} (x_j - \overline{x}_j)^2}} \tag{7}$$

Calculating the Amount of Information for Each Indicator. The formula for calculating the information quantity C_k for each index is shown in Eq. (8).

$$C_k = \sigma_k \sum_{j=1}^{m} (1 - r_{kj}) \tag{8}$$

Calculating Objective Weights. The objective weights w_{ok} of each indicator is calculated as shown in Eq. (9).

$$w_{ok} = \frac{C_k}{\sum\limits_{k-1}^{m} C_k} \tag{9}$$

Combination Empowerment. After obtaining the subjective weights w_{sk} and objective weights w_{ok}, the combination weights W_k are calculated according to the multiplicative synthetic normalization method as shown in Eq. (10).

$$W_k = \frac{w_{ok} w_{sk}}{\sum\limits_{k=1}^{m} w_{ok} w_{sk}} \tag{10}$$

Fuzzy Comprehensive Evaluation. Fuzzy comprehensive evaluation method specifically consists of the following steps.

Building Fuzzy Sets. Firstly, the factor set of the evaluation object is determined, including m evaluation indicators at this level. Secondly, the evaluation set of comprehensive evaluation is established, which is the evaluation of the state of each indicator.

Determining the Relative Affiliation Matrix. The measured data of n evaluation objects and m evaluation indexes are used as the original matrix and are dimensionless by row. If the row is a positive indicator, the original data is divided by the maximum value of the row. If the row is a negative indicator, the minimum value is divided by the original data. The relative affiliation matrix R is shown in Eq. (11), where r is the value of each indicator after dimensionless processing of the original data.

$$R = r_{m \times n} = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mn} \end{bmatrix} \tag{11}$$

Fuzzy Comprehensive Evaluation. The combined weight set W_k is synthesized with the relative affiliation matrix R to obtain the fuzzy comprehensive evaluation model of each index, as shown in Eq. (12).

$$E = W_k \cdot R = (W_1, W_2, \cdots, W_m) \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mn} \end{bmatrix} = (e_1, e_2, \cdots, e_n) \tag{12}$$

The composite score S under the percentage system is calculated by $S = 100E$.

3 Example Analysis

3.1 Calculating Combination Weights

Three experts were invited to score the importance of each index of the improved evaluation index system to obtain the subjective weights. In Python, the objective weights were obtained from the test data. According to Eq. (8), the combination weights of each indicator in this example were calculated as shown in Table 4, where the details of each indicator in the first column are shown in Table 2.

Table 4. Weights of each evaluation index of vehicle intelligent obstacle avoidance function by changing lanes.

Evaluation indicators	Subjective weights	Objective weights	Combination weights
A1	0.511	0.526	0.536
A2	0.489	0.474	0.463
A21	0.524	0.479	0.503
A22	0.476	0.521	0.497
B11	0.217	0.152	0.201
B12	0.204	0.176	0.218
B13	0.163	0.144	0.143
B14	0.131	0.195	0.155
B15	0.130	0.202	0.160
B16	0.153	0.131	0.122
B211	0.212	0.156	0.201
B212	0.199	0.168	0.204
B213	0.180	0.152	0.167
B214	0.128	0.189	0.147
B215	0.128	0.194	0.151
B216	0.149	0.142	0.129
B221	0.212	0.151	0.196
B222	0.199	0.151	0.184
B223	0.180	0.168	0.186
B224	0.128	0.201	0.157
B225	0.128	0.185	0.145
B226	0.149	0.145	0.132

3.2 Fuzzy Comprehensive Evaluation

The evaluation starts from the indicator level and goes up the hierarchy. Take the indicator level of the element straight road test condition as an example, which contains 6 evaluation indexes. The elements of the evaluation set are excellent, good, general, pass, and fail. The evaluation level is divided as shown in Table 5.

Table 5. Evaluation level classification.

Evaluation level	*S*
Excellent	[90, 100]
Good	[80, 90)
General	[70, 80)
Pass	[60, 70)
Fail	[0, 60)

The test data of the three vehicles and the standard data were used as the original data matrix, and after dimensionless processing, the relative affiliation matrix $R_{\mathrm{A}1}$ was obtained, as shown in Eq. (13).

$$R_{A1} = \begin{bmatrix} 1.000 & 1.000 & 1.000 & 0.500 \\ 1.000 & 1.000 & 0.000 & 0.500 \\ 0.875 & 1.000 & 0.554 & 0.187 \\ 0.840 & 1.000 & 0.339 & 0.210 \\ 0.947 & 1.000 & 0.750 & 0.360 \\ 0.826 & 0.758 & 0.606 & 1.000 \end{bmatrix} \tag{13}$$

According to Eq. (12), the comprehensive evaluation result of this level was obtained as shown in Eq. (14).

$$\begin{aligned} E_{A1} &= W_{A1}R_{A1} \\ &= (0.201, 0.218, 0.143, 0.155, 0.160, 0.122)\begin{bmatrix} 1.000 & 1.000 & 1.000 & 0.500 \\ 1.000 & 1.000 & 0.000 & 0.500 \\ 0.875 & 1.000 & 0.554 & 0.187 \\ 0.840 & 1.000 & 0.339 & 0.210 \\ 0.947 & 1.000 & 0.750 & 0.360 \\ 0.826 & 0.758 & 0.606 & 1.000 \end{bmatrix} \\ &= (0.927, 0.969, 0.527, 0.448) \end{aligned} \tag{14}$$

Similarly, the results of other levels and comprehensive evaluation can be obtained, as shown in Table 6, where the details of each indicator in the first column are shown in Table 2.

Table 6. Comprehensive evaluation results of intelligent obstacle avoidance function by changing lanes tests of C1, C2, and C3.

	C1	C2	C3
A21	94.9	97.7	67.6
A22	90.5	97.2	21.9
A1	92.7	96.9	52.7
A2	92.7	97.5	44.9
Total score	92.7	97.1	49.0
Evaluation level	Excellent	Excellent	Fail

3.3 Analysis of Evaluation Results

The comprehensive evaluation method based on the improved evaluation index system was used to evaluate the vehicle intelligent obstacle avoidance function by changing lanes, and the results of the comprehensive evaluation were consistent with the actual test conclusions. The evaluation grades of C1, C2 and C3 are excellent, excellent and fail respectively. The test showed that C3 was not equipped with the intelligent obstacle avoidance function by changing lanes because it pressed line after changing lanes under the three test conditions and a collision occurs under the curve road test condition. C1 and C2 did not crash and did not press the line, and both received excellent. Among them, C2 outperformed C1 in all test conditions. The improved evaluation index system can distinguish whether the vehicle has the intelligent d obstacle avoidance function by changing lanes and evaluate the performance of this function.

4 Conclusion

In order to make a comprehensive evaluation of the intelligent obstacle avoidance function by changing lanes of the unmanned vehicle, the evaluation index system was improved from two aspects of whether the vehicle has the function and the performance of the function. Then, based on the improved G1 method and CRITIC method, the combination weights were obtained by multiplicative synthesis and normalization, and the fuzzy comprehensive evaluation model was established. Finally, the test data of three intelligent commercial vehicles under three test conditions were verified. The results show that the improved evaluation index system can provide more comprehensive, scientific and reasonable evaluation results for the intelligent obstacle avoidance function by changing lanes of vehicles, and can provide a basis for the improvement of this intelligent function. It is necessary to further study the comprehensive evaluation method of vehicle intelligent obstacle avoidance function by borrowing lanes, and form a comprehensive evaluation method of vehicle intelligent obstacle avoidance function.

Acknowledgement. The authors acknowledge the support of National Key Research and Development Program (No. 2019YFC1511505) and Central Public-Interest Scientific Institution Basal Research Fund (No. 2021-9044a).

References

1. Feng, Y., Wang, Z.: Development and Application of Automated-driving Test Scenario Technology, vol. 2. China Machine Press, Beijing (2020)
2. Lu, P.F., Zou, B.S., Li, J.T.: A methodology for cyber security quantitative assessment of intelligent connected vehicles based on CRITIC and entropy method. Cyberspace Secur. **11**(10), 98–103 (2020)
3. Dong, F., Zhao, Y.N., Gao, L.: Application of gray correlation and improved AHP to evaluation on intelligent U-turn behavior of unmanned vehicles. In: International Symposium on Computational Intelligence and Design, Hangzhou, pp. 25–29. IEEE (2016)
4. Zhang, X.X., Liu, W., Yu, B., et al.: Data driven test and evaluation method for intelligent vehicle object detection capability. Comput. Syst. Appl. **26**(11), 249 (2017)
5. Sun, Y., Yang, H., Meng, F.: Research on an intelligent behavior evaluation system for unmanned ground vehicles. Energies **11**(7), 1764 (2018)
6. Li, R., Ma, Y.L., Tian, H., et al.: Comprehensive intelligent quantitative evaluation of autonomous vehicle based on entropy and G1 methods. Automot. Eng. **42**(10), 1327–1334 (2020)
7. Zhao, F.Z., Wang, J.H., Wei, Z.C., et al.: Hierarchical evaluation of smart distribution grid based on improved G1-TOPSIS method. Power Syst. Technol. **40**(10), 3169–3175 (2016)
8. Wu, X.S., Tian, S.X., Yuan, M., et al.: Research on coal mine intelligent evaluation based on subjective and objective weighting VIKOR method. Min. Res. Dev. **41**(04), 165–169 (2021)

An Evaluation Method of Wireless Communication Key Performance Through Receiving the Signal Transmitting by Itself

Qimin Xu[1](✉), Zhi Zhang[1], Xuan Dong[2], and Zhiyu Zheng[3]

[1] Southeast University, Nanjing 210096, China
jimmy.xqm@gmail.com
[2] Research Institute of Highway Ministry of Transport, Beijing 100088, China
[3] Eagle Drive Tech Shenzhen Co., Ltd., Shenzhen 518057, China

Abstract. This paper designs a wireless communication key performance evaluation method through receiving the signal transmitting by itself. The device includes a transmitter and a receiver. The receiver performs message analysis and transmission and measures the consumption of time when processing each message. The transmitter measures the total duration of each message's sending and receiving and counts the number of the messages. The basic parameters measured by the receiver and the transmitter can be used for the quantitative evaluation of communication delay and packet loss rate. This paper proposes a clock frequency deviation calibration method that integrates the internal and external characteristics of the Microprogrammed Control Unit (MCU) crystal oscillator to improve the measurement accuracy. The receiver uses a clock frequency deviation dynamic calibration method based on the real-time temperature. Besides, the transmitter further uses the Pulse Per Second (PPS) signal to dynamically estimate and calibrate clock frequency deviation based on Kalman filter. The evaluation method has the characteristics of high measurement accuracy and low device cost.

Keywords: Communication performance · Receiving the signal transmitting by itself · MCU clock frequency calibration

1 Introduction

Autonomous driving has always been a hot topic in the intelligent transportation system. In order address the problem that autonomous driving is hard to meet the requirements of safety and reliability at this stage, developing the intelligent vehicle-infrastructure system and allowing 'smart' roads to support some of the functions of autonomous vehicles is an effective way to achieve the high degree of automation of cars through the coordinating operation between cars and roads or between cars and cars [1, 2].

Wireless communication has become one of the key basic supporting technologies [3], which can be regarded as a pipeline connecting of 'vehicle to infrastructure or 'vehicle to vehicle'. The performance of wireless communication will directly affect

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 22–29, 2022.
https://doi.org/10.1007/978-981-19-3486-5_3

whether the vehicle-to-road and vehicle-to-vehicle cooperative system can be operated normally.

When evaluating wireless communication performance, a normal method is to install devices that can provide time reference information at the transmitter and the receiver respectively [4, 5], measuring the sending time and the arriving time of the messages to measure the communication delay; analyzing the messages received and sent within a certain period of time, and the frequency of message sending can also be obtained. This method uses a high-precision unified time reference (generally provided by the timing equipment based on the global navigation satellite system) at the transmitter and the receiver, which can ensure high measurement accuracy, but it also leads to troublesome installation and high cost. When the satellite signal is blocked, the time accuracy will be reduced, and the measurement accuracy will be affected.

This paper designs a new type of wireless communication performance evaluation method. The method adopts the way of receiving the signal transmitting by itself and uses the low-cost MCU high-speed internal oscillator clock source to measure the basic parameters required for evaluation. Because the crystal oscillator of the MCU is easily affected by the environment temperature and produces cumulative errors [6], this paper proposes a clock frequency deviation calibration that integrates the internal and external characteristics of the crystal oscillator of the MCU, and according to the working characteristics of the receiver and the transmitting end, different strategies are adopted for dynamic clock frequency calibration to improve the measurement accuracy of the parameters required for evaluation. The method in this paper can perform segmented statistics on the transmission time and analysis time of wireless communication messages, and uses a local clock signal, which is not affected by environmental occlusion, supports the evaluation of multiple communication standards, has the characteristics of good environmental adaptability, high accuracy, and low cost.

2 Evaluation Plan Design

This paper designs a method to evaluate the key performance of wireless communication by the way of receiving the signal transmitting by itself. Both the transmitter and receiver are used in the evaluation. The receiver sets up the message analysis and transmitting mechanism and measures the time for analyzing and transmitting each message. The transmitter measures the total time of each message's sending and receiving and counts the number of messages. The transmitter and receiver respectively use the MCU crystal oscillator for measurement and statistics of the basic parameters required for evaluation. The clock frequency deviation calibration method that integrates the internal and external characteristics of the MCU crystal oscillator is used to improve the accuracy of the counter clock reference, including the clock frequency deviation dynamics based on real-time temperature as well as Calibration and Kalman filter dynamic estimation method of clock frequency deviation based on PPS signal, achieving accurate and reliable evaluation of the key performance of wireless communication.

The MCU is a kind of integrated circuit chip, which adopts super-large-scale integrated circuit technology to integrate the central processing unit with data-handling capability, random access memory, read-only memory, multiple I/O ports, timer/counter, analog-digital converter, a small and complete microcomputer system composed of oscillator clocks and other components integrated on a silicon chip, is widely used in the field of industrial control. In this paper, both the receiver and the transmitter use MCU as the main control unit. The MCU model used in this paper is STM32F107VCT6. The MCU contains multiple 16-bit-counters, temperature sensors, analog-digital converters, commonly used I/O ports and other functions. It also supports serial ports, Universal Serial Bus (USB), network ports, Controller Area Network (CAN) bus interfaces, and other communication methods.

The MCU of the receiver is connected to the wireless device through one of the serial port, USB, network port, and CAN bus interface, to obtain the message received by the wireless device, and can judge whether the wireless device has received the message. The working process of the MCU at the receiver is as follows:

① Initialize the MCU at the receiver and set the clock frequency of counter 1 as 50 kHz.
② Wait for the receiver to receive the message, when the receiver receives the information from the transmitter, it immediately starts counter 1.
③ Dynamic calibration of counter 1 clock deviation. The receiver needs to count the time of analyzing and transmitting time. When calculating the communication delay, this part of the time needs to be subtracted to obtain the real transmission delay. Therefore, the accuracy of the counter 1 clock frequency will also affect the accuracy of communication time evaluation. This text adopts the clock frequency deviation dynamic calibration method based on real-time temperature to improve the clock frequency accuracy of the MCU counter in the receiver.
④ Analyze the received messages, and pack all the analyzed messages with the time of the last frame of messages' analyzing and transmitting, and send them to the receiver interface, and then send them back from the receiver to the transmitter.
⑤ Record the count-value n_1 of counter 1 at this time and reset the counter, then the time consumed for analyzing and transmitting this time $t_1 = n_1/50$ ms, save t_1 and send it back after being packed with the next frame of the message.

The MCU at the transmitter is also connected to the transmitter through one of the serial port, USB, network port, and CAN bus interface, to obtain the message received or sent by the transmitter and can judge whether the transmitter has received or sent a message. The working process of the transmitter is as follows:

① Initialize the MCU at the transmitter and set the clock frequency of counter 2 as 50 kHz.
② When the transmitter sends out the first message, it starts the counter 2 of the MCU at the transmitter, and at the same time adopts the clock frequency deviation dynamic calibration method based on real-time temperature similar to the receiver to set the clock adjustment register, and set the message value N_1 to 1.
③ Judge whether the message has been received. When the message is received, save the count value n_2 of counter 2 and reset the counter, and at the same time add the value of N_1 by 1, to analyze the message processing time t_1 of the previous frame contained in the message.

④ Judge whether a message has been sent. When a message is sent, start the counter 2 and then enter the cycle of judging whether the message is received. Every time the counter 2 is started, the clock frequency deviation dynamic calibration method based on real-time temperature is used to set the clock adjustment register.

Using the clock frequency of n_2 and counter 2, we can get t_2, which is the total time of a message sent from the transmitter and processed and sent back by the receiver.

3 Clock Frequency Deviation Calibration Method

3.1 Dynamic Calibration Method of Clock Frequency Deviation Based on Real-Time Temperature

The receiver needs to count the time consumed by analyzing and transmitting messages. When calculating the communication delay, this part of the time needs to be subtracted to obtain the real transmission delay. Therefore, the accuracy of the counter 1 clock frequency will also affect the accuracy of the evaluation of the communication time. This text adopts the clock frequency deviation dynamic calibration method based on real-time temperature to improve the clock frequency accuracy of the MCU counter at the receiver.

The temperature sensor inside the STM32F107VCT6 MCU is connected to the input of the analog-digital converter 1. Every time the counter 1 is started, the AD conversion of the analog-digital converter 1 is also started to obtain the current temperature information, which is used to calculate the frequency deviation *DFi*:

$$\begin{aligned} DFi = {} & DFA + DFB * (TMPDAT - Toff) + DFC * (TMPDAT - Toff)^2 \\ & + DFD * (TMPDAT - Toff)^3 + DFE * (TMPDAT - Toff)^4 \end{aligned} \tag{1}$$

Among them, *DFA/DFB/DFC/DFD/DFE* are the compensation coefficients, *TMPDAT* is the output value of the temperature sensor, and *Toff* is to correct the temperature sensor offset.

DFi can be used to set the internal high-speed clock adjustment register HSITRIM to realize clock deviation dynamic calibration inside the MCU.

3.2 Clock Frequency Deviation Kalman Filter Dynamic Estimation Method Based on PPS Signal

The accuracy of the clock frequency of the MCU counter at the transmitter directly affects the accuracy of t_2 and will also determine the accuracy of the evaluation of communication delay. Therefore, the transmitter introduces the PPS signal for dynamic calibration of the clock frequency of the MCU and statistics of the total duration of the evaluation. Since t_2 is significantly bigger than t_1, t_2 is also more affected by the clock frequency deviation. The transmitter not only uses the clock frequency deviation dynamic calibration method based on real-time temperature to correct the clock deviation inside the MCU, but also uses the PPS signal to observe the external characteristics of the clock frequency. Perform clock offset correction again to further improve the measurement accuracy of t_2. PPS signal is an accurate pulse signal which is one second for one time [7], which can be derived from the internal satellite positioning system receiver of the transmitter or the external satellite positioning system receiver.

The I/O interface of the MCU of the transmitter is connected with the PPS signal, to realize the capture of the PPS signal, and MCU at the transmitter performs the working process of clock frequency dynamic calibration and total time statistics evaluation is as follows:

① Initialize the MCU at the transmitter, set the clock frequency of counter 3 to be the same as that of counter 2, which is 50 kHz.

② When the first PPS signal is received, start the counter 3, and use the clock frequency deviation dynamic calibration method based on real-time temperature to set the clock adjustment register, and set the PPS count value N_2 as 1 at the same time.

③ Judge whether the next PPS signal is captured. When the next PPS signal is captured, save the count value n_3 of counter 3 and N_1 at this time, and add 1 to N_2, restart the counter. Every time counter 3 is started, use clock frequency deviation dynamic calibration method based on real-time temperature to set the clock adjustment register.

④ Continue to judge whether the next PPS signal of the loop is received.

The time interval between the two PPS signals is exactly 1 s, so the count value n_3 is the clock frequency observed with the PPS signal. Counter 3 is a 16-bit counter, the maximum count value is 65535.When the clock frequency is 50 kHz, n3 should be about 50000, and there will be no overflow that the maximum count value is exceeded. The clock frequency deviation of counter 3 observed by the PPS signal is (n_3 – 50000). Since the clock frequency set by counter 2 and counter 3 are the same and belong to the same MCU, (n_3 – 50000) can also be regarded as the observation value of clock frequency deviation of counter 2, and based on Kalman filter, perform counter 2 clock frequency deviation dynamic estimation:

The matrix form of the discretized Kalman filter state equation is:

$$\mathbf{X}(k) = \boldsymbol{\varphi}(k, k-1) \cdot \mathbf{X}(k-1) + \mathbf{W}(k-1) \tag{2}$$

In Eq. (2), k represents the discretization time; the system state vector quantity is $\mathbf{X} = [\Delta f]$, that is the estimated counter 2 clock frequency deviation; $\mathbf{W}(k-1)$ represents the system white Gaussian noise vector quantity of zero mean value, the system noise covariance matrix $\mathbf{Q}(k-1)$ corresponding to $\mathbf{W}(k-1)$ is: $\mathbf{Q}(k-1) = [\sigma_w^2]$, σ_w^2 represents the variance corresponding to the system white Gaussian noise w of; the state transition matrix is $\boldsymbol{\varphi}(k, k-1) = [1]$ (unit matrix). This is because the clock frequency deviation in a short time has good consistency, so it can be considered that the clock frequency deviation at the current sampling time is equal to the clock frequency deviation at the next sampling time.

The discretization matrix form of the Kalman filter observation equation is:

$$\mathbf{Z}(k) = \mathbf{H}(k) \cdot \mathbf{X}(k) + \mathbf{V}(k) \tag{3}$$

In Eq. (3), **Z** is the observation vector, **H** is the observation matrix, and **V** is the zero mean value observation white noise vector quantity that is not correlated with ***W***. Because both the observation vector and the state vector are both clock frequency deviation, so, $\mathbf{H}(k) = [1]$, $\mathbf{Z}(k) = [fo]$, fo is the clock frequency deviation measured by the PPS signal, $fo = \mathrm{n}_3 - 50000$, and the observing noise variance matrix **R** corresponding to **V** can be expressed as $\mathbf{R} = [\sigma^2]$, σ^2 represents the variance of the observing noise.

For the system state equation and measurement equation described in Eq. (2) and (3), the Kalman filter theory is used to establish the following standard filter recursion process [8]:

State one-step prediction equation:

$$\hat{\mathbf{X}}(k, k-1) = \boldsymbol{\varphi}(k, k-1)\hat{\mathbf{X}}(k-1)$$

One-step prediction error variance matrix:

$$\mathbf{P}(k, k-1) = \boldsymbol{\varphi}(k, k-1)\mathbf{P}(k-1)\boldsymbol{\varphi}'(k, k-1) + \mathbf{Q}(k-1)$$

Filter gain matrix:

$$\mathbf{K}(k) = \mathbf{P}(k, k-1) \cdot \mathbf{H}'(k) \cdot \left[\mathbf{H}(k)\mathbf{P}(k, k-1)\mathbf{H}'(k) + \mathbf{R}(k)\right]^{-1}$$

State estimation:

$$\hat{\mathbf{X}}(k) = \hat{\mathbf{X}}(k, k-1) + \mathbf{K}(k)\Big[\mathbf{Z}(k) - \mathbf{H}(k) \cdot \hat{\mathbf{X}}(k, k-1)]\Big]$$

Estimated error variance matrix:

$$\mathbf{P}(k) = [\mathbf{I} - \mathbf{K}(k) \cdot \mathbf{H}(k)] \cdot \mathbf{P}(k, k-1)$$

After the above recursion calculation, the clock frequency deviation Δf of the counter 2 can be estimated in real time.

Use Δf to get the calibrated clock frequency $f = 50 + \Delta f$ KHz, and then use the dynamically calibrated clock frequency to calculate t_2, $t_2 = n_2/f$.

4 Key Performance Indicator Calculation Method

After obtaining the time-related parameters t_1 and t_2, as well as the number of sent messages N_1 and the number of received messages N_2, the evaluation of wireless communication performance can be realized.

In each evaluation, the first PPS signal captured time is used as the initial point of the evaluation, and the analyzing and transmitting consumption time of the ith message is t_{1i}, and the sending and retrieving time of the ith message is t_{2i}, $i = 1, 2, \ldots, N_1$, the communication delay of the ith message is:

$$\tau_i = \frac{t_{2i} - t_{1i}}{2} \tag{4}$$

The communication delay of this evaluation is:

$$\tau = \frac{1}{N_1}\sum_{i=1}^{N_1}\tau_i = \frac{1}{N_1}\sum_{i=1}^{N_1}\frac{t_{2i} - t_{1i}}{2} \tag{5}$$

The packet loss rate of this evaluation is:

$$\eta = \frac{N_1 - N_2}{N_1} \times 100\% \tag{6}$$

5 Experimental Verification

In this paper, ANPU-Link5200-30NHD, an industrial self-organized network equipment, is used as the test object to verify the proposed evaluation method. The evaluation equipment is shown in Fig. 1.

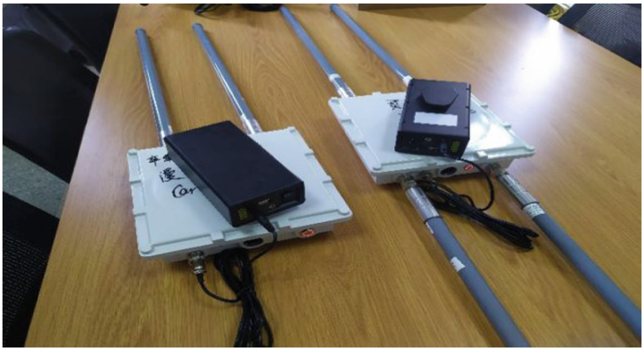


Fig. 1. Tested wireless communication equipment.

The software interface of the evaluation process is shown in Fig. 2.

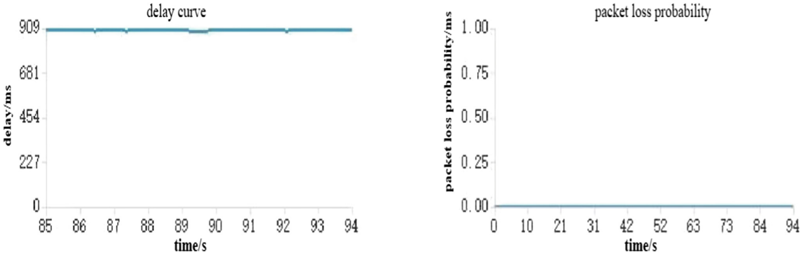


Fig. 2. Evaluation results.

The above-mentioned equipment has been tested and evaluated many times, and the test results are relatively stable. The delay is 909 ms and the packet loss probability is 0%, which is consistent with the nominal value of the product.

6 Summarize

This paper adopts the method of receiving the signal transmitting by itself to realize the evaluation of wireless communication performance. It does not need to unify the clock standard of the transmitter and the receiver, and there is no requirement for the wireless communication mode. According to the working characteristics of the receiver and the transmitter, different strategies are used to perform dynamic clock frequency calibration to improve the measurement accuracy of the time-related parameters required for the evaluation. The transmitter is less affected by the clock frequency deviation due to the shorter measurement time. thus, the clock frequency deviation dynamic calibration method based on real-time temperature is used. The measurement time required by the transmitter is relative long. In addition to the real-time clock frequency deviation dynamic calibration, the PPS signal is further used to perform the Kalman filter dynamic estimation of the clock frequency deviation, realizing the clock frequency deviation calibration that integrates the internal and external characteristics of the MCU crystal oscillator. This paper achieves an accurate evaluation of the key performance of wireless communication.

Acknowledgement. This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFB1600803, in part by the National Natural Science Foundation of China under Grant 41904024.

References

1. Grau, G.P., Pusceddu, D., Rea, S., Brickley, O., Koubek, M., Pesch, D.: Vehicle-2-vehicle communication channel evaluation using the CVIS platform. In: 2010 7th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP 2010), Newcastle, pp. 449–453. IEEE (2010)
2. Gupta, M., Benson, J., Patwa, F., et al.: Secure V2V and V2I communication in intelligent transportation using cloudlets. IEEE Trans. Serv. Comput. **13**(14), 1–13 (2020)
3. Dey, K.C., Rayamajhi, A., Chowdhury, M., et al.: Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network–Performance evaluation. Transp. Res. Part C: Emerg. Technol. **68**, 168–184 (2016)
4. He, C.Z., Xia, Y.S., Wang, L.Y.: A universal asynchronous receiver transmitter design. In: 2011 International Conference on Electronics, Communications and Control (ICECC), pp. 691–694. IEEE (2011)
5. Zuo, G.Q., Luo, W.B., Fei, L.: The synchronization of the transmitter and receiver design based on GPS. Geophys. Geochem. Explor. **30**(2), 159–161 (2006)
6. Wenrich, M.L., Christensen, P.R.: Optical constants of minerals derived from emission spectroscopy: application to quartz. J. Geophys. Res.: Solid Earth **101**(B7), 15921–15931 (1996)
7. Gasparini, L., Zadedyurina, O., Fontana, G., et al.: A digital circuit for jitter reduction of GPS-disciplined 1-pps synchronization signals. In: 2007 IEEE International Workshop on Advanced Methods for Uncertainty Estimation in Measurement, pp. 84–88. IEEE (2007)
8. Verhagen, S., Teunissen, P.J.G.: Least-squares estimation and Kalman filtering. In: Teunissen, P.J.G., Montenbruck, O. (eds.) Springer Handbook of Global Navigation Satellite Systems. SH, pp. 639–660. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-42928-1_22

A Method for Optimizing Communication Network Topology Based on Genetic Algorithm

Pengfei Yu[1], Yonghong Shi[2], Lei Wang[1](✉), Shijie Ke[3], and MengMeng Yin[1]

[1] Army University of Engineering, Nanjing 210001, Jiangsu, China
iponly@126.com
[2] Troop 69036, Korla 841000, Xinjiang, China
[3] Troop 75841, Haikou 570100, Hainan, China

Abstract. This Paper studies the reliability of communication network. Taking the communication network of peer-to-peer structure as the research object, from the perspective of topological structure, the reliability optimization model of communication network is constructed, and an improved genetic algorithm is proposed to solve the model. For the objective function based on natural connectivity, the paper designs variable coding, improves the selection operation, and defines the crossover operation and mutation operation. Experiments show that as the number of iterations increases, the natural connectivity value shows an upward trend, and the network topology changes from "dispersed periphery" to "closer core-periphery". The simulation analyzes the structural attributes of the optimized communication network, and verifies the effectiveness and feasibility of the communication network topology optimization model and the use of genetic algorithm to solve the model. After the network topology is optimized, the network degree distribution is changed, in which the number of low-degree nodes increases, while the number of high-degree nodes decreases. The reliability of the communication network after the optimization of the algorithm proposed in this paper is improved under both random and deliberate attacks.

Keywords: Communication network · Reliability · Genetic algorithm (GA) · Topology optimization · Natural connectivity

1 Introduction

The network structure (i.e., network topology) of the communication network [1] generally refers to the geometric connection shape of network nodes and transmission lines, which is related to the problem of network connectivity [2]. It is an important requirement to explore the communication network with high reliability from the internal structure of the network in various practical applications.

At present, many achievements have been made in the research of communication network reliability. Literature [3] proposes a communication network topology optimization method to realize navigation sharing, establishes the MCCN topology model of navigation sharing in order to find the communication network topology with the minimum number of communication connections (MCCN) under different conditions, and

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 30–40, 2022.
https://doi.org/10.1007/978-981-19-3486-5_4

designs the corresponding methods, which theoretically proves the effectiveness of the algorithm. Literature [4] proposed the reliability analysis and optimization algorithm of power communication network (PCN) based on resource correlation characteristics, and improved the reliability of power communication network through resource redundancy and expansion strategy. Literature [5] proposes a power communication network fault recovery algorithm based on service characteristics and node reliability. By comparing with traditional algorithms, it is verified that this algorithm can improve the fault recovery rate and profit of power communication network, which has great practical application value. Literature [6] takes complex networks as the research object and establishes a network reliability and node importance evaluation model based on redundancy. The results show that the model algorithm can provide a solution to the construction problem of high reliability networks under certain constraint cost. Literature [7] uses FCM algorithm to identify and backup key resources of power communication network, thus improving the reliability of power communication network.

This paper constructs the reliability optimization model from the perspective of the communication network topology structure, which belongs to NP-hard problem and is difficult to solve directly. Aiming at the objective function, this paper designs an improved genetic algorithm, a heuristic method to solve the model. The coding process is that the network is transformed into the adjacency matrix. The optimized variable is the coding in the form of the adjacency matrix of the graph. Roulette, truncation and sorting and grouping are selected as the three selection operations. The simulation results show that the algorithm can improve the reliability of the communication network effectively.

2 Communication Network Reliability Optimization Model Based on Natural Connectivity

In this paper, the natural connectivity is used as the network reliability measure index to optimize its topology [8, 9]. The basic assumptions for the communication network graph G are as follows:

(1) The communication network is an unauthorized and undirected simple graph, Set a_{ij} as $\{a_{\mathrm{ij}} = a_{ji} = 1|e(v_i, v_j) \in E(G)\}$ and $\{a_{ij} = a_{ji} = 0|e(v_i, v_j) \notin E(G)\}$.

(2) It satisfies the connected graph, that is, the subsmall eigen root of its Laplace matrix $\mu > 0$. When the network size increases, the solving time of subsmall characteristic roots is too long. To facilitate processing, the function is defined in this paper. $C(G) = \begin{cases} > 0, \mu > 0 \\ \leq 0, \mu \leq 0 \end{cases}$, C(G). traverse every node through depth-first search, and the result of traversing all nodes can connect any other nodes.

Natural connectivity is defined as follows:

Assume that in one network, the number of ways of length k between any node v_i and v_j is n_{ij}^k, and then sum over the relation of i, j, k:

$$S = \sum_{i=1}^{N} \sum_{j=1}^{N} \sum_{k=0}^{\infty} n_{ij}^k \tag{1}$$

The value of S reflects the number of redundant paths in the network. Obviously, S will be a complex expression, expressed by the number of v_i closed paths of length k starting and ending as follows:

$$S = \sum_{i=1}^{N} \sum_{k=0}^{\infty} n_i^k = \sum_{k=0}^{\infty} n_k \tag{2}$$

The contribution of closed paths is measured by dividing S by the factorial of the length between nodes as k. Shorter closed paths have a greater impact on the redundancy of alternative paths, which is expressed as follows:

$$S' = \sum_{k=0}^{\infty} \frac{n_k}{k!} \tag{3}$$

the number of all closed channels n_k of length k in the network, which can be expressed as:

$$n_k = \sum_{i=1}^{N} \mu_k(i) = \sum_{i=1}^{N} \lambda_i^k \tag{4}$$

So:

$$S' = \sum_{k=0}^{\infty} \frac{n_k}{k!} = \sum_{k=0}^{\infty} \frac{\sum_{i=1}^{N} \lambda_i^k}{k!} = \sum_{i=1}^{N} e^{\lambda_i} \tag{5}$$

λ_i is the eigen root of the network adjacency matrix.

There are many factors that affect the reliability of network [10]. When the number of network nodes is certain, the number of links in the network becomes the main factor. The natural connectivity value is strictly monotonically increasing with respect to the increase of the edge. If there is no limit on the number of network links, the fully connected network topology will be the most reliable network. But in fact, the network construction will be limited by the cost and so on. Obviously, the more the number of links, the more the network cost will be. Therefore, it is necessary to study the problem of network reliability when the number of links W is certain. In this paper, it is assumed that the constraint conditions of the number of links in the communication network are as follows:

$$W = |\mathrm{E}| = \frac{1}{2} \sum_{i=0}^{N} \sum_{j=0}^{N} a_{ij}, \tag{7}$$

Based on the above analysis, the topology optimization model of the communication network can be established:

$$\begin{gathered}
\max_{G} \bar{\lambda} = \ln(\frac{1}{N}\sum_{i=1}^{N} e^{\lambda_i}) \\
s.t. \sum_{i=0}^{N}\sum_{j=0}^{N} a_{ij} = 2W \\
a_{ij} = 0 \; or \; a_{ij} = 1 \\
a_{ii} = 0 \\
a_{ij} = a_{ji} \\
C(G) > 0
\end{gathered} \tag{8}$$

where, λ_i is the eigen root of the adjacency matrix A (G) composed by a_{ij}.

3 Communication Network Reliability Simulation and Optimization Method Based on Genetic Algorithm

The above model (8) belongs to the nonlinear 0–1 integer programming problem and is a typical NP-hard problem, which cannot be solved directly by using some current solvers. Traditional methods to solve NP-hard problems include using similar problems to replace the original problem, which is complicated and difficult to solve and cannot be solved directly, and looking for problems with high similarity and easy to solve to replace them. The other method is to use the heuristic search method [11]. Swarm intelligence algorithm is preferred in this paper. Since the adjacency matrix of network graph is 0–1 matrix, the genetic algorithm is chosen in this paper to search the problem for the convenience of coding method.

3.1 Variable Coding

As mentioned above, the communication network can be represented as a simple graph with no right and no direction, and the graph itself can be represented by 0–1 adjacency matrix, which is appropriate to be directly regarded as a chromosome. Therefore, each adjacency matrix is the optimization variable of the genetic algorithm, namely, the code of the solution.

3.2 Selection Operation

In order to find the communication network topology with higher reliability, the individuals with larger results are selected according to the objective function value in each selection operation. In this paper, roulette selection, truncation selection, sorting and grouping selection were selected for comparison and analysis of three different operations.

The truncation selection method sorted the individuals in the population in descending order according to the value of the objective function (solving Max) and selected the first N individuals to enter the next generation. The algorithm was operated as follows:

(1) Calculate the objective function value of each individual (adjacency matrix) in the initial population;
(2) Rank in descending order according to fitness value;
(3) Intercept the top n best individuals to enter the next generation.

The idea of sorting, grouping and selection is graphically represented as follows:

① Set an initial population with 9 individuals as an example, the data in the table is the individual fitness value of the population

5.53	5.47	4.88	5.36	4.81	5.30	5.19	6.03	6.00
1	2	3	4	5	6	7	8	9

② The individuals of the population were arranged according to the fitness value from the largest to the smallest

6.03	6.00	5.53	5.47	5.36	5.30	5.19	4.88	4.81
8	9	1	2	4	6	7	3	5

③ On average, three segments were taken from the arrayed individuals
④ Each segment is selected at random in a different proportion.
⑤ Selected individuals

6.03	6.00	5.53	5.47	5.30	5.19
8	9	1	2	6	7

⑥ Select from the beginning the individual that was lost due to the selection operation.
⑦ Insert the head individual selected in step ③ into step ⑤ to form a new individual

6.03	6.00	5.53	5.47	5.30	5.19	6.03	6.00	5.53
8	9	1	2	6	7	8	9	1

Compared with the initial population, the average fitness value of the final population was improved. The three selection algorithms selected in this paper are easy to operate. After calculating the fitness value, the superior individuals can be selected only by sorting, grouping, inserting and other basic operations.

3.3 Cross Operation

Selecting different adjacency matrices to exchange the intermediate elements of the matrix to carry out gene location transformation in the crossover position. The specific operation steps are as follows:

(1) Conduct random pairing operation on population individuals;

(2) Set the same position crossing points for the paired chromosomes;
(3) Match each other according to the set cross probability P (Fig. 1).

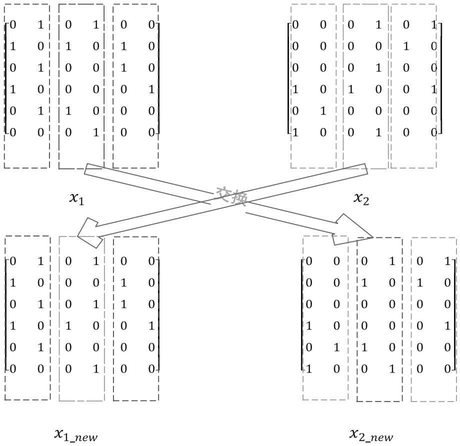


Fig. 1. Cross process

3.4 Mutation Operation

This paper mainly uses single-point mutation, that is, only a certain bit in the gene sequence needs to be mutated, taking binary coding as an example, that is, 0 becomes 1, and 1 becomes 0. Mutation is a process of randomly selecting individuals from a population and getting new individuals by mutation with a certain probability. For example, mutate an individual by the following method:

$$X[i][j] = \begin{cases} X[i][j], & p > v\_c \\ 1 - X[i][j], & p \leq v\_c \end{cases} \tag{9}$$

$X[i][j]$ is an element in the adjacency matrix, P is a random number located between [0, 1], and V_c is the mutation probability.

4 Algorithm Improvement and Model Constraint

4.1 Algorithm Improvement

The traditional genetic algorithm is prone to the problem of slow convergence speed. This paper improves the local optimization strategy, as follows.

(1) Local search: at the end of each iteration, local search optimization is carried out for each chromosome in the population. The specific operation of local search is

the inverse operation of any bit of the adjacency matrix represented by the current chromosome, which can be expressed as the function N (G). The update of staining by local search can be expressed as:

$$G_k^{(next)} = \begin{cases} N(G_k), F(G_k) < F(N(G_k)) \\ G_k, F(G_k) \geq F(N(G_k)) \end{cases} \tag{10}$$

where, (G) represents the fitness of chromosomes and the local optimization times of fixing each chromosome, such as 50 times.

Parameter adaptation: in order to ensure the diversity of the algorithm in the early stage and the concentration in the later stage, this paper adaptively adjusts the crossover probability and mutation probability:

$$\begin{aligned} P_c^{(i)} &= P_c \rho_1^i \\ V_c^{(i)} &= V_c \rho_2^i \end{aligned} \tag{11}$$

where ρ_1 and ρ_2 are constants less than 1 respectively, i denoting the number of iterations.

4.2 Model Constraints

Because the optimization model contains a large number of constraints, most of which are strong constraints, such as the limit on the number of edges of the graph is constant, such constraints will make most chromosomes do not meet the conditions and will be eliminated, resulting in too few or even zero number of offspring chromosomes in the early iteration. Therefore, in this paper, the method of repairing infeasible solution and penalty function are combined to deal with the constraint conditions of the problem. The details are as follows:

(1) Undirected simple graph constraint of network graph. In population initialization, crossover, mutation and local optimization, the adjacency matrix of graph may not satisfy the undirected simple graph constraint, like $a_{ij} \neq a_{ji}$. Therefore, in this paper, the adjacency matrix is repaired by successive scan after each operation involving changing the graph structure.

(2) Constraint on the number of edges in the network graph. Since almost any operation will change the number of edges of the graph, this paper chooses to repair the infeasible solution of the graph. The repair method is: Assume that the number of edges is

(3) $W' = \frac{1}{2}\sum_{i=0}^{N}\sum_{j=0}^{N} a_{ij}$, $\Delta W = |W' - W|$, $W' - W > 0$, ΔW element $\{\mathrm{a}_1, \mathrm{a}_2, \ldots, \mathrm{a}_{\Delta \mathrm{W}}\}$, the value of each element in the set is 1, and the subscript in the original adjacency matrix is satisfied $j \geq i$. The value of the elements in the set is changed to 0, and then the undirected simple graph repair operation in satisfying (1) is performed. On the contrary, if $W' - W < 0$, do the opposite operation.

(4) Connectivity constraints on graphs. It is difficult to repair the connectivity of graphs. In addition, through experiments, it is found that the probability of randomly generated graphs being connected is more than 95%, which means that only a relatively

small number of graphs are not connected graphs. Therefore, in the training process, if the solution does not meet the connectivity constraint, the solution is abandoned, that is, the penalty function method is used, and the fitness value of the solution that does not meet the constraint is set as negative infinity.

5 Simulation Experiment and Analysis

5.1 Experimental Simulation of Optimized Topology Structure

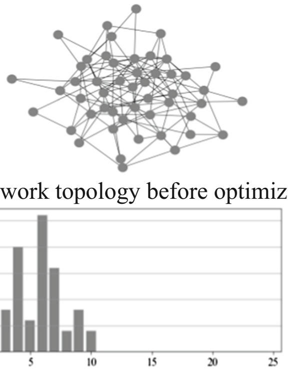
In order to verify the effectiveness of the network topology optimization algorithm proposed in Sect. 2, the simulation running environment is: 64-bit Windows10 operating system, Python 3.8, Intel i7 9570H processor, main frequency 2.6 GHz, memory 16 GB, and parameter Settings are shown in Table 1. Firstly, the initial communication network is constructed to obtain its adjacency matrix A (G). Then initialize the genetic algorithm through the parameters set in Table 1. Then the optimal value of natural connectivity is obtained according to the steps of genetic algorithm in Sect. 4.

Table 1. Parameter settings

Parameter	The values
(W)	50
The population size (POPU_NUM)	100
Number of genetic iterations (ITER_TIME)	100
Crossover probability (P_C)	0.88–0.92
Crossover probability diminishing parameter (ρ_1)	0.995
Mutation probability (V_c)	0.008–0.012
Variation probability decreasing parameter (ρ_2)	0.995
Number of local optimization search iterations (ITER_LOCAL)	50

5.2 Network Topology Analysis

In the process of simulation, ER random graph was selected as the research object. The basic parameters were defined as: the number of nodes N = 50 and the probability of side connection p = 0.12. The generated ER network (connected graph) topology structure and degree distribution were shown in Fig. 2.

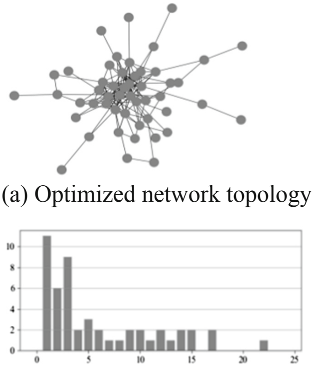


(a) Network topology before optimization

(b) Network degree distribution before optimization

Fig. 2. Network topology and degree distribution

With the number of network nodes and links unchanged, the topology and degree distribution of the communication network before and after optimization are shown in Fig. 3 and Fig. 4 respectively. As the number of iterations increases, the natural connectivity values all show an obvious upward trend, as shown in Fig. 5. Therefore, genetic algorithm can be used to solve the topology optimization model of communication network, and the advantages of fast convergence of algorithm are used. The horizontal axis shows the distribution of degrees and the number line is the probability in Fig. 3.



(a) Optimized network topology

(b) Optimized network degree distribution

Fig. 3. Network topology and degree distribution

Based on the above simulation results, the following basic conclusions can be drawn:

(1) Simulation analysis verifies the effectiveness of the communication network topology optimization model and the feasibility of using genetic algorithm to solve the model.
(2) After optimization by genetic algorithm, the degree distribution of the communication network is changed, in which the network nodes tend to be connected with

the degree nodes, and the number of degree nodes increases while the number of degree nodes decreases.

(3) According to Fig. 3(b) and Fig. 4, the degree distribution of the network is basically a binomial distribution before optimization, while the number of nodes with high medium value increases after optimization, and the number of nodes with high degree decreases successively from low to high degree. Therefore, after the optimization of ER network topology, nodes with low degree tend to connect with nodes with high degree.

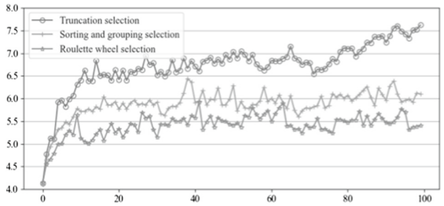


Fig. 4. Iterative optimization of natural connectivity

6 Conclusion

In this paper, the topology optimization model of the communication network is established, and the solution method based on genetic algorithm is proposed. The feasibility of the model and method is verified by simulation analysis. The main work includes: 1) establishing a combinatorial optimization model for the reliability of communication network, which takes the natural connectivity degree as the objective function and the number of edges as the constraint condition; 2) A simulation and optimization algorithm of communication network reliability based on genetic algorithm is proposed. Variable coding is designed, selection operation is improved, crossover operation and mutation operation are defined, and the algorithm flow is given. 3) analyzed the network topology structure and the distribution properties before and after optimization, the research shows that the optimized network presents obvious correlation patterns with match degree, degree of small nodes tend to be connected to the degree of the node, a relatively high number of nodes gathered themselves together, and connection between the high number of nodes is more, most of the connection between the nodes is less, present a “core - periphery” network topology structure. Through the reliability analysis, it is found that the communication network optimized by genetic algorithm has higher anti-damage ability when facing random de-point attacks and de-edge attacks according to the number of mesas, while the anti-damage ability is relatively poor when facing deliberate de-point attacks. Therefore, in practical application, the initial communication network topology should be constructed according to the adaptability of attack strategies.

References

1. Zhuo, Y., Peng, Y.F., Long, K.P.: Improving robustness against the coordinated attack by removing crashed hub nodes in complex network. In: 2009 Asia Communications and Photonics Conference and Exhibition (ACP), vol. 2009. IEEE (2009)
2. Dong, F.H., Feng, Y.Q., Yin, Z.H., et al.: Topology design of network based on deep reinforcement learning with strategy of elite. J. Air Force Eng. Univ. **20**(04), 52–58 (2019)
3. Dang, Z.H., Zhang, Y.L.: Optimization of communication network topology for navigation sharing among distributed satellites. Adv. Space Res. **51**(1), 143–152 (2013)
4. Ye, Z.Y., Chen, Z.Y., Ni, P.C., Pu, Q., Li, L.L.: Reliability analysis and optimization algorithm of power communication network based on resource association features, pp. 116–119 (2020)
5. Yan, L.J., et al.: Power communication network fault recovery algorithm based on service characteristics and node reliability. In: 2020 4th International Conference on Smart Grid and Smart Cities (ICSGSC). IEEE (2020)
6. Wang, Z.H., Jiang, D.L., et al.: Complex network invulnerability and node importance evaluation model based on redundancy. Complex Syst. Complex. Sci. **17**(03), 78–85 (2020)
7. Fu, J.J., et al.: Reliability optimization algorithm for power communication network based on improved clustering algorithm. Comput. Technol. Autom. **39**(04), 92–95 (2020)
8. Tan, Y.J., Lv, X., Wu, J., et al.: Some thoughts on the research of the destructibility of complex networks. Syst. Eng.-Theory Pract. **28**, 116–120 (2008)
9. Zhang, Y., Yang, G.Y.: The optimization of wireless sensor network topology based on FW-PSO algorithm. J. Electron. Inf. Technol. **43**(02), 396–403 (2021)
10. Zhang, B., Gan, Z.C., Yu, C.R.: Complex network topology optimization based on NSGA-II. J. Inf. Eng. Univ. **20**(05), 532–537 (2019)
11. Yang, J.H., Peng, X.D., Chao, T.J.: Topology analysis and optimization of power communication network based on complex network. Comput. Digit. Eng. **46**(11), 2319–2322+2328 (2018)

Network Security Risk Analysis of Ship Intelligent Navigation

Yu Zang[1,2](✉), Wen Liu[1,2], Shikai Sun[2], Mingzhi Shi[2], Ming Li[3], and Xiaoyong Kang[1]

[1] China Transport Telecommunications and Information Center, Beijing, China
zangyu@bjtu.edu.com

[2] National Engineering Laboratory of Transportation Safety and Emergency Informatics, Beijing, China

[3] China Ship Research and Development Academy, Beijing, China

Abstract. The intelligent ship is drawing increasing attention with its advantages of safety, reliability, energy-saving, environmental protection, and economic efficiency. Compared with traditional ships, the intelligent ship is manifested based on autonomous situational perception, risk identification, and intelligent decision-making functions. The realization of these functions depend on the support of an efficient, reliable, and stable ship-to-shore communication network. Therefore, network security risk analysis of intelligent ship navigation becomes critical. This paper comprehensively analyzed the intelligent ship navigation network security attacks and risks. Firstly, the intelligent ship and some typical schemes such as Advanced Autonomous Waterborne Applications (AAWA) were introduced, and the technical framework and functional modules of intelligent ship navigation were presented. Then the network security requirements from system potential threats and external malicious attacks were analyzed, four security risks including damage, misdirection, obfuscation, and denial of service were classified. Meanwhile, a risk analysis model to quantify the risks from different modules was envisaged and a case study was carried to verify this model. Finally, we drew some interesting conclusions and prospects.

Keywords: Intelligent ship · Ship intelligent navigation · Cyber-attack · Risk analysis · Potential threats

1 Introduction

In recent years, intelligent ships incorporate new technologies such as modern information and artificial intelligence, which own outstanding characteristics such as safety, reliability, energy-saving, environmental protection, and economic efficiency [1]. They are extensively applied in maritime transportation, ocean research, maritime rights protection, and military fields [2], which become the key direction of the future ship researches. Aiming to improve the safety of marine operations and reduce consumption of ship fuel, countries around the world are actively carrying out research on related technologies and accelerating the transformation of the role of the crew on board. In the future, drivers

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 41–50, 2022.
https://doi.org/10.1007/978-981-19-3486-5_5

working in shore-based control centers can remotely control multiple remote ships at the same time. In the meantime, each ship can automatically perceives the ship's status and surrounding environment, make a certain degree of navigation decision, timely upload relevant information to the shore-based control center, and obtain relevant support information from the shore-based as needed. Therefore, compared with traditional ships, the intelligent ships are mainly manifested in the intelligent navigation function based on autonomous situational perception, risk identification, and intelligent decision-making techniques. Ship-to-shore communication networks support the future development of intelligent ships in the direction of autonomy and unmanned [3]. Hence, intelligent ship navigation poses a higher challenge to network security risk management and control. Nowadays, cyber security incidents in the shipping industry are increasing [4]. In 2015, the London Shipowners' P&I Association announced that the number of ship online frauds is increasing, including intercepting the mail of ship agents, hacking their email accounts to implement plans to replace the original payment account with a new bank account. In 2017 and 2018, Petya's cyber virus hit the world, as a result, the IT systems of many well-known shipping companies' offices and some business units around the world failed and suffered heavy losses. There is a research gap to analyze and monitor the network security risk of ship intelligent navigation. This paper comprehensively analyzes the research status of the ship intelligent navigation network security attacks and risks, the organization is as follows: Sect. 2 introduced the intelligent ship and some typical schemes such as AAWA and presented the technical framework and modules of ship intelligent navigation. Section 3 analyzed the network security requirements from system potential threats and external malicious attacks, 4 security risks including damage, misdirect, obfuscate, and Denial of Service (DoS) were classified. Section 4 envisaged a risk analysis model to qualify the risks from different modules mentioned in Sect. 3. Section 5 drew the conclusion and prospects.

2 Background

Intelligent ships apply multiple techniques such as sensors, communications, and the internet of things. Specifically, seven techniques including information perception, communication and navigation, energy efficiency control, route plan, condition monitoring, and fault diagnosis, intelligent navigation are connected in the intelligent integration platform [5–10].

Ship intelligent navigation is to use perception, communication, network information, big data, and artificial intelligence techniques to represent the eyes, ears, brain, hands, and mouth of the pilot. According to the technological evolution of intelligent navigation, International Maritime Organization (IMO) divides the level of autonomy of intelligent ships into four levels, level 1 means seafarers are on board with automated processes and decision support, level 2 means seafarers are on board and ships can be remotely controlled, level 3 means ships can be remotely controlled but the seafarer is not on the ship, level 4 means fully autonomous ship. There are three kinds of typical scenarios for intelligent navigation, remote driving, automatic berthing, and unberthing, autonomous navigation. The technical framework of intelligent ship can be found in Ref [11].

The core of the ship is the intelligent navigation system, it automatically plans the route according to the navigation task firstly. Then situation awareness system is applied to detect the surrounding targets during the route execution. After the target is found, the collision avoidance decision module generates safe collision avoidance, meanwhile, this module continuously verifies the ship's state and evaluates the current control mode. Once the problem is found, and the intelligent navigation system cannot process it. The alarm information is uploaded promptly to the shore-based control center through the data link, the shore-based control center will take over the ship. During the entire process of the route execution, the shore-based control center can remotely monitor the ship's state and location, environment, and the ship through the data link, so that a single control center can monitor and control multiple intelligent ships.

3 Network Security Requirements

The network security issues of ship intelligent navigation contain two categories, one is to maintain the integrity and availability of information and systems to ensure business continuity and the continuous use of the system. The other is to prevent hackers from accessing systems and information, to avoid the loss of confidential information and control. Therefore, the analysis of ship intelligent navigation network security requirements is mainly carried out from two aspects. One is the system potential network threats generated by the system's design, and the other is the external malicious attack that the system may suffer.

3.1 System Potential Threats

In Sect. 2, the functional modules are presented in ship intelligent navigation, including route planning, situation awareness, collision avoidance decision, state definition, data link, and remote control.

Route Planning

(1) Tampering of the current location, mainly comes from the positioning system, such as Global Navigation Satellite System (GNSS) deception. (2) Invalidation of current position, mainly comes from the positioning system, such as GNSS interference. (3) Tampering of destination location, mainly comes from data tampering. (4) False risk information on the route ahead, for example, receiving false Navigational Telex (NAVTEX) navigation warning information, air guidance services, chart correction information, etc.

Situation Awareness

(1) Falsification of the electronic nautical chart, for example, if the modified map data is tampered with, such as the water depth value is maliciously increased, the underwater obstruction is maliciously deleted, etc. (2) False targets of Automatic Identification System (AIS), for example, adding a virtual aid to navigation in front of the route will cause the intelligent navigation system to be induced by false targets. (3) Tampering of the AIS data, which cause the ship to misroute, and bring risks to the subsequent route execution risk and action. (4) The false target of ship radar, false radar targets will

likely lead to errors in module, which in turn will bring risks to route execution and collision avoidance operations. (5) Tampering of anemometer data, which brings risks to the ship's maneuvering, especially the ship's entrance and exit ports, berthing, and departure ports. (6) Tampering of the log data, the tampered log data will cause serious accidents such as the ship colliding with the dock.

Collision Avoidance Decision

(1) Falsification of parameters such as collision risk assessment, which will lead to delays in avoiding collisions, wrong decisions, and serious consequences such as urgent situations, urgent dangers, and collision accidents. (2) Falsification of ship maneuverability assessment data, which will lead to misjudgment of the ship maneuverability.

State Definition

(1) Tampering of intelligent navigation state data, for example, the state definition module always believes that the ship is in a safe state and does not need to be taken over by remote control. (2) Tampering of Voyage Data Recorder (VDR) data, for example hiding traces of attacks, and affecting accident investigation.

Data Communication

(1) Functional failure: the route planning module, situation awareness module, collision avoidance decision module, and state definition module cannot obtain various information from sensors, and the modules cannot exchange data. (2) Data is collected viciously: the data transmitted between ship and shore, ship and ship was collected viciously, causing data leakage, and ship dynamic data such as ship location, voyage plan, ship states, and other information were stolen. (3) Data transmission is unavailable: ship-to-shore data transmission is unavailable, which means that the ship cannot report distress alarms and business data to the shore-based control center, and cannot obtain instructions from the shore-based control center, causing the intelligent ship to lose connection and control.

Remote Control

(1) Tampering of the remote monitoring command, which will cause the intelligent ship cannot execute the route according to the expected target, and the tampering of the key parameters of safe navigation will cause serious collisions, groundings, and other accidents. (2) The remote-control function denies service. The control commands issued by the remote-control system cannot be accurately received and executed by the ship-side intelligent navigation system. (3) An unauthorized third party obtains remote control authority. Third-party attackers obtained control of the ship through illegal attacks, resulting in the hijacking of the ship.

The above potential threats can be classified into 4 categories including damage, misdirect, obfuscate, and DoS. In the route planning module, tampering of the current location, tampering of a destination location, and false risk information on the route ahead belong to obfuscation and misdirect, invalidation of current position belongs to damage. In the situation awareness module, falsification of the electronic nautical chart, tampering of the AIS data, tampering of anemometer data, and tampering of the log data belong to obfuscation and misdirect, false targets of AIS and false target of ship radar belong to obfuscation. In collision avoidance decisions, falsification of parameters such as collision risk assessment and falsification of ship maneuverability assessment data belong to misdirect. In state definition, tampering of intelligent navigation state data and tampering of VDR data belong to obfuscation and misdirect. In the data communication system, functional failure belongs to damage, data is collected viciously and data transmission is unavailable belong to damage and DoS. In the remote control system, tampering of the remote monitoring command belongs to obfuscation and misdirect, the remote-control function denies service belongs to DoS, an unauthorized third party obtains remote control authority belongs to misdirect.

3.2 External Malicious Attack

Section 3.1 analyzes the potential threats of the system from the perspective of the system's structure and business design. This section analyzes the network security requirements from the perspective of external physical attacks that the system may suffer. The attack motives of different attackers were explored, including attack cost and attack reward, to determine the security requirements of the ship intelligent navigation.

Attack Cost

Attack cost means the cost that the attacker must pay when the system is attacked. When determining the cost of an attack, personnel and environmental factors play an important role. For example, the experience and awareness of personnel can prevent or allow cyber-attacks to occur. In addition, the ship's configuration (such as firewalls) and physical location may also determine the likelihood of an attack. For example, In the areas with frequent pirates will mean an attack advantage at these coordinates. If data theft is the target of an attacker, certain ports and networks with weak anti-virus capabilities will increase the risk of being attacked. This paper applies a five-layer structure based on traditional computing systems to indicate the level of "hacking ability" and the available resources required for utilization, more details can be found in Ref [12].

Attack Reward

In addition to the attack cost, attack rewards are also a factor when executing an attack. To fully understand the psychological factors of cyber attackers, it is necessary to deeply analyze the types of hackers and their motivations. BIMCO divides the cyber attackers in the existing standard security environment into 5 categories including activists, competitors, criminals, terrorists, elitists.

Activists are also called "hacktivists", the ideal goal of radical groups is to achieve ideological influence. Their attack actions contain disrupt activities, disclose information to change the targeted behavior. Although these actions are not offensive, their activities may create opportunities to benefit other attackers or cause accidental damage or leakage. Competitors mean competing companies, and even opposing countries, who may apply cybercrime to increase their market influence in the global economy. In most non-extreme situations, the expected goal is to obtain information. In addition, it is also an incentive to interfere with competitors' ship operations to damage their financial status or reputation. Criminals can range from individuals to groups of different sizes and levels of complexity. Most criminals hope to profit from material theft, fraud, smuggling, and extortion. Simple cyber-attacks can obtain the direct economic benefit, meanwhile, it is organized to sell network tools to all types of attackers to obtain indirect economic benefits. Terrorists' attack purposes are always to seek casualties and property damage. In a more sophisticated attack, the ship may become an asset for a long-range cyber-attack. Elitism always invades the system to test or show off their abilities, such attacks rarely show negative results and are not considered in this paper.

4 Network Security Risk Analysis

4.1 Risk Analysis Model

Section 3.1 analyzed the potential threats and external attacks from different modules in ship intelligent navigation. This section tries to build the risk analysis model for identified threats and attacks. A two-dimensional quadrant risk analysis framework was applied to quantify the threats and attacks. Tam [12] investigated a model-based method to provide a comprehensive analysis of maritime cyber-risks and the risks can be displayed in 2D and 3D projections separately, the case studies were carried based on the physical structure includes the GNSS, electronic chart display and information system, automatic identification system, etc. For example, misdirection and damage are risks from GNSS. Compared with that, this paper adopted the method proposed by Tam to analyze the risks from different functional scenarios, new ideas are listed as follows: (1) network security risks were analyzed when the ship is navigating from the technical/situational perspective. (2) system potential threats were discussed from the route planning, situation awareness and other functional scenarios. For example, GNSS deception and receiving false NAVTEX navigation warning information both belong to the risks from route planning functional scenario. (3) this research is oriented by the intelligent navigation functional scenarios, which can complement the research conducted by Tam, and finally provide advice on the safety of the ship's intelligent navigation network.

$\boldsymbol{axis_s}$, $\boldsymbol{axis_e}$, and $\boldsymbol{axis_r}$ represent the potential threats, attack cost, and attack reward. Two variables $\boldsymbol{Attacker_a}$ and $\boldsymbol{Target_t}$ are considered to model an attack. The attributes of these two variables are shown in Eqs. (1) and (2).

$$\boldsymbol{Attacker_a} = (a_{vector}, a_{goal}, a_{type}, a_{resources}) \tag{1}$$

$$\boldsymbol{Target_t} = (t_{vulnerabilities}, t_{effects}, t_{type}, t_{resources}) \tag{2}$$

For $\boldsymbol{Attacker_a}$, there are 4 variables. a_{vector} means the attack object such as vulnerable web application, a_{goal} means attackers' expected results such as stolen information and physical collision. a_{type} means the type of attackers. $a_{resources}$ means the ways for attackers to acquire skills, time, money, and members. For$\boldsymbol{Target_t}$, there are 4 variables too. $t_{vulnerabilities}$ means the system vulnerabilities such as outdated operation system or firewall. $t_{effects}$ indicates the possible impact such as loss of navigation after exploiting the vulnerability. t_{type} means the object type such as ferry. $t_{resources}$ represents experienced crew, anti-virus, and other factors that can stop or catch attackers. These 8 variables are not independent of each other. Attackers will decide the a_{vector} according to the$t_{vulnerabilities}$. Combination of a_{goal} and $t_{effects}$ can determine whether an attack succeeds. Four variables such as a_{type}, $a_{resources}$ and t_{type}, $t_{resources}$ should be considered simultaneously, then an attack can be evaluated accurately. Two-dimensional quadrant risk analysis is to model the function between the $\boldsymbol{Attacker_a}$, $\boldsymbol{Target_t}$ and $\boldsymbol{axis_s}$, $\boldsymbol{axis_e}$, $\boldsymbol{axis_r}$, which is shown in Eqs. (3) and (4).

$$axis_s = f_{vulnerability}(a_{vector}, t_{vulnerabilities}, t_{effects}) \tag{3}$$

$$axis_e = f_{ease}(a_{type}, t_{type}, a_{resources}, t_{resources}) \tag{4}$$

$$axis_r = f_{reward}(a_{type}, t_{type}, a_{goal}, t_{effects}) \tag{5}$$

Based on Eqs. (3), (4), and (5), an action with attacker and target can be quantified from three aspects $\boldsymbol{axis_s}$, $\boldsymbol{axis_e}$, $\boldsymbol{axis_r}$ also means vulnerability $f_{vulnerability}$, ease f_{ease}, and rewards f_{reward}. The projection formula is shown in Eq. (6)

$$\begin{aligned} F_{action}(attacker, target) &= \mathrm{I}(axis_s, axis_e, axis_r) \\ &= \mathrm{I}(f_v(a,t), f_e(a,t), f_r(a,t)) \end{aligned} \tag{6}$$

Each vulnerability in different modules in ship intelligent navigation can be modeled by ease and rewards as shown in Fig. 1.

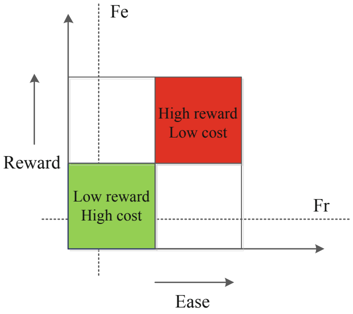


Fig. 1. 2-D mapping of risk quadrant for ship intelligent navigation.

In Fig. 1, each risk can be projected to a 2D risk quadrant, evaluators compare the risks of various systems numerically, and they can also consider a series of factors such as attacker types, goals, and effects. The risk also can be assessed by the distance between the data point and the origin. Figure 2 characterized the risk by quadrant to which the vulnerability is mapped. Vulnerabilities in the first quadrant have a high risk because the attackers can get rich rewards for the lower cost. Vulnerabilities in the third quadrant have a low risk because the attacker has the higher cost but the lower reward. If the analysts only own limited resources to mitigate the threat, then filters Fe and Fr can be introduced to filter out the risks that have low rewards but a high-cost investment. In this way, security efforts can be focused on the most likely network security risks.

4.2 Network Attack Analysis Based on Risk Analysis Model

Based on the risk analysis model constructed in Sect. 4.1, when all variables in $\boldsymbol{Attacker_a}$, $\boldsymbol{Target_t}$ are fully considered, the two-dimensional quadrant risk model will become too complicated for effective and comprehensive evaluation. Therefore, this paper specifies 2 $\boldsymbol{Target_t}$ variables and 4 $\boldsymbol{Attacker_a}$ variables. In Sect. 3.1, four potential threats are concluded from different modules in ship intelligent navigation include damage, misdirect, obfuscate, and DoS. Experts from ship intelligent navigation score the potential risks for attackers contain activists, competitors, criminals, and terrorists, and different modules, all the data is shown in Table 1.

Table 1. Scores of potential risks for different attackers and modules.

Module	Risk	H_r	H_e	Co_r	Co_e	Cr_r	Cr_e	T_r	T_e
Route planning	Damage	2	4	3	3	4	2	4	2
	Misdirect	2	3	3	3	5	3	5	3
	Obfuscate	1	4	3	3	4	3	4	2
Situation awareness	Misdirect	2	3	3	2	4	2	4	2
	Obfuscate	2	4	3	3	3	3	3	3
Collision avoidance decision	Misdirect	3	3	4	2	5	3	5	2
State definition	Misdirect	2	3	4	2	4	2	4	3
	Obfuscate	1	4	3	3	3	3	3	3
Data communication	DoS	2	3	3	4	4	2	3	4
	Damage	3	3	3	3	4	2	4	3
Remote control	DoS	2	3	3	3	4	2	4	2
	Misdirect	3	2	4	2	5	1	5	1
	Obfuscate	2	2	3	3	5	2	5	1

According to Table 1, different projection views can be calculated to visualize the cyber risk of ship intelligent navigation. Evaluation based on the two-dimensional quadrant risk analysis method is not for a risk assessment of a single module, but a summary of the risks associated with each consequence to determine the most likely outcome of a cyber-attack. Figure 2 shows the risk analysis results of the ship intelligent navigation based on the two-dimensional quadrant risk analysis method.

Figure 2 shows the risk identification for different attackers. For all attackers, the DoS and damage belong to the low-reward and high-cost area, which is low risk. For activists, misdirect is in the high-reward and low-cost area, which is high-risk, obfuscate is in the high-reward and high-cost area, which is a great reward for the attacker, but it requires more cost. For competitors, misdirect and obfuscate have the same reward, but the cost of misdirect is lower. For criminals, the rewards for misdirect and obfuscate are roughly the same, but the cost of obfuscate is lower. For terrorists, misdirect can take advantage of

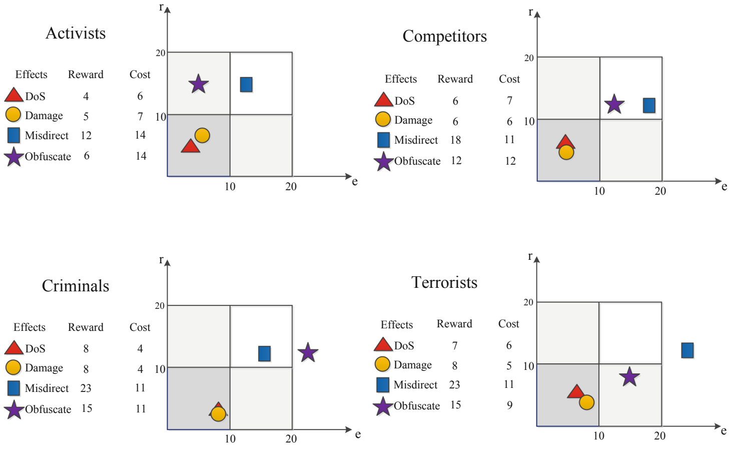


Fig. 2. Summary of risks focused on effects.

lower costs to obtain higher rewards, while obfuscate requires additional cost investment, and there is no way to obtain the same return as the misdirect. In summary, for the four types of attackers, the misdirect and the obfuscate are both high-risk threats.

5 Conclusion

Compared with conventional network security analysis methods, this paper focused on the unique risks that arise in the process of traditional ship navigation networks and intelligence. First, we comprehensively analyzed the current research status of ship intelligent navigation network security, including intelligent ship technology and various typical intelligent ship solutions, intelligent navigation technology, and its typical functional modules. Then we analyzed the security requirements of the ship intelligent navigation network for each typical functional module, designed a two-dimensional quadrant risk analysis method to quantitatively analyze the network attack and risk of the ship intelligent navigation system, including risk analysis model construction and network attack analysis. Finally, the high-risk threats of ship intelligent navigation networks were determined and concluded, which can provide the theoretical guidance for actual on-site operations.

However, there are few limitations, only two variables are applied in the two-dimensional quadrant risk analysis method, 2 target variables, and 4 attacker variables. So, the risk cannot be fully depicted. In the future, all variables in target and attacker should be considered or selected according to scenarios.

Acknowledgment. The paper is financially supported by National Key R&D Program of China (2018YFB1601500, 2018YFB1601504).

References

1. Li, Y.: Research status and development trend of intelligent ships. Int. Core J. Eng. **5**(11), 49–57 (2019)
2. Yang, T.: Intelligent ships. In: Mukherjee, P.K., Mejia, M.Q., Xu, J. (eds.) Maritime Law in Motion. WSMA, vol. 8, pp. 703–711. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-31749-2_34
3. Guanghang, W., Fenghao, S., Xianbo, X.: Unmanned boat design for challenges and verification of unmanned surface ship intelligent navigation. In: IEEE 8th International Conference on Underwater System Technology: Theory and Applications (USYS), pp. 1–5. IEEE, Wuhan (2018)
4. CNSS Homepage. https://www.cnss.com.cn/html/sdbd/20191012/331834.html. Accessed 02 Dec 2021
5. RØ, J.: The MUNIN project: assessing the feasibility of unmanned ships. Naval Archit. (JAN.SUPPL.), 45–47 (2016)
6. Acanfora, M., Luca, F.D.: An experimental investigation on the dynamic response of a damaged ship with a realistic arrangement of the flooded compartment. Appl. Ocean Res. **69**, 191–204 (2017)
7. VesselFinder Homepage. https://www.vesselfinder.com/vessels/SVITZER-HERMOD-IMO-9788124-MMSI-219022265. Accessed 02 Dec 2021
8. FinFerries Homepage. https://www.finferries.fi/en/news/press-releases/finferries-falco-worlds-first-fully-autonomous-ferry.html. Accessed 02 Dec 2021
9. KONGSBERG Homepage. https://www.kongsberg.com/maritime/about-us/news-and-media/news-archive/2020/first-adaptive-transit-on-bastofosen-vi/. Accessed 02 Dec 2021
10. Anderson, M.: Bon voyage for the autonomous ship mayflower. IEEE Spectr. **57**(1), 36–39 (2020)
11. Rolls-Royce Homepage. https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/%20customers/marine/ship-intel/rr-ship-intel-aawa-8pg.pdf. Accessed 02 Dec 2021
12. Tam, K., Jones, K.: MaCRA: a model-based framework for maritime cyber-risk assessment. WMU J. Marit. Aff. **18**(1), 129–163 (2019). https://doi.org/10.1007/s13437-019-00162-2

A Security Reinforcement Model for Edge Computing Facilities in 5G Power Network

Nige Li[1,2](✉), Peng Zhou[3], Zhipeng Shao[1,2], and Xiaoxiao Chen[3]

[1] Power Grid Digitizing Technology Department, State Grid Smart Grid
Research Institute Co., Ltd., Jiangsu 210003 Nanjing, China
48548962@qq.com

[2] State Grid Key Laboratory of Information and Network Security, Nanjing 210003, China

[3] State Grid Zhejiang Electric Power Corporation Information and Telecommunication Branch,
Hangzhou, China

Abstract. 5G network has attracted much attention from the vertical industry since its commercial use. Compared with previous generations of mobile communication technologies, 5G bandwidth, delay and other communication KPI indicators have been greatly improved. 5G network has three typical application scenarios of large bandwidth, low delay and wide connection. In the power grid scenario, it can meet the needs of various power grid business access. As the key technology to realize 5G, multi-access edge computing (MEC) plays an important role in high-speed and low delay wireless data transmission network and has made indelible contributions to improving end-to-end service quality. In view of today's increasingly complex network security environment and changing attack means, security attacks against MEC systems and applications have become endless. In order to deal with large-scale and various attacks, this paper studies the micro application security reinforcement and independent application security reinforcement technology deployed in edge computing facilities in the environment of 5G power network, proposes the security reinforcement model of MEC, and strengthens the source code of edge computing facilities based on the so file confusion technology of OLLVM, so as to ensure the safe and stable operation of MEC.

Keywords: Mobile edge computing · Micro application security reinforcement · Independent application security reinforcement

1 Introduction

The new generation of communication technology promotes the change of network architecture. As an extension of cloud computing, multi-access edge computing (MEC) has become the key technology to realize 5G communication network with its strong network management ability, high bandwidth data transmission ability and low delay business response ability in order to realize the efficient processing of massive data generated by a large number of devices [1].

However, edge computing nodes carry vertical industry applications, they are heterogeneous, and the network scale is relatively small compared with the core cloud,

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 51–59, 2022.
https://doi.org/10.1007/978-981-19-3486-5_6

once the attacker successfully controls the edge node, the application of the whole edge node will be affected. In addition, the edge computing node is close to the user, and the introduction of third-party app will increase the exposure surface, and edge computing will introduce new security risks [2]. Specifically, the security risks faced by edge computing include infrastructure security, network security, data security and application security. Infrastructure security risk: due to the distributed deployment of edge computing nodes, dependence on remote operation and maintenance, and untimely upgrade and patch repair, attackers will exploit vulnerabilities; Network security risk [3]: due to the large number of access devices, it is easier to implement DDoS attacks, and the newly introduced MEP and edge computing orchestration system have become important attack objects of attackers; Data security risk: due to the limited resources of the edge computing node and the lack of effective data backup, recovery and audit measures, the attacker may modify or delete the user's data on the edge node to destroy some evidence; Application security risk: because edge devices may contain multiple apps, there is a security threat of illegal access between apps. Therefore, the introduction of edge computing brings more challenges to the security protection and security operation management of edge computing.

Edge computing deployment modes such as 5G network edge computing technology and multi station integrated data center station not only provide business convenience, but also produce new security risks due to their deployment location and application characteristics [4]. Firstly, the edge computing node sinks the computing power of the cloud data center to the network edge. Compared with the security environment of the core network, the security capacity of the network edge is limited. The edge computing node is easy to be exposed to the untrusted physical environment [5], and is more likely to be attacked; Secondly, 5G network edge computing nodes will adopt technologies such as open application programming interface, open network function virtualization and deployment of third-party applications. The introduction of openness is easy to expose 5G network edge computing nodes to external attackers; Thirdly, the edge computing node can deploy multiple applications, and the isolation mechanism between applications is easy to break through. Due to the sharing of relevant resources between applications, once the protection of an application is weak, it will affect the safe operation of other applications on the edge computing platform. In order to deal with the above security risks, the edge computing node of 5G power network needs to make use of the existing cloud and virtualization security technologies, and strengthen the third-party authentication and authorization management and user data protection to build the edge computing security of 5G power network [6].

Me app is an important part of edge computing services. The me app can obtain information from the MEC platform and provide external services through the MEC platform. On the one hand, me app may provide illegal services through MEC platform, or maliciously consume MEC platform resources. On the other hand, me app may be attacked, resulting in data leakage or life cycle management destruction. The security threats of me app are as follows: malicious third-party app can access the network to provide illegal services; Attackers can illegally access me app, resulting in the disclosure of sensitive data of the application; There is a risk of illegal creation, deletion and update in the life cycle management of me app; The me app has the risk of maliciously consuming the resources of the MEC system, resulting in the unavailability of other services of the MEC system; The overload traffic generated by me app after being attacked will cause DoS attack on MEC system.

2 Application of Security Reinforcement Technology in Edge Computing Facilities in 5G Power Network

2.1 Security Reinforcement Technology of Micro Application JS Code Based on Source Code Confusion

With the large-scale popularization of 5G technology, its large bandwidth and low delay characteristics will bring great changes to the operation mode and R & D ecology of the mobile application industry. Traditional mobile applications store code executable files, a large number of library files and resource files on the user client. Such schemes pose a great challenge to the hard disk space of the user's mobile terminal and the research and development of application multi platform. The cross platform H5 micro application based on JavaScript as the development language stores the application executable source code and a large number of resource files on the server for users to download and call, which greatly reduces the application R & D cost, significantly shortens the adaptation cycle of different operating systems and terminal manufacturers, and makes full use of 5G ultra-high-speed bandwidth to meet users' smooth application experience.

However, compared with traditional mobile applications, micro applications are always facing security threats closer to web penetration attacks. An attacker can obtain the JS application source code downloaded from the server through technical means, analyze the vulnerabilities based on the interpretation of the original logic of the code, and attack the micro application through SQL injection, XSS, js-hook, browser malicious debugging and other means. Therefore, it is necessary for this paper to carry out the following research on the safety reinforcement technology of micro application.

Step 1: Study the confusion technology of structural complexity of JS source code. At present, the complexity of source code structure can be improved mainly through two aspects of research. In terms of source code transformation technology based on control flow flattening, control flow flattening essentially deforms the control flow of program source code, transforms the relationship between basic blocks into a flattened structure, and drowns the code logic in a large number of code blocks by transforming the if else logic relationship into a large number of while switch types, Increase the complexity of JS source code; In the aspect of JS based waste code injection technology, a large number of meaningless false control flow instructions are inserted into the JS source code, which significantly expands the reference of the JS source code and greatly reduces the readability of the code.

Step 2: Study a diversified protection mechanism based on JS source string. JS code string is often used to record key, IP, random number seed and other application sensitive information. By taking protective measures for JS code string, it can effectively prevent attackers from stealing application key information from the source code by static scanning. Firstly, by studying the fission protection function of JS string, the string in

JS code is disassembled into several fragments and stored in multiple array blocks of JS. When the application logic is executed to the calling string part, the string will be restored through the corresponding code block; Secondly, in the research of JS string array protection mechanism based on matrix transformation, the selected string is transformed into string matrix through the selection of a certain probability, and the elements of string matrix are displaced or disrupted and reorganized through correlation matrix operation, so as to hide the original appearance of character string.

Step 3: Study a protection scheme for global variables and function names of JS source code. By obtaining the function name and global variable name of JS source code, a one-to-one mapping relationship between function name, global variable and random hexadecimal character is established, and the mapping relationship is hidden in the confused code. Finally, the attacker cannot infer the source code logic by analyzing the function name and global variable name.

2.2 5G Independent Application Safety Reinforcement Technology

With the large-scale commercialization of 5G technology and the continuous sales and promotion of 5G terminals in the market, how to maximize the security protection ability of mobile applications on the basis of ensuring the excellent user experience of 5G applications has become a major topic of mobile application security protection in the future 5G era. For Android applications, although the traditional methods of DEX shelling and function extraction can meet the reinforcement needs of mobile applications in the past to a certain extent, with the continuous development of mobile application reverse technology, some free reverse and shelling tools with high automation and low threshold gradually appear on the market, The cost of cracking a generally reinforced Android application is almost zero. Moreover, the inherent performance loss disadvantage of traditional reinforcement schemes will be further amplified in 5G application scenarios. Therefore, it is particularly important to study a lightweight and high-strength Android mobile application security scheme suitable for 5G scenarios.

Step 1: Research on Android application security reinforcement technology based on Virtualization instruction protection. The core of this research is realized by software technology based on Virtualization protection. Virtualization protection technology uses a new bytecode instruction “language” to translate the original code. This “language” can only be understood by a custom virtual machine engine. Without any reference materials, it is extremely difficult for crackers to fully master this “language” in a limited time. By converting the Java function to be protected into a native function, and converting the bytecode of the Java function to be protected into a new bytecode format, we can achieve the effect of deep Protection of Java source code. Further, the Android reinforcement engine can build multiple different virtualization interpretation engines at the same time. Different methods use different virtualization execution engines to further improve security in this way.

Step 2: Research on Android source code reinforcement technology based on local layer transformation. At present, most of the mainstream Android applications on the market are developed by the Java language. DEX file is the executable file of Android system, which contains all operation instructions and runtime data of the application. The

Android java source code is transformed into bytecode after compilation and encapsulated into DEX executable files for interpretation and execution by Dalvik virtual machine. Due to the inherent characteristics of bytecode, the DEX executable of Android is very easy to decompile and get all the source code. However, after the native local layer code represented by C/C++ is compiled into so library file, it is extremely difficult to decompile. Therefore, the local layer conversion technology can be used to convert the Java code in the DEX file into C or C++ code and compile it into so library for execution, So as to effectively improve the decompilation difficulty of Android application package (APK) and achieve the purpose of protecting DEX. Moreover, the Android source code is strengthened by local layer transformation, which is much better than the Virtualization Management Platform (VMP) reinforcement scheme in performance, and is more suitable for scenarios with more stringent requirements for bottom delay in 5G scenarios.

Step 3: Deeply study the self-security detection technology of Android applications with multiple policy integration. Even after reinforcement, Android applications may face multiple attack threats from attackers, such as professional shelling attacks using xposed, Frida and even customized ROM, and black box malicious debugging attacks directly on applications without shelling. If the application needs to resist these potential attack threats at its own level, multiple security detection capabilities can be implanted through the security reinforcement link. First, the reinforcement application itself should have the ability to prevent malicious debugging, including preventing process attachment and memory dump of malicious debugging tools such as Java debugger(JDB) and Frida; Second, the reinforcement application itself should have perfect terminal environmental security detection capability, and the environmental detection strategy should cover but not limited to terminal root detection, simulator detection, WiFi agent detection, etc. Third, the reinforcement application should realize the encrypted storage of local sensitive data files based on private high-strength encryption algorithm, and realize the application's own anti tamper detection based on file summary verification means.

3 Security Reinforcement Model for Edge Computing Facilities

3.1 Security Architecture Design of Edge Computing Facilities

In 5G power network, by studying the micro application security reinforcement technology and independent application security reinforcement technology of the above edge computing facilities, this paper establishes a security reinforcement model for edge computing facilities to ensure the safe and stable operation of MEC. The security architecture design of edge computing facilities is shown in Fig. 1.

According to the layers in the edge computing facilities, the security reinforcement requirements of each layer are analyzed, and the security reinforcement model of edge computing facilities is designed. In the service security layer, the functions of storage and encryption of local data, logs and sensitive information are used to solve the problem of local storage security of terminal private key; In the source security layer, through the security shell of ELF files, code confusion and other technologies, the business logic is protected from exposure, and the application package is not implanted with malicious code, advertisements and viruses; In the environment security layer, continue to use

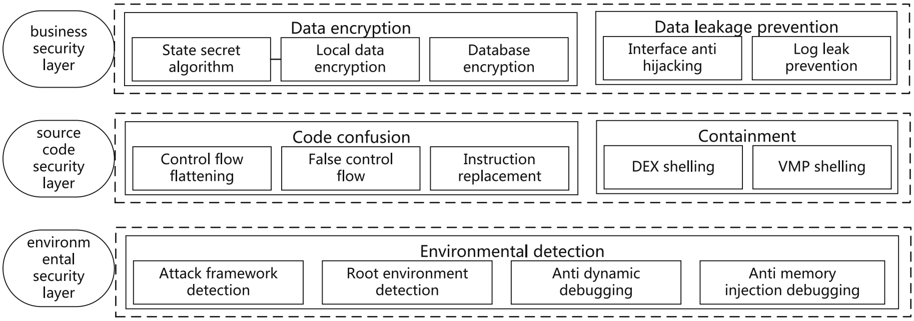


Fig. 1. Security achitecture design of EGE computing facilities

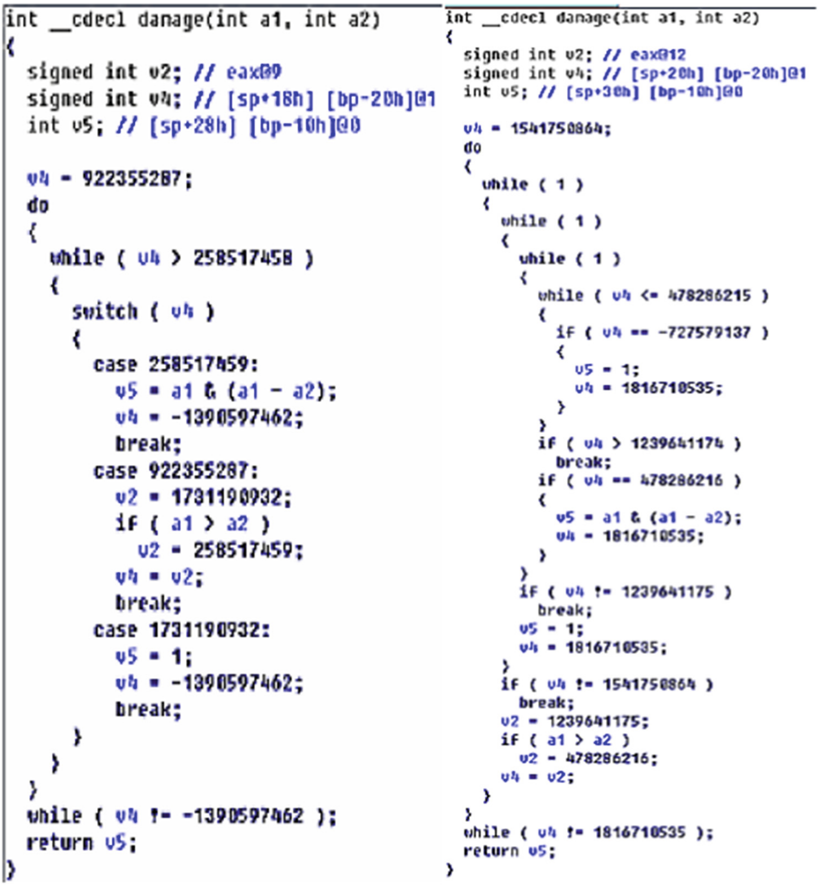
the application detection and monitoring technology for the environment, and timely find the unsafe root permission of the terminal, application attack framework process, application dynamic debugging, etc. This paper focuses on the security reinforcement of source code security layer.

3.2 Research and Effect of so File Confusion in OLLVM

Next, according to the characteristics of edge computing facilities, we use the so file obfuscation technology of OLLVM to carry out security research on the source layer. Control flow flattening, false control flow and instruction replacement are common code protection methods used in OLLVM. Firstly, this paper studies and practices the control flow flattening function:

Step 1: Judge whether it can be flattened. If you can, jump into flatten method to execute. At the beginning of the function, use lowerswitchpass to remove the switch and replace the switch structure with an if structure. Save all basic code blocks. If there is only one basic code block, it will not be processed; If the end of the first basic block is a conditional jump instruction, it needs to be split and saved to origbb;
Step 2: Create two basic blocks to store the instructions of the loop head and tail. Then move the first BB to the front of the loopentry, and create a jump instruction to jump from the first BB to the loopentry. Then an instruction to jump from loopend to loopentry is created. Finally, the switch instruction and switch default block are created, and the corresponding jump is created.
Step 3: Delete the jump instruction of first BB, instead jump to loopentry, add all basic blocks to the switch structure, and calculate the switch variable according to the original jump.

In the control flow flattening mode, add the source code of so file in the edge computing facility to the parameter - OLLVM Fla. the effect is shown in Fig. 2 (left). It can be seen that the program logic is disrupted and many branches appear, but fla will only deal with the functions with branches. After the modification, the switch feature can be removed by inserting more garbage code in the switch branch and garbage code in the backbone function, as shown in Fig. 2.

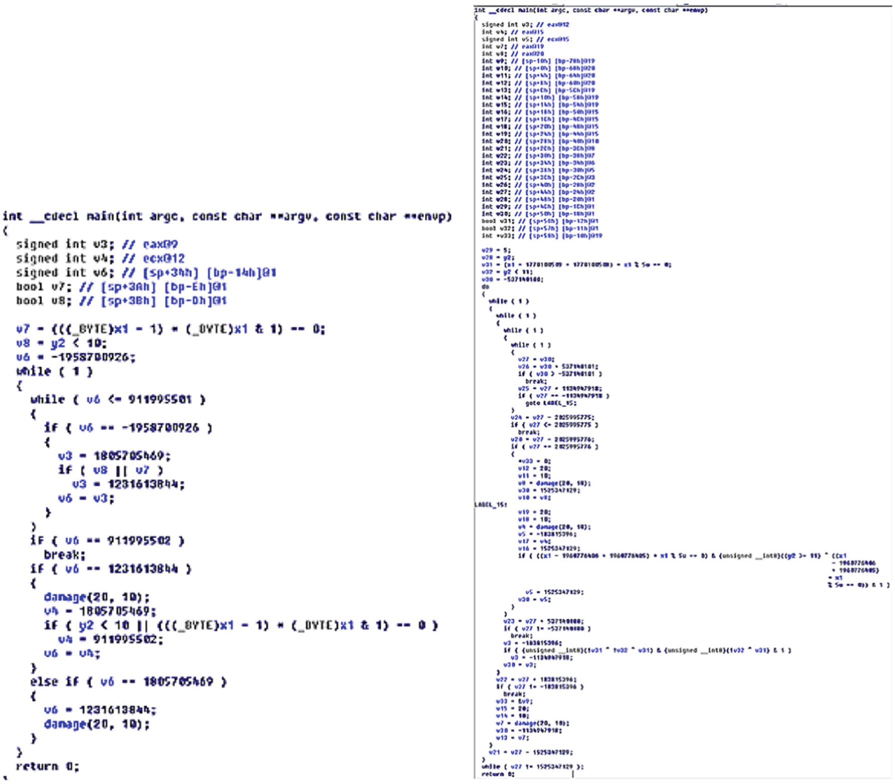


```
int __cdecl danage(int a1, int a2)
{
  signed int v2; // eax@9
  signed int v4; // [sp+18h] [bp-20h]@1
  int v5; // [sp+28h] [bp-10h]@0

  v4 = 922355287;
  do
  {
    while ( v4 > 258517458 )
    {
      switch ( v4 )
      {
        case 258517459:
          v5 = a1 & (a1 - a2);
          v4 = -1390597462;
          break;
        case 922355287:
          v2 = 1731190932;
          if ( a1 > a2 )
            v2 = 258517459;
          v4 = v2;
          break;
        case 1731190932:
          v5 = 1;
          v4 = -1390597462;
          break;
      }
    }
  }
  while ( v4 != -1390597462 );
  return v5;
}
```

```
int __cdecl danage(int a1, int a2)
{
  signed int v2; // eax@12
  signed int v4; // [sp+20h] [bp-20h]@1
  int v5; // [sp+30h] [bp-10h]@0

  v4 = 1541750864;
  do
  {
    while ( 1 )
    {
      while ( 1 )
      {
        while ( 1 )
        {
          while ( v4 <= 478286215 )
          {
            if ( v4 == -727579137 )
            {
              v5 = 1;
              v4 = 1816710535;
            }
          }
          if ( v4 > 1239641174 )
            break;
          if ( v4 == 478286216 )
          {
            v5 = a1 & (a1 - a2);
            v4 = 1816710535;
          }
        }
        if ( v4 != 1239641175 )
          break;
        v5 = 1;
        v4 = 1816710535;
      }
      if ( v4 != 1541750864 )
        break;
      v2 = 1239641175;
      if ( a1 > a2 )
        v2 = 478286216;
      v4 = v2;
    }
  }
  while ( v4 != 1816710535 );
  return v5;
}
```

Fig. 2. Before inserting garbage code after inserting garbage code

Next, combined with control flow flattening, false control flow and instruction replacement to realize code confusion, the security of the source code of edge computing facilities is strengthened. The one-time processing effect is shown on the left of Fig. 3, and the customized confusion code after modification is shown on the right of Fig. 3.



```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  signed int v3; // eax@9
  signed int v4; // ecx@12
  signed int v6; // [sp+3Ch] [bp-14h]@1
  bool v7; // [sp+3Ah] [bp-Eh]@1
  bool v8; // [sp+3Bh] [bp-Dh]@1

  v7 = (((_BYTE)x1 - 1) * (_BYTE)x1 & 1) == 0;
  v8 = y2 < 10;
  v6 = -1958700926;
  while ( 1 )
  {
    while ( v6 <= 911995501 )
    {
      if ( v6 == -1958700926 )
      {
        v3 = 1805705469;
        if ( v8 || v7 )
          v3 = 1231613844;
        v6 = v3;
      }
    }
    if ( v6 == 911995502 )
      break;
    if ( v6 == 1231613844 )
    {
      damage(20, 10);
      v4 = 1805705469;
      if ( y2 < 10 || (((_BYTE)x1 - 1) * (_BYTE)x1 & 1) == 0 )
        v4 = 911995502;
      v6 = v4;
    }
    else if ( v6 == 1805705469 )
    {
      v6 = 1231613844;
      damage(20, 10);
    }
  }
  return 0;
}
```

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  signed int v3; // eax@12
  int v4; // eax@15
  signed int v5; // ecx@15
  int v7; // eax@19
  int v8; // eax@20
  int v9; // [sp-10h] [bp-78h]@19
  int v10; // [sp+0h] [bp-68h]@20
  int v11; // [sp+4h] [bp-64h]@20
  int v12; // [sp+8h] [bp-60h]@20
  int v13; // [sp+Ch] [bp-5Ch]@19
  int v14; // [sp+10h] [bp-58h]@19
  int v15; // [sp+14h] [bp-54h]@19
  int v16; // [sp+18h] [bp-50h]@15
  int v17; // [sp+1Ch] [bp-4Ch]@15
  int v18; // [sp+20h] [bp-48h]@15
  int v19; // [sp+24h] [bp-44h]@15
  int v20; // [sp+28h] [bp-40h]@10
  int v21; // [sp+2Ch] [bp-3Ch]@8
  int v22; // [sp+30h] [bp-38h]@7
  int v23; // [sp+34h] [bp-34h]@6
  int v24; // [sp+38h] [bp-30h]@5
  int v25; // [sp+3Ch] [bp-2Ch]@3
  int v26; // [sp+40h] [bp-28h]@2
  int v27; // [sp+44h] [bp-24h]@2
  int v28; // [sp+48h] [bp-20h]@1
  int v29; // [sp+4Ch] [bp-1Ch]@1
  int v30; // [sp+50h] [bp-18h]@1
  bool v31; // [sp+56h] [bp-12h]@1
  bool v32; // [sp+57h] [bp-11h]@1
  int *v33; // [sp+58h] [bp-10h]@19

  v29 = 5;
  v28 = y2;
  v31 = (x1 - 1770100509 + 1770100508) * x1 % 2u == 0;
  v32 = y2 < 11;
  v30 = -537140100;
  do
  {
    while ( 1 )
    {
      while ( 1 )
      {
        while ( 1 )
        {
          while ( 1 )
          {
            v27 = v30;
            v26 = v30 + 537140101;
            if ( v30 > -537140101 )
              break;
            v25 = v27 + 1134947918;
            if ( v27 == -1134947918 )
              goto LABEL_15;
          }
          v24 = v27 - 2025995775;
          if ( v27 <= 2025995775 )
            break;
          v20 = v27 - 2025995776;
          if ( v27 == 2025995776 )
          {
            *v33 = 0;
            v12 = 20;
            v11 = 10;
            v8 = damage(20, 10);
            v30 = 1525347129;
            v10 = v8;
LABEL_15:
            v19 = 20;
            v18 = 10;
            v4 = damage(20, 10);
            v5 = -183815396;
            v17 = v4;
            v16 = 1525347129;
            if ( ((x1 - 1960776406 + 1960776405) * x1 % 2u == 0) & (unsigned __int8)((y2 >= 11) ^ ((x1
                                                                                                  - 1960776406
                                                                                                  + 1960776405)
                                                                                                 * x1
                                                                                                 % 2u == 0)) & 1 )
              v5 = 1525347129;
            v30 = v5;
          }
        }
        v23 = v27 + 537140100;
        if ( v27 != -537140100 )
          break;
        v3 = -183815396;
        if ( (unsigned __int8)(!v31 ^ !v32 ^ v31) & (unsigned __int8)(!v32 ^ v31) & 1 )
          v3 = -1134947918;
        v30 = v3;
      }
      v22 = v27 + 183815396;
      if ( v27 != -183815396 )
        break;
      v33 = &v9;
      v15 = 20;
      v14 = 10;
      v7 = damage(20, 10);
      v30 = -1134947918;
      v13 = v7;
    }
    v21 = v27 - 1525347129;
  }
  while ( v27 != 1525347129 );
  return 0;
```

Fig. 3. Combined use of confusion Custom obfuscation modified obfuscation

4 Conclusions

In order to realize flexible security protection mechanism under the condition of rapid change and continuous security threat, this paper studies the application of security reinforcement technology of 5G grid edge computing facilities, analyzes their security reinforcement requirements from the business security layer, source code security layer and environmental security layer, and designs the security reinforcement model of edge computing facilities. Focusing on the source code security layer, this paper studies and practices the control flow flattening function based on the so file obfuscation technology of OLLVM. Finally, combined with the control flow flattening, false control flow and instruction replacement, this paper realizes code obfuscation, and strengthens the source code of edge computing facilities, so as to ensure the source code security of edge computing facilities.

Acknowledgments. This work is supported by the science and technology project of State Grid Corporation of China: "Research on Multi-access Edge Computing (MEC) Security Technology Adaptive to 5G Power Network" (Grand No. 5700-202119443A-0-0-00).

References

1. Vorobiev, A., Bekmamedova, N.: An ontology-driven approach applied to information security. J. Res. Pract. Inf. Technol. **42**(1), 61 (2010)
2. Liu, H., Xie, Y., Wang, G., Jiang, S.: Information security analysis based on cross domain ontology. Inf. Netw. Secur. **20**(09), 82–86 (2020)
3. Gao, J., Zhang, B., Chen, X.: Research progress of security ontology. Comput. Sci. **39**(08), 14–19 + 41(2012)
4. Zhu, L.: Application of ontology in network security situational awareness. Digit. Technol. Appl. **36**(05), 188–189 (2018)
5. Zhang, X., Xu, J., Gu, C.: Ontology based information security vulnerability association analysis. J. East China Univ. Technol. (Nat. Sci. Edn.) **40**(01), 125–131 (2014)
6. Parkin, S.E., van Moorsel, A., Coles, R.: An information security ontology incorporating human-behavioural implications. In: Proceedings of the 2nd International Conference on Security of Information and Networks, pp. 46–55 (2009)

Research on Multi-dimensional Sensitivity Economic Evaluation Method of Digital Technology in Power Grid Enterprises

Liang Zhu[1,2](✉), Aidi Dong[3], and Jianhong Pan[3]

[1] Global Energy Interconnection Research Institute Co. Ltd., Nanjing, Jiangsu, China
zhuliang19881003@126.com

[2] State Grid Key Laboratory of Information and Network Security, Nanjing, Jiangsu, China

[3] State Grid Jilin Electric Power Co., Ltd., Changchun 130021, China

Abstract. The participation of power grid enterprises is essential to meet the requirements of new energy reform for carbon neutralization. Aiming at the multi-dimensional sensitivity of power grid enterprises, this paper proposes a digital technical and economic analysis model for power business needs and a digital benefit technical and economic evaluation method based on multi-dimensional index sensitivity analysis, which can meet the requirements of safe and stable operation of power grid, intelligent operation management of enterprises, construction of energy Internet ecosystem, economic accounting of energy Internet industry Driving the demand for the benefit evaluation of digital construction from the aspects of integration economic impact, innovating the production mode of power grid enterprises and the construction of energy Internet service system has important practical significance to improve the economic benefits of power grid enterprises, so as to provide an economic evaluation method for realizing carbon peak.

Keywords: Economic evaluation · Sensitivity analysis · Digital technology

1 Introduction

The digital platform will play a great role in the future energy system. The automatic control system, management system, market system, settlement system and operating system of "net + grid + net" and "source network load storage integration" of smart energy in the future will change the existing digital mode. The establishment of the new system requires strong enterprise informatization and digital platform cooperation, as well as the establishment of new digital system, data platform and mathematical model. However, at present, the research on technical and economic evaluation of digital construction benefits of power grid enterprises is still blank. In recent years, companies in the global power industry are undergoing digital transformation. At present, there are many research work related to digital construction, but the technical and economic evaluation research on the benefits of digital construction of power grid enterprises has not been carried out. There is no targeted, quantifiable and systematic benefit evaluation

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 60–67, 2022.
https://doi.org/10.1007/978-981-19-3486-5_7

method and technical and economic evaluation model. There is no forward-looking research on quantifiable technical and economic evaluation of the digital construction effect of power grid enterprises to adapt to different application scenarios, no scientific and complete benefit evaluation index system required for the benefit evaluation of enterprise digital construction has been established, and there is a lack of quantifiable dynamic evaluation control methods.

Therefore, based on the research on the economic benefit optimization of power grid digital construction project, this paper introduces the design idea of technical and economic evaluation methods such as sensitivity analysis and quantitative control, comprehensively considers various factors such as digital system and cross domain data reuse, establishes the index system of enterprise digital economic benefit evaluation, and constructs the digital economic benefit evaluation model and analysis model, Further, under the constraints of enterprise digital architecture, the dynamic theory of quantitative control is introduced to establish an intelligent quantitative control analysis model.

2 Digital Technical and Economic Analysis Model for Power Business Demand

2.1 Multi Source Correlation Method for Digital Development of Power Enterprises

Firstly, it analyzes the demand of social development for digital development from the aspects of basic resource operation, power data value-added service and digital platform ecological construction. According to the construction principles of digital architecture flexibility, applicability and sustainability, it designs the hierarchical division mechanism of enterprise level digital architecture, and uses brainstorming method Delphi method creates a multi-source association table between business requirement scenarios and digital architecture [1].

Brainstorming. Use collective thinking to guide everyone participating in the meeting to speak widely around the central topic and stimulate inspiration. Each new idea can arouse the association of others, produce a series of new ideas, produce chain reactions, and form a pile of new ideas, which provides more possibilities for creative problem-solving and give full play to their creative thinking ability to the greatest extent, Express independent opinions freely and collect typical business demand scenarios of digital construction as far as possible.

Delphi Method. Eliminate the influence of authority in a back-to-back way, consult the prediction opinions of the expert group members, after several rounds of consultation, make the prediction opinions of the expert group tend to be concentrated, finally make a prediction conclusion in line with the future development trend, and analyze and build a typical business demand scenario of digital construction facing the new industry, new business form and new business model of energy Internet, The requirement tracking matrix method is used to construct the technical association table of typical business requirement scenarios.

Secondly, based on the abstract expression of enterprise business process and digital system facilities, the enterprise level digital architecture scheme is designed by combining work breakdown structure and business process reengineering method according to the needs of enterprise digital socio-economic development, industry and enterprise under the new industry, new business format and new business flow of energy Internet. Then, the value engineering method is used to complete the preliminary screening of digital planning scheme, the digital project economic benefit evaluation technology based on sensitivity analysis is used to complete the financial test of digital planning scheme, and the digital benefit technical and economic evaluation model based on multi-dimensional index sensitivity analysis is used to complete the comprehensive evaluation of digital planning scheme [2]. The model realizes business demand scenario - Technical and economic analysis rules - Technical and economic evaluation model - new industry, new business form, new business model variable factors - digital technical and economic evaluation model information integration and fusion technology.

2.2 Technical and Economic Analysis Flow of Multi-source Correlation Between Power Business Demand Scenario and Digital Architecture

Based on the abstract description of enterprise business process and digital system facilities, the enterprise level digital architecture scheme is designed by combining work breakdown structure and business process reengineering method according to the needs of enterprise digital socio-economic development, industry and enterprise under the new industry, new business format and new business model of energy Internet for carbon neutralization. Then, the value engineering method is used to complete the preliminary screening of digital planning scheme, the digital project economic benefit evaluation technology based on sensitivity analysis is used to complete the financial test of digital planning scheme, and the digital benefit technical and economic evaluation model based on multi-dimensional index sensitivity analysis is used to complete the comprehensive evaluation of digital planning scheme. The model realizes the business demand scenario - Technical and economic analysis rules - Technical and economic evaluation model - new industry, new format, new business model variable factors - digital technical and economic evaluation model information integration technology, and uses the model to carry out technical and economic analysis [3].

The process of technical and economic analysis method of digital project associated with economic business demand scenario and digital architecture is shown in Fig. 1.

The technical and economic analysis method of digital project with multi-source correlation between business demand scenario and digital architecture proposed in this paper innovatively studies the correlation between business demand scenario - Technical and economic analysis rules - Enterprise Digital Architecture - digital planning, and constructs a digital benefit analysis model with multi-source correlation between business demand scenario and digital architecture based on variable factor integration According to different business scenarios such as power data value-added service and digital platform ecological construction, dynamic adjustment of technical and economic evaluation indicators and weights can more accurately complete the digital economic benefit evaluation of power grid enterprises [4].

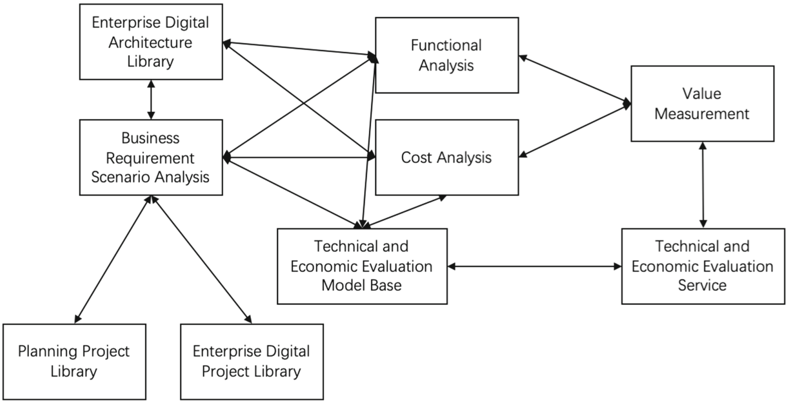

Enterprise Digital Architecture Library
Functional Analysis
Value Measurement
Business Requirement Scenario Analysis
Cost Analysis
Technical and Economic Evaluation Model Base
Technical and Economic Evaluation Service
Planning Project Library
Enterprise Digital Project Library

Fig. 1. Flow chart of technical and economic analysis method of digital project related to business demand scenario and digital architecture.

3 Technical and Economic Evaluation Method of Digital Benefits Based on Multi-dimensional Index Sensitivity Analysis

3.1 Multidimensional Index Sensitivity Analysis

Sensitivity analysis refers to the analysis of the impact on financial or economic evaluation indicators when the main uncertain factors of power grid construction projects change, the calculation of sensitivity coefficient and critical point, the identification of sensitive factors, the determination of their sensitivity, and the analysis of the project's bearing capacity when the factor reaches the critical value. It can be divided into single factor sensitivity analysis and multi factor sensitivity analysis [5].

Single Factor Sensitivity Analysis. The so-called single factor sensitivity analysis method refers to the analysis of the impact of the change of a single uncertain factor on the economic effect of the scheme. The general steps are as follows: determine the sensitivity analysis index. Select the uncertain factors to be analyzed. Analyze the fluctuation degree of each uncertain factor and its possible increase or decrease to the analysis index. Identify sensitivity factors. Calculate the critical point of variation factor. Scheme selection.

Multivariate Sensitivity Analysis. Multi factor sensitivity analysis method is to calculate and analyze the impact of two or more uncertain factors on the economic benefit value of the project under the assumption that other uncertain factors remain unchanged, and determine the sensitivity factors and their limit values. Multi factor sensitivity analysis is generally conducted on the basis of single factor sensitivity analysis, and the basic principle of analysis is roughly the same as that of single factor sensitivity analysis. However, it should be noted that multi factor sensitivity analysis must further assume that several factors that change at the same time are independent of each other, and the probability of change of each factor is the same [6].

3.2 Data Basis of Power Grid Digital Technical and Economic Evaluation Model

On the basis of fully collecting massive historical data such as investment amount, performance, technology, function points, economic benefits, data scale, social benefits and environmental benefits of power grid digitization projects, this paper understands the digitization development trend and demand of power grid enterprises, calculates the weight value of evaluation indexes by using subjective and objective weight methods, and obtains the weight range of each index, Then, the Monte Carlo simulation method is used to randomly generate the weight value of the evaluation index, obtain the multi index weight sample set, and realize the optimal decision-making of the digital project according to the sensitivity of the project evaluation results to the weight, so as to complete the construction of the digital technical and economic evaluation model based on multi-dimensional index sensitivity analysis [7].

3.3 Technical and Economic Analysis Model of Multi-source Correlation Between Business Demand Scenario and Digital Architecture

Based on the comprehensive and in-depth analysis of the impact of new energy Internet industries, new business formats and new business models on the enterprise level digital architecture, the hierarchical division mechanism of enterprise level digital architecture is designed, the support planning scheme for the development needs of the digital system construction foundation of power grid enterprises is created, and the value engineering method and the digital project economic benefit evaluation technology based on sensitivity analysis are applied The technical and economic evaluation model of digital benefits based on multi-dimensional index sensitivity analysis completes the construction of technical and economic analysis model related to business demand scenario and digital architecture.

3.4 Technical and Economic Evaluation Method of Digital Benefits Based on Multi-dimensional Index Sensitivity Analysis

Based on the data of digital technology of power grid enterprises, this paper analyzes the functional and technical composition of digital system and identifies the cost-effectiveness of digital system. This paper studies the correlation between digital system and projects in multiple application scenarios, identifies project constraints and judgment standards, and constructs the scheme of power grid digital system and the financial evaluation model of the project, Complete the technical and economic analysis of digital economic benefits of power grid enterprises, carry out the sensitivity analysis of the impact of uncertain factors on the economic benefits of digital projects, and establish the economic benefit evaluation technology of digital projects based on sensitivity analysis.

Firstly, through investigation and interview, system decomposition and intelligent mining technology, this paper analyzes the functional and technical composition of the digital system of power grid enterprises, and comprehensively combs the existing digital system. The system decomposition method is used to refine and decompose the composition of power grid digital system from multi-dimensional, and the support vector machine and particle swarm optimization algorithm are used to accurately mine the function points of each part. Then, by consulting the software quota, using the functional cost method, service charge price calculation and cost decomposition, the preliminary identification of cost-benefit is completed. Secondly, identify the technical, scale and quality requirements of infrastructure, enterprise platform, business application, value ecology, safety protection and operation guarantee, form the development parameters of digital projects, analyze the independent, interdependent, mutually exclusive and complementary relationship between digital projects, and analyze the financial flow according to the input of digital projects, Formulate project feasibility judgment criteria. Complete the financial evaluation according to the steps of identifying financial costs and benefits, estimating financial costs and benefits, preparing financial statements, calculating financial indicators, etc. For different project types, financial evaluation indicators are selected for analysis and demonstration [8].

Finally, a digital evaluation model based on two-dimensional normal cloud is designed [9], which is used to deal with the uncertain transformation between qualitative concept and quantitative description. Let u be the quantitative domain of the advantages and disadvantages of the benefit evaluation index expressed by accurate numerical value, that is, C is the fuzzy description on u, that is, the primary, intermediate and advanced evaluation of the digital benefit level. If one of the scores x is a random realization in the score U of the overall level of digital benefit, and X is the random number of the stable tendency of C, then x can be called cloud drop, and the distribution of X in the quantitative domain is cloud. The reverse cloud generator is used to realize the transformation from the evaluation score obtained by the evaluation index to the grade division of the evaluation index, and the steps are as follows:

As a cloud drop, the index value of each evaluation index is divided into quantitative value x_i, its membership degree is y_i, and then the expression mode of a cloud drop is (x_i, y_i).

If there are n indicators for evaluation,, calculate the sample mean (1), first-order sample absolute central moment (2) and sample variance (3) of the index score of each evaluation index.

$$\overline{X} = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{1}$$

$$\frac{1}{n}\sum_{i=1}^{n} \left| x_i - \overline{X} \right| \tag{2}$$

$$s^2 = \frac{1}{n-1}\sum_{i=1}^{n} \left(x_i - \overline{X} \right)^2 \tag{3}$$

The sample mean is the expected value E_x, which is the most typical sample from qualitative to quantitative evaluation index.

In combination with the sample mean value, the entropy E_n is obtained by the formula difference (4). Entropy represents the degree of dispersion of index scores, and its value also reflects the value range of index scores that can be accepted by concepts in the universe space.

$$E_n = \left(\frac{\pi}{2}\right)^{\frac{1}{2}} \times \frac{1}{n}\sum_{i=1}^{n}\left|x_i - \overline{X}\right| \tag{4}$$

From the above sample variance and entropy, the super entropy H_e is obtained through formula (5). the greater the super entropy, the greater the dispersion of the evaluation index, and the randomness of the membership degree also increases.

$$H_e = \sqrt{s^2 - E_n^2} \tag{5}$$

The technical and economic analysis and evaluation method of digital economic benefits of power grid enterprises applies the single factor sensitivity analysis and multi factor sensitivity analysis methods to calculate the critical value and sensitivity coefficient of each uncertain factor, analyze and demonstrate the tolerance of digital projects to uncertain factors, Finally, the digital evaluation model based on two-dimensional normal cloud design is used to analyze the super entropy of the influence of uncertain index factors (such as function, technical method, data integration, security protection, performance, infrastructure, construction objectives, operation guarantee, etc.) on the dispersion of digital projects (such as investment, cost, income, life cycle, etc.).

4 Summary

The traditional economic benefits are often based on the economic analysis module of cost and income. Facing the digital economic benefit evaluation scenario of power grid enterprises, this paper studies the digital new technology, new industry, new business form, new business, economy and technology innovation based on fuzzy theory and sensitivity analysis Social coupling relationship and digital economic benefit evaluation method based on multi-dimensional index sensitivity analysis. Compared with the existing technology, the quantitative evaluation model of digital benefits of power grid enterprises based on multi-dimensional index sensitivity analysis in this paper can more accurately complete the economic benefit evaluation of digital technology of power grid enterprises, and provide the methodological basis of economic evaluation for future energy carbon neutralization.

Acknowledgments. This paper was supported by the Science and Technology project in State Grid Corporation of China, which name is ‘Research on the evaluation system and technology tools of digital technology and economy of enterprises, No. 5700-202129180A-0-0-00’.

References

1. Bogner, E., Voelklein, T., Schroedel, O.: Study based analysis on the current digitalization degree in the manufacturing industry in Germany. Proc. CIRP **57**, 14–19 (2016)

2. Yoo, Y., Henfridsson, O., Lyytinen, K.: Research commentary—the new organizing logic of digital innovation: an agenda for information systems research. Inf. Syst. Res. **21**(4), 724–735 (2010)
3. Tong, Y., Li, Y.: The evaluation of enterprise informatization performance based on AHP/GHE/DEA. In: Proceeding of the International Conference on Management. China (2007)
4. Paulus, R.D., Schatton, H., Bauernhansl, T.: Ecosystems, strategy and business models in the age of digitization-how the manufacturing industry is going to change its logic. Proc. CIRP **57**, 8–13 (2016)
5. Hylving, L., Henfridsson, O., Selander, L.: The role of dominant design in a product developing firm's digital innovation. JITTA: J. Inf. Technol. Theory Appl. **13**(2), 5 (2012)
6. Tilson, D., Lyytinen, K., Sørensen, C.: Research commentary—digital infrastructures: the missing IS research agenda. Inf. Syst. Res. **21**(4), 748–759 (2010)
7. Negroponte, N.: Being digital. Vintage (1996)
8. Paritala, P.K., Manchikatla, S., Yarlagadda, P.K.D.V.: Digital manufacturing-applications past, current, and future trends. Proc. Eng. **174**, 982–991 (2017)
9. Yang, Z.H., Li, D.Y.: Planar model and its application in prediction. Chin. Comput. **21**, 961–969 (1998)

Heterogeneous Data Fusion Method for Abnormal Network Traffic

Hong Zhao, Yi Luo, Lei Di, and Wan Rongbai(✉)

State Grid Gansu Electric Power Research Institute, Lanzhou 730070, China
baiwanrong@yeah.net

Abstract. With the iterative development of information technology, the use of mobile terminals, application software and middleware has penetrated into all aspects of life. At the same time, many new security issues have also been raised. Attackers can use loopholes in the system to steal users' personal privacy information and account information. Attackers can also carry out malicious attacks, causing the background system to be paralyzed and causing economic losses to individuals and businesses. This paper takes the abnormal network traffic detection system Snort and the power system state estimation method as examples. First, the traditional power system bad data detection based on state estimation is introduced. Then, a Snort-based grid communication flow anomaly detection and grid data credibility evaluation method is proposed. Finally, how to guide the power system state estimation through the credibility of the measurement data is discussed in detail to realize the detection of data attacks in the power Internet of Things network.

Keywords: Heterogeneous data · Fusion method · Abnormal network traffic · Attackers

1 Introduction

With the iterative development of information technology, the use of mobile terminals, application software and middleware has penetrated into all aspects of life. People's daily work, social interaction and entertainment are all carried out by software, and the popularity of computers and mobile phones has greatly improved the efficiency of handling daily affairs. On August 20, 2018, the China Internet Information Center released a report indicating that as of June 30 of that year, the number of Internet users in my country had reached 802 million, and the Internet penetration rate reached 57.7%, of which the number of mobile phone Internet users accounted for about 98%, which was 7.88 Billion [1]. Netizens' reliance on this convenient interconnection technology is increasing day by day, and it has also caused many new security issues. Attackers can use system vulnerabilities to steal users' personal privacy information and account information, or they can carry out malicious attacks, causing the background system to be paralyzed and causing economic losses to individuals and businesses. In 2017, hackers used the vulnerability tool Eternal Blue leaked by the National Security Agency

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 68–74, 2022.
https://doi.org/10.1007/978-981-19-3486-5_8

to target Windows operating system users and spread the ransomware "Wanna Cry" to the public and intranet through port 445 for file sharing [2]. Nearly 100 countries around the world were quickly affected by the ransomware virus. Important infrastructure including governments, banks, power systems, and medical systems were all attacked, causing significant losses. On December 23, 2015, the power grid of the Ivano-Frankivsk region in western Ukraine was attacked by BlackEnergy malicious code. This caused 7 110 kV and 23 35 kV substations to fail, resulting in a large-scale blackout in Ukraine, affecting 1.4 million people. The entire blackout lasted for 6 h. Through analyzing and investigating actual power grid security cases, as well as recent smart grid security research, it is found that the above-mentioned attacks mainly consist of two parts. First, use network attack technology to conduct attacks on power system information networks such as detection, intrusion, privilege escalation, and control. Second, tampering with the configuration parameters, measurement data, control commands, etc. of the system (data tampering attack) for the work process and security protection mechanism of the power system. The target and main process of the power grid attack reflected in the data tampering attack is the main difference between the power grid attack and the information network attack.

2 Related Research

Many scholars have conducted a lot of research in the face of various attack vulnerabilities arising from irregular software code writing. Zhao et al. proposed a method combining two-way GRU and attention mechanism to effectively detect the code [3]. The advantage of this method is that it can effectively suppress the high false alarm rate and false alarm rate of traditional algorithms. In addition, the method proposed by Zhao et al. also compares the performance of two mature products. The comparison results show that this method has much better performance than these two mature products. On the corresponding data set, the performance of this method is 5.22% and 4.29% higher than that of other scholars' F1 Score, respectively. Static defense has always been a pain point for the power grid. How to switch from passive defense to active defense is a hot topic that scholars have always studied. Zhao et al. proposed a defense strategy to look at the power grid from the perspective of attack [4]. They used the means of game analysis to analyze and research the greatest benefits of the power grid. Finally, a defense plan with great reference significance is given to the grid side. In addition, research on power grid information network attacks has shown that the emergence of new components, equipment and structures has introduced more uncertain factors and risks to the power system [1]. Davis et al. studied the security analysis of smart grid devices and introduced a smart meter worm at the hacker conference (Black Hat). These viruses can propagate themselves in smart devices and cause power grid security threats [2]. Sargolzaei et al. introduced a "time delay attack" in the power system dynamic model. By modifying the signal timestamp, this attack can delay the delivery of the state feedback signal of the dynamic system state space model, thereby destroying the stability of the power system [5]. For the possible secondary frequency modulation control signal (AGC) attack in the power system, Sridhar et al. formally model it, and further divide it into four types: zoom attack, climb attack, pulse attack and random attack. These scholars then analyzed the impact of AGC attacks on power system frequency stability and power market operations [6–8]. Liu et al. proposed that remote coordinated control of the on-off status of multiple circuit breakers in the power grid can interfere with the operation of the generator, thereby destroying the stability of the power system [9].

Stable operation is the core security requirement of the power grid. How cyber attacks damage the stability of the power grid is a hot topic for power grid security this year. In 2009, Liu et al. studied from the perspective of power system state estimation and data verification, and proposed that by constructing specific power measurement data, the false data detection of the power system can be bypassed, which caused tampering attacks on the measurement data in the smart grid. Wide attention of researchers [10]. Shange et al. proposed an electricity meter vulnerability mining and propagation model, which can evade the collection of electricity charges by the power company by modifying the observation value of the electricity consumption of the electricity meter [11]. Kim et al. proposed to tamper with the power measurement data and topology data of the power system at the same time, bypassing the anomaly detection of the power system [12]. In the case of incomplete grid information, Liu et al. proposed a local power flow redistribution algorithm, which can inject local error data into the grid without being discovered. Later, under the condition that the grid information was deleted, it was proposed how to construct wrong data for the local grid to avoid the detection of wrong data.

3 HeteData Fusion Method

Based on the detection methods of abnormal flow of power grid information network and abnormal data of power system, this paper explores the coupling relationship between abnormal network flow and abnormal data of power system in the process of smart grid data tampering attack. The focus is on the heterogeneous data fusion method of various abnormal network traffic and abnormal grid measurement data (HeteData fusion method). This paper takes the abnormal network traffic detection system Snort and the power system state estimation method as examples. First, the traditional power system bad data detection based on state estimation is introduced. Then, a Snort-based grid communication flow anomaly detection and grid data credibility evaluation method is proposed. Finally, how to guide the power system state estimation through the credibility of the measurement data is discussed in detail to realize the detection of data attacks in the power Internet of Things network.

3.1 Bad Data Detection of Power System Based on State Estimation

State estimation is widely used to reduce the observation error of the power system for the purpose of detecting bad data and monitoring the real-time operating status of the power system. The redundancy of the quantity measurement can also be used to reduce the influence of transmission errors on the estimated state. In state estimation, node active/reactive power and line real-time power flow can be used as measurement data.

Let z be the measurement vector, the power system measurement model is:

$$z = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{bmatrix} = \begin{bmatrix} h_1(x_1, x_2, \cdots, x_n) \\ h_2(x_1, x_2, \cdots, x_n) \\ \vdots \\ h_m(x_1, x_2, \cdots, x_n) \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{bmatrix} = h(x) + e \tag{1}$$

where ***x*** is the state of the system, including the voltage amplitude and phase angle of the node; ***h_i(x)*** is the non-linear function between the ***i-th*** measured value and the system state value; ***e*** is the measurement error.

The model is implemented by Maximum Likelihood Estimation (MLE). In weighted least squares estimation, the optimization goal is to minimize the weighted sum of squares of the residuals between the estimated value of the measured data and the true value. The common likelihood function is:

$$J(x) = \sum_{i=1}^{m} (z_i - h_i(x))^2 / R_{ii} = [z - h(x)]^T R^{-1} [z - h(x)] \tag{2}$$

In order to achieve the optimization goal, the first derivative of the likelihood function needs to be 0:

$$\begin{aligned} g(x) &= \frac{\partial J(x)}{\partial x} = -H^T(x) R^{-1} [z - h(x)] = 0 \\ H(x) &= \frac{\partial h(x)}{\partial x} \end{aligned} \tag{3}$$

Expand the nonlinear function g(x) into a Taylor polynomial and omit the high-order terms (usually only one term is retained), and then use Newton-Raphson iteration to solve the state to be estimated. State estimation utilization measurement redundancy can eliminate the influence of errors to a certain extent. However, large measurement deviations may cause errors in the state estimation results. Some bad data can be checked by the laws of physics such as energy conservation. Therefore, in most cases, it is necessary to use more advanced methods for bad data detection (Chi-squares Test). Under normal circumstances, the measurement error is considered to be a set of independent random variables obeying a zero-mean Gaussian distribution, then the objective function of weighted least squares:

$$J(x) = \sum_{i=1}^{m} (r_i)^2 / R_{ii} = \sum_{i=1}^{m} (z_i - h_i(x))^2 / R_{ii} = \sum_{i=1}^{m} \left(\frac{z - h_i(x)}{\sqrt{R_{ii}}} \right)^2 \tag{4}$$

J(x) satisfies the chi-square distribution of m–n degrees of freedom under normal conditions. This is because the power system measurement model is an equation group with m measurement equations and the independent variable is an n-dimensional state vector. The formula for calculating the cumulative and area of the probability density function of the chi-square distribution is:

$$\Pr\{x \geq x_t\} = \int_{x_t}^{\infty} \chi^2(u)\, du \tag{5}$$

When bad data exists, the residual between the true value of the measured value and the estimated value will be abnormal, and the cumulative sum of squares is likely to not obey the chi-square distribution.

3.2 SmaGrid AbnFlow and Credibility Calculation Method

Here, we propose a smart grid abnormal flow detection technology and grid data credibility calculation method (SmaGrid AbnFlow and Credibility Calculation Method). Snort is a widely used intrusion detection system that provides a simple way to protect the system from intrusion by interpreting the work logs of network devices such as routers, firewalls, and servers. It can detect unauthorized access, use, and attacks on systems, networks, equipment, and related resources. As a conventional information security strategy, the target object of Snort at the beginning of the design was a computer network, and it did not consider the needs of the power system. This makes it not directly applicable to power critical infrastructure.

Therefore, it is necessary to use Snort's rule customization function to support the analysis and monitoring of smart grid communication control protocols. Aiming at the Modbus/TCP communication protocol used by smart meter devices, through the analysis of communication data packets and network traffic characteristics of several typical attack behaviors, it is found that typical attack cases targeting smart power devices generally have the following characteristics:

(1) The target of the attack is usually the key register of the power equipment storing sensitive information. Take the smart meter used in the smart grid as an example. Its key parameters such as current mutual inductance ratio, voltage mutual inductance ratio, and meter connection type are stored in different registers. The primary current information of Siemens SERTRON PAC4200 smart meter is stored in register C35B. The connection type of the electric meter is stored in the register C351. Since the primary current information and the connection type of the electric meter are directly related to the measurement and calculation of power consumption data, these key register locations are potential targets and targets of malicious attackers.

(2) Different attack types and attack behaviors have obviously different data and traffic characteristics. For a typical attack case of a smart meter, the behavior of a malicious attacker to decipher the password will cause frequent read requests to the smart meter's password status register. Malicious users tampering with the smart meter's mutual inductance ratio and "stealing electricity" will cause write operations to the registers that store the "primary current" and "secondary current". These different types of security attacks will present different access operation behaviors, which can be used as pattern characteristics and identification basis to detect different types of attack behaviors. According to this, intrusion detection suitable for smart grid information network is based on the conventional Snort definition of related detection rules about the communication flow of electricity meter equipment and the Modbus/TCP communication protocol. So as to monitor the read and write operations of the sensitive registers of the smart power equipment. By parsing network data packets and analyzing traffic behavior through rules, we have realized the detection of attack behaviors such as smart meter password blasting, mutual

inductance ratio tampering, and connection type modification. The attack types and threat indicators of abnormal traffic alarms are recorded in the alarm log. This can quantify the impact of abnormal network traffic and generate an information network impact factor.

All abnormal traffic information of any power equipment node can be traced back through the IP address. At the same time, the corresponding attack types and threat indicators can be determined. Therefore, based on the information/physical topology of the power system, all the alarm records of any terminal node $\boldsymbol{i}$ in the system will be aggregated, and the corresponding influence factor will be calculated.

3.3 EstCredibility Measurement Method

Here, we propose a power system state estimation method guided by the credibility of measurement data(EstCredibility measurement Method). Considering that when an attack occurs on the smart grid, both the tampered data and the attacked device will generate specific communication messages. These messages can be analyzed using abnormal traffic detection technology, and based on the influence factors of the abnormal traffic of each node. In turn, the trustworthiness of the data reported by each node can be evaluated. The information influence factor matrix of n equipment nodes in the power system defines $\Omega = DiagonalMatrix(\Omega_1, \Omega_2, \ldots \Omega_n)$. The information impact factor matrix can be directly integrated into the objective function J(x) of formula (5) as additional weights, namely:

$$\min_x J_{ATSE}(x) = \min_x [z - h(x)]^T (\Omega R)^{-1} [z - h(x)] \tag{6}$$

4 Conclusion

In short, this paper proposes a HeteData fusion method to solve the problem of difficult data fusion for power grid attacks. First, the traditional power system bad data detection based on state estimation is introduced. Then, a Snort-based grid communication flow anomaly detection and grid data credibility evaluation method is proposed. Finally, how to guide the power system state estimation through the credibility of the measurement data is discussed in detail to realize the detection of data attacks in the power Internet of Things network.

Acknowledgments. This work was supported by State Grid Gansu Electric Power Research Institute Project-Intelligent Recognition and Defense of Intrusion Behavior of Electric Power Information and Physical Fusion System in Cyber Attack Environment (No. 52272219000E).

References

1. Mei, S., Zhu, J.: Several mathematics and control science problems in smart grids and their prospects. Acta Autom. Sinica **39**(2), 119–131 (2013)

2. Davis, M.: SmartGrid device security: adventures in a new medium. In: Black Hat. Las Vegas, USA (2009)
3. Zhao, J.X., Guo, S., Mu, D.: DouBiGRU-A: software defect detection algorithm based on attention mechanism and double BiGRU. Comput. Secur. **111**, 102459 (2021)
4. Zhao, J.X., Zhang, X.: Exploring the optimum proactive defense strategy for the power systems from an attack perspective. Secur. Commun. Netw. **2021**, 1–8 (2021)
5. Sargolzaei, A., Yen, K., Abdelghani, M.N.: Delayed inputs attack on load frequency control in smart grid. In: Innovative Smart Grid Technologies Conference (ISGT), IEEE PES 2014. IEEE (2014)
6. Sridhar, S., Hahn, A., Govindarasu, M.: Cyber-physical system security for the electric power grid. Proc. IEEE **100**(1), 210–224 (2012)
7. Liu, S., et al.: A coordinated multi-switch attack for cascading failures in smart grid. IEEE Trans. Smart Grid **5**(3), 1183–1195 (2014)
8. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. In: Proceedings of the 16th ACM Conference on Computer and Communications Security. Chicago, Illinois, USA (2009)
9. Shange, M., et al.: A game-theory analysis of the rat-group attack in smart grids. In: 2014 IEEE 9th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP). IEEE (2014)
10. Kim, J., Tong, L.: On topology attack of a smart grid: undetectable attacks and countermeasures. IEEE J. Sel. Areas Commun. **31**(7), 1294–1305 (2013)
11. Liu, X., Li, Z.: Local load redistribution attacks in power systems with incomplete network information. IEEE Trans. Smart Grid **5**(4), 1665–1676 (2014)
12. Liu, X., et al.: Modeling of local false data injection attacks with reduced network information. IEEE Trans. Smart Grid **6**(4), 1686–1696 (2015)

Contactless Access Control System Based on Voiceprint Recognition

Leyuan Zhang, Juanjuan Li(✉), Miaoyun Feng, Weiye Qu, and Jiale Xu

Soochow University, No. 1 Shizi Street, Suzhou, China
lijuanjuan@suda.edu.cn

Abstract. In order to increase the security and convenience of access control system, a contact-free access control system based on voiceprint recognition is designed and has been tested for many times. This system takes the speaker's voiceprint feature as the "key", and it contains an Android-based voiceprint recognition APP—which is related to voiceprint registration, voiceprint verification, model addition or deletion and other functions—and a self-designed control system which communicates with the APP through Bluetooth technology. During functioning, a random 8-bit dynamic number was obtained from the cloud through the network API interface provided by IFLYTEK (Chinese information technology company) as the text password, and then the voiceprint information was uploaded to the cloud for identification, and the result was transmitted to the hardware control module through Bluetooth. By testing, the similarity between the speaker's voiceprint information and the corresponding model is more than 97%, and the negative rate of recognition was 0%, with the average recognition time less than 0.4 s.

Keywords: Voiceprint · Recognition access control system · Bluetooth communication

1 Introduction

With the innovation of computer technology and the development of Internet Of Things technology (IOT), traditional keys and locks are gradually replaced by the card access control. However, access control card has unavoidable security risks. For example, it's easy to lose access control card and the access control card can be cracked and copied. While the access control system based on the voiceprint recognition technology takes people's voiceprint characteristics as the password, and judges the identity of the speaker by the voice, which can effectively increase the security and convenience of the access control system [1].

Voiceprint recognition, also known as speaker recognition, is to extract the speaker's personality characteristics from a speech of the speaker, and to identify or confirm the speaker through the analysis and recognition of these personal characteristics. People's vocal characteristics are mainly determined by two factors. One is the shape, size, dimension and position of various organs in the vocal cavity, which determines the tension

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 75–84, 2022.
https://doi.org/10.1007/978-981-19-3486-5_9

of the vocal cords and the size of the frequency range of the sound. The other is the sound characteristics produced by the coordination and movement of the vocal organs [2]. Voiceprint recognition technology collects people's unique voiceprint characteristic information to establish voiceprint models, which serve as the discriminant basis of identity authentication.

The voiceprint recognition technology is applied to the door guard system, and the security of the door guard system is greatly improved by comparing the voiceprint characteristics and the voice pattern model and distinguishing the voice content and the text content. At the same time, compared with card access control, voiceprint access control can change and delete users' permissions at any time, making the system more convenient to use and have lower cost.

2 System Design Scheme

Voiceprint recognition system refers to a system that can identify and verify the speaker's identity according to the speaker's voice. Based on the analyses of the basic requirements of the system, the design of the system is based on mobile platform, and the application scenario is access control system. For the consideration of security, the content of identifying people's speech should be random dynamic password. Therefore, the whole voiceprint recognition system is a mobile platform based on text-related speaker identification system [3].

According to the basic requirements of the system, the design process of the system is roughly shown in Fig. 1: During the process of training, users are required to register first and input their identity information, and then the background checks whether the user information exists. If it already exists, the user is not allowed to register his or her voiceprint. If the user's information does not exist, the user is required to register the voiceprint according to the dynamic password prompted by the text and then he or she will be informed whether the registration is successful. In the process of identification, the user is required to input the identity information first, and then the background checks whether the user's voiceprint model exists. If the voiceprint model does not exist, the user is regarded as an invalid user and is not allowed to perform voiceprint verification. If the voiceprint model exists, the user is required to perform voiceprint verification according to the dynamic password prompted by the text, and the verification result is returned and informed to the user [4]. Considering the stability and security of the verification result transmission, Bluetooth technology is used to communicate with the self-designed hardware module.

The basic principle of voiceprint recognition is as shown in Fig. 2. voiceprint recognition is mainly composed of preprocessing, endpoint detecting, feature extracting, model building, calculation matching and judgment recognizing [5]. Voiceprint recognition includes two stages: training stage and recognition stage [6]. The training stage is also called as voiceprint registration. Each speaker of the system speaks several training statements, according to which the system establishes the template or model parameters of each user [8]. In the recognition stage, the voice of the person to be recognized after feature extraction is compared with the model generated by system training, and the speaker corresponding to the speaker model with the smallest matching distance of the test voice is taken as the recognition result [9].

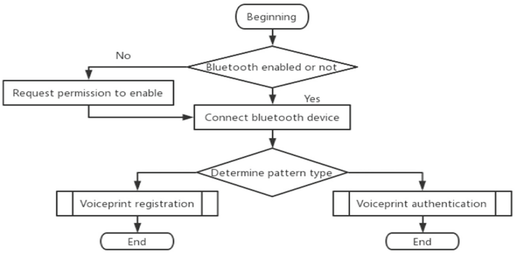


Fig. 1. Flow chart of system design

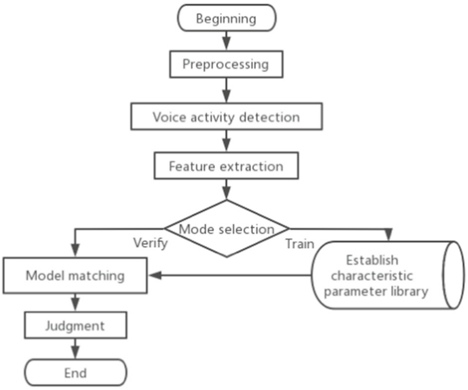


Fig. 2. Flow chart of principle of voiceprint recognition system

In order to meet the accuracy and real-time performance of voiceprint recognition, the system will adopt the Software development Kit (SDK) provided by *iFLYTEK* for developers and conduct voiceprint recognition in the cloud by calling the API interface of the cloud platform of *iFLYTEK*. As a national backbone software enterprise specializing in intelligent voice and voice technology research and voice information service, *iFLYTEK* has in-depth research in the field of voiceprint recognition. The interface of voiceprint feature extraction provided by its SDK can extract a variety of feature parameters as the voiceprint model, which has a high recognition rate in the voiceprint verification and can quickly and accurately identify the speaker in a relatively quiet environment. At the same time, the SDK also provides an interface to obtain 8-bit random dynamic numeric password from the cloud, which meets the security requirements of the work design.

The hardware module consists of STM407ZET6 core board, steering gear, Bluetooth module, serial screen, infrared ranging. When STM32 is connected to the Bluetooth module, it communicates with the mobile phone APP. If the phone's voiceprint is identified successfully, the message will be returned to STM32 and STM32 controls the steering gear to control the door switch after receiving the message. Meanwhile, the corresponding human-computer interaction interface will be displayed on the serial port screen. When people walk through the threshold, the infrared tube will detect the change of distance, so as to determine whether people have entered. After entering, the door will be closed through the steering gear.

3 Module Analysis

The whole system can be divided into software part and hardware part, and the software part (see Fig. 3) mainly includes voiceprint registration, voiceprint recognition, Bluetooth communication and other functional modules.

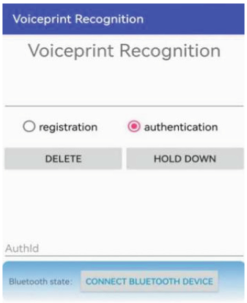


Fig. 3. The main interface

3.1 Voiceprint Registration Module

The running process of voiceprint registration module system is shown in Fig. 4. The specific processes are as follows:

1. Call initUi() function to initialize UI interface, Button control, dialog box control, and input box control.
2. Initialize each listener, including the following listeners: PcmRecordListener, DownloadPwdListener and EnrollListener and so on. A listener is a callback function, and the function of a listener is that whenever your button or other components are clicked on by the mouse, it will generate an event, and that event requires us to listen for it. After listening for it, we give the code that needs to be executed to the clicked event [7].
3. Determine the session scenario type. SST_ENROLL indicates a voiceprint registration scenario, and SST_VERIFY indicates a voiceprint verification scenario.
4. Configure defined parameter variables, including user ID, session type, password type, password, model operation command, and registration times and so on.
5. Input AuthID. The AuthID is the unique identifier of the user's identity information. A user input the AuthID manually and the getAuthid() function is called. After the user input the AuthID, the ModelListener (model operation listener) listens to the AuthID and determine whether the model corresponding to the ID exists. If the model exists, the user is not allowed to register and then the user is required to input the AuthID again.

6. Call the downloadPwd() function to obtain a string of random numbers from the cloud, for example, 13587459–89732657-6548 7321–9568412348915198. Divide the string into five 8-bit numeric strings, each as a password for five registrations.
7. Start recording. Start the recorder and save the sound input by the user in "*.wav" format.
8. Determine the number of registrations. In the voiceprint registration stage, users is required to register for five times according to the five digital passwords obtained from the cloud.
9. Upload the voice information input by the user to the cloud platform. The cloud platform extracts the voiceprint feature parameters and returns them to the client. After the client establishes the voiceprint model, it is stored in external memory.

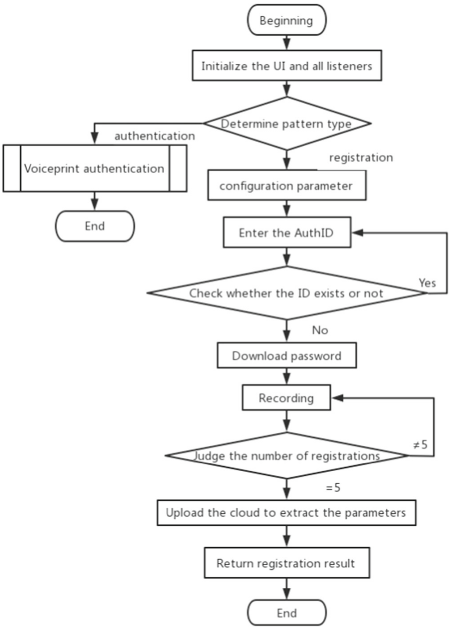

Beginning
Initialize the UI and all listeners
Determine pattern type
authentication
registration
Voiceprint authentication
End
configuration parameter
Enter the AuthID
Yes
Check whether the ID exists or not
No
Download password
Recording
≠5
Judge the number of registrations
=5
Upload the cloud to extract the parameters
Return registration result
End

Fig. 4. Voiceprint registration flow chart

3.2 Voiceprint Verification Module

The running process of the voiceprint verification module and the voiceprint registration module is roughly similar. The running process of the voiceprint verification is as shown in Fig. 5 and the specific steps are as follows:

1. Initialize the UI interface, button control, dialog box control and input box control.
2. Initialize PcmRecordListener, DownloadPwdListener, and VerifyListener and so on.

3. Determine the type of the session scenario.
4. Configure defined parameter variables.
5. Input AuthID. As the unique identifier of user identity information, AuthID is used in all modules of the system and is the most important parameter in the entire system [10].
6. Check whether the voiceprint model corresponding to this AuthID exists in the voiceprint library. If not, ask the user to input the voiceprint model again.
7. Call the downloadPwd() function to obtain the authentication password from the cloud. Unlike voiceprint registration, voiceprint authentication only needs to read the password once, so the password obtained from the cloud is an 8-digit dynamic password.
8. Start the recorder and start recording.
9. Upload the voice information of the person to be recognized so that the voice pattern model will be matched in the voice pattern library and be calculated its similarity in the cloud.
10. The cloud will return the recognition result and similarity to the client.
11. After receiving the verification result, the client sends specific command characters to the access control through Bluetooth communication.

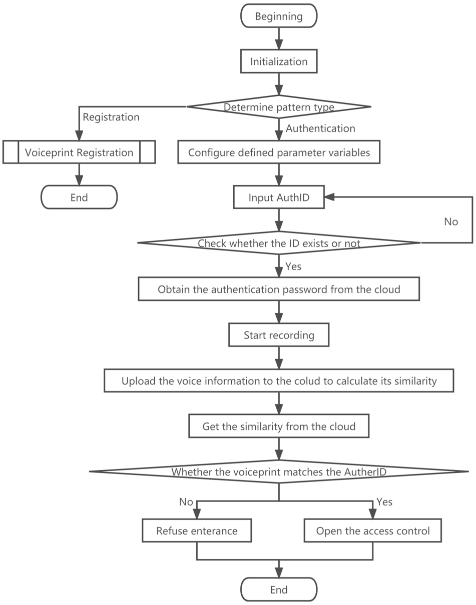

Beginning
Initialization
Determine pattern type
Registration
Authentication
Voiceprint Registration
End
Configure defined parameter variables
Input AuthID
No
Check whether the ID exists or not
Yes
Obtain the authentication password from the cloud
Start recording
Upload the voice information to the colud to calculate its similarity
Get the similarity from the cloud
Whether the voiceprint matches the AutherID
No
Yes
Refuse enterance
Open the access control
End

Fig. 5. Flow chart of voiceprint recognition

3.3 Model Operation Module

Model operation module has two session scenarios, namely model query and model deletion. When ModelListener (model operation listener) listens to voiceprint registration and voiceprint verification, model query operation is performed when the event that the user has input AuthID occurs. When ModelListener listens to the event that "delete voiceprint" button is pressed, the model deletion operation is carried out. The specific workflow is shown in Fig. 6.

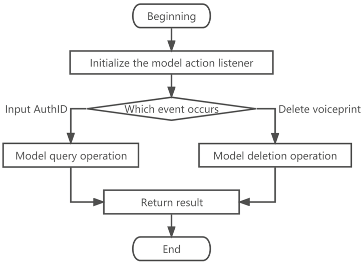


Fig. 6. Operation flow chart of model operation module

3.4 Hardware Implementation Module

STM32 is mainly responsible for the control of the door and the display of human-computer interaction after receiving instructions [11]. When the voiceprint is recognized successfully, the mobile phone will send a command character "F" via Bluetooth communication. When the STM32 receives the characters, it will control the steering gear to revolve the supporting shaft of the door, thus to control the door open. At the same time, related interaction information will be displayed on the serial port screen, such as "Welcome home" "Successful Recognition" and so on. When the user is going through the door, the infrared sensor will measure the distance. If someone passes, the distance will be sharply reduced, so as to judge that someone passes. When the distance is restored, the door will be closed by controlling the steering gear, so as to complete the control of the whole hardware part [12]. Below are model diagram and schematic diagram of the main control module (Fig. 7).

4 Test Results

In order to test the performance of the Android-based voiceprint recognition APP designed in part of this software, the mobile phone is connected to the Android Studio platform to build a real machine testing environment and carries out a comparative test on recognition similarity and training time [13]. In addition, the recognition effect of speakers of different genders will be tested, and acceptance rate and misrecognition rate will be analyzed to verify the performance of the design [14].

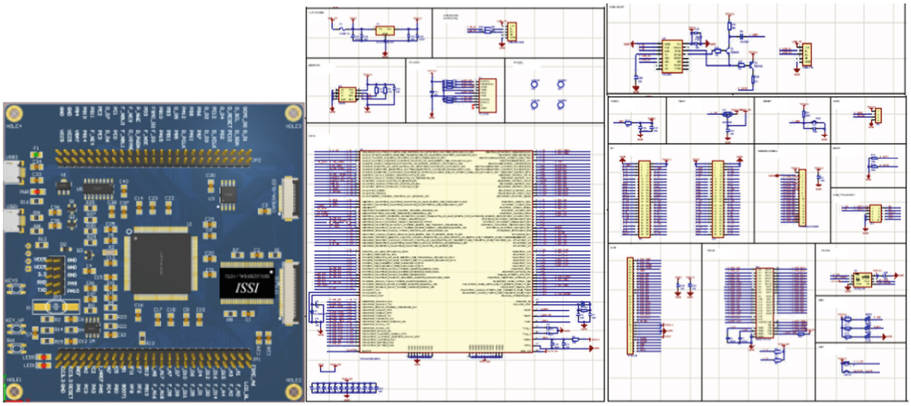


Fig. 7. Model diagram and schematic diagram of the main control module

4.1 Test Environment

This test will be conducted on the Android Studio platform connected to the real computer. During the process of debugging, we can find the similarity of voiceprint recognition and receive information by viewing logs [15]. The space around the test site is relatively open, and the influence of environmental noise on the test results is limited.

4.2 Test Contents

Table 1. The test result

Serial number	Average similarity (%)	True positive rate (%)	False positive rate (%)	Negative rate (%)	Average recognition time
1	97.500	100	0	0	391 ms
2	98.380	100	0	0	323 ms
3	8.050	0	100	0	297 ms
4	29.269	0	100	0	305 ms

There were 40 participants in this experiment, 20 male students numbered from 1 to 20 and 20 female students numbered from 21 to 40. The objects of test 1 are 20 males Student1 to Student20, and the test models are corresponding to each object. The test object of test 2 is 20 female Student21 to Student40. The test model is the corresponding model of the test object. The test object of test 3 is male Student1 to Student5, and the test mode is female Student21 and Student22. The test object of test 4 are male Student1 to Student5, and the test models are male Student11 and Student12. All test results are shown in Table 1 above.

4.3 The Analyses of Test Result

In Test 1, all the test objects were male, and the test model was corresponding to each test object. The recognition result was "Accepted", and the average similarity of recognition was 97.500%. In Test 2, all the test objects were female, and the test model was the corresponding model of each test object. The detected recognition result was "Accepted", and the average similarity of recognition was 98.380%. In Test 3, all the test objects are male, and the test model is the corresponding model of the female non-test object. The recognition result is "Rejected", and the average similarity of recognition is 8.050%. In Test 4, all the test objects are male and the test model is the corresponding model of the male non-test object. The recognition result is "Rejected" and the average similarity of recognition is 29.269%.

Compared with the experimental results above, the similarity between the voiceprint information of the person to be identified and the model of the corresponding voiceprint reached more than 97%, the negative rate of recognition was 0%, which meets the accuracy requirements of the system design. The average time of the four tests were 391 ms, 323 ms, 297 ms and 305 ms respectively, and the average test time was less than 0.4 s, which meets the real-time requirement of the system design. At the same time, the text-related voiceprint recognition method is designed in this paper. The 8-bit random digit password obtained from the cloud is used as the recognition text, which meets the security requirements of the system design.

5 Conclusion

This paper introduces the overall design of this design in detail. With the technical support of *iFLYTEK* cloud platform, a contact-free access control system based on voiceprint recognition has been successfully designed. voiceprint recognition and voiceprint verification can be carried out successfully in this work, and the work can communicate with hardware through Bluetooth. After testing, the similarity of recognized voiceprint model is above 97%, the negative rate of recognition was 0%, and recognition time is within 0.4 s.

There are also some deficiencies in the voiceprint recognition access control system designed in this paper. First, a relatively quiet environment is required, the robustness of the system needs to be further improved, and the noise reduction scheme can be improved. Second, the verified voiceprint features have not been added to the training database. To realize the real-time update of the feature model database, optimization of the training algorithm can be considered.

Acknowledgement. This work was supported by China National Training Program of Innovation and Entrepreneurship for Undergraduates (No. 202110285029Z).

References

1. Pei, X.: Research of Voiceprint Recognition System. Harbin University of Science and Technology (2014)

2. Xue, Z.Y.: Design of Door Access Control System based on Voiceprint Recognition. Inner Mongolia University of Technology (2017)
3. Fang, Z., Li, L.T., Zhang, H., et al.: Overview of voiceprint recognition technology and applications. J. Inf. Secur. Appl. **2**(1), 44–57 (2016)
4. Li, Y.D.: Design and Implementation of Voiceprint Recognition on Android Platform. Xidian University (2020)
5. Gao, M.: Software Design and Implementation of Voiceprint Recognition Module Based on ARM. Southeast University (2019)
6. Yang, M., Chen, Y.M.: Voice identification technology and it's application. Audio Eng. **02**, 45–46 (2007)
7. Yu, S.: Design and Implementation of Android App Rapid Development Platform. Xidian University (2015)
8. Sun, M.: Research on Correlation Between Language Features and Voiceprint Recognition System Based on LPCC and MFCC. South-Central University for Nationalities (2017)
9. Bahuguna, S., Raiwani, Y.P.: A study of speech emotion and speaker identification system using VQ and GMM. Int. J. Comput. Sci. Issues **13**(4), 41 (2016)
10. Wu, Z., Evans, N., Kinnunen, T., et al.: Spoofing and countermeasures for speaker verification: a survey. Speech Commun. **66**, 130–153 (2015)
11. ST. Microcontrollers & Microprocessors/STM32 32-bit Arm Cortex MCUs/STM32 High Performance MCUs/STM32F4 Series/STM32F407/ 417/STM32F407VG, https://www.st.com/en/microcontrollers-microprocessors/stm32f407vg.html. Accessed 20 May 2020
12. yuanjun33: Schematic and PCB Package of STM32F407VGT6, www.csdn.net. Accessed 22 May 2020
13. Li, J.W.: Research and Implementation of the Voiceprint Recognition System Based on Android. Fuzhou University (2014)
14. Nugraha, A., Rahman, F.A.: Android application development of student learning skills in era society 5.0. J. Phys. Conf. Ser. **1779**(1), 012–014 (2021)
15. Zhang, Y.L.: Android Development Application Combat Details. China Railway Press, Beijing (2011)

Establishment of Vulnerability Sample Database in Network Attack Environment

Hongzhong Ma, Yi Luo, Lei Di, and Wan Rongbai(✉)

State Grid Gansu Electric Power Research Institute, Lanzhou 730070, China
baiwanrong@yeah.net

Abstract. In recent years, the number of software vulnerabilities has been on the rise. Attackers can use vulnerabilities to gain access to the system or network to perform malicious actions. This paper relies on CVE, Exploit Database (vulnerability database website) and other platforms to automatically grab information on the vulnerability platform through Python crawlers and scripts to obtain all vulnerability information with POC. At the same time, we take the code before and after the modification given by the vulnerability platform as positive and negative samples, and locate the modified position. According to the classification standard of CWE (Common Weakness Enumeration), vulnerabilities are classified into buffer overflow, conditional competition, UAF, information leakage, XSS, SQL injection, CSRF, etc. In order to build a database of vulnerability samples for the study of malicious attacks.

Keywords: Establishment · Vulnerability sample database · Network attack environment · CVE

1 Introduction

Software vulnerabilities, also called vulnerabilities, are caused by the negligence of software developers when developing software or by the programming language limitations. For example, the C language family is more efficient than Java but has more vulnerabilities. Usually refers to the defects in the computer system, or problems arising from the use of the system. According to the definition of the authoritative vulnerability publishing organization CVE, vulnerabilities refer to calculation logic errors found in software and some hardware components (for example, firmware). When an attacker exploits this weakness, it will have a negative impact on one of the three elements of information security (confidentiality, integrity, and availability) [1]. Attackers can use vulnerabilities to gain access to the system or network to perform malicious actions. In recent years, the number of software vulnerabilities has been on the rise. According to CVE data, the number of vulnerabilities recorded in CVE in 2010 was approximately 4,600. By 2018, the number of vulnerabilities had increased to more than 100,000. The number of vulnerabilities has increased rapidly since 2017. According to the 41st "Statistical Report on Internet Development in China" [2] released on January 31, 2018, in 2017 alone, CNVD [5] collected a total of 15,981 security vulnerabilities. Compared with 10,821

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 85–91, 2022.
https://doi.org/10.1007/978-981-19-3486-5_10

in 2016, an increase of 47.7%. In the Internet industry, competition is fierce, software development cycles are getting shorter and shorter, and security issues are becoming increasingly prominent. Undercurrents in the field of network security are surging, and the trend of attacks continues to rise. T-level DDoS attacks have broken out many times, data breaches have emerged one after another, and ransomware has become popular. In addition, with the advent of a new wave of "going out to sea" in my country's Internet industry, the surge in overseas business has stimulated a large number of overseas hackers to join the "cake-sharing" team. In addition to increasing sources of attacks, the range of targets being attacked is also expanding. More and more attacks are appearing in more segmented industry sectors that were previously rare. Websites in various industries are facing a more severe security test. Take DDoS attacks as an example. Know that the network attack and defense data of Chuangyu Cloud Defense Platform focuses on the display and analysis of DDoS attacks and web attack data in 2018. The collected data showed that the peak value of DDoS attacks exceeded the T level. The industry's highest peak of defensive attacks has reached 1980Gbps, a year-on-year increase of up to 200%. At the same time, the emergence of new types of reflection attacks indicates the severity and difficulty of DDoS attacks.

2 Related Research

Code data is the basis for studying vulnerabilities. Foreign research on database construction is earlier, and there are many vulnerability databases with greater international influence. The more common ones are NVD, Exploit-Database, Bugtraq, OSVDB, and so on. NVD (National Vulnerability Database) [3] is the representative of a standards-based vulnerability management database used by the US government using the Secure Content Automation Protocol (SCAP). The database can automate vulnerability management, security measurement, and compliance requirements. NVD not only includes security list references (i.e. CVE), but also includes software-related code vulnerabilities, misconfigurations, product names, and gives indicators of the impact of vulnerabilities (i.e. CVSS). Exploit-Database [4] is a database composed of public vulnerabilities compatible with CVE and corresponding vulnerable software. The database also provides a wealth of test examples for vulnerability researchers to study and learn. The database obtains the most comprehensive exploits by collecting direct submissions from users and other public resources, and presents them in a freely accessible and easy-to-navigate database. Users can search by CVE number, OSVDB number, vulnerability description, etc. OVSDB (Open Sourced Vulnerability Database) [5] is an open source vulnerability database that provides accurate and detailed vulnerability information. It has more than 64,000 vulnerability information, rich data resources, and provides complete vulnerability retrieval functions and vulnerability classification browsing methods. In addition, it also provides vulnerability data in different formats for users to download, and a detailed vulnerability description is attached to the vulnerability.

SARD (Software Assurance Reference Dataset) [6] is a database led by the National Institute of Standards and Technology (NIST). Its purpose is to provide a set of known security flaws for users, researchers and security engineers, and to provide test cases for test evaluation and software development. These test cases include framework design, source code, binary files, etc., which come from all stages of the software life cycle. The data set includes code test cases from industry and academia, including various vulnerability types, programming languages, system platforms, compilers, etc. The SARD data set also provides test cases for users to learn and reference. Since the standards of each database are different, it has caused great difficulties in data sharing among vulnerable databases. This requires a common vulnerability standard to solve the compatibility problem between various databases. SCAP (security content automation protocol) is a set of information security assessment standard system widely used internationally [7]. SCAP is composed of a series of common open standards that work together to comprehensively define, describe, and evaluate vulnerabilities. Among the many vulnerability standards, this project focuses on CVE, CWE and CVSS. CVE (Common Vulnerabilities and Exposures) [8] is a list of common identifiers for network security vulnerabilities known to the public. CVE is now the industry standard in the field of vulnerabilities. More than 100,000 vulnerabilities are covered in the CVE, which is available for users to download. All vulnerabilities in CVE use the CVE number as a unique identifier, which is compatible with other vulnerability databases. CWE (Common Weakness Enumeration) [9] is a list of common software weakness types, often used as a common language for describing software security weaknesses in architecture, design or code. In addition, some scholars study power grid security from the perspective of code security and attackers [10, 11].

3 Vulnerability Sample Database Construction

3.1 Ideas for Constructing Vulnerability Sample Database

The construction design of the vulnerability database in this paper is shown in Fig. 1. Relying on CVE, Exploit Database (vulnerability database website) and other platforms, through the means in Fig. 1, all the vulnerabilities with POC and their information are obtained. At the same time, we take the code before and after modification given by the vulnerability platform as positive and negative samples, and locate the modified position. According to the classification standard of CWE (Common Weakness Enumeration), vulnerabilities are divided into buffer overflow, conditional competition, UAF, information leakage, XSS, SQL injection, CSRF and other categories. The standards are shown in Fig. 1 below:

NVD is a standards-based vulnerability management database represented by the US government using the Secure Content Automation Protocol (SCAP). This data can be used to automate vulnerability management, security measurement, and compliance. NVD includes the database referenced by the safety checklist, safety-related software defects, misconfigurations, product names and impact indicators. The vulnerabilities in NVD are rich in resources, and the vulnerabilities are described in detail. In addition, Json files and XML files are provided for users to download and use. The Exploit database is an archive of CVE-compatible public vulnerabilities and corresponding vulnerable software for use by penetration testers and vulnerability researchers. By directly submitting the mailing list, it can be presented in a freely accessible and easy to navigate database. Users can search by CVE number, OSVDB number, vulnerability description, etc. CVE, Common Vulnerabilities and Disclosures, is a list of common identifiers for

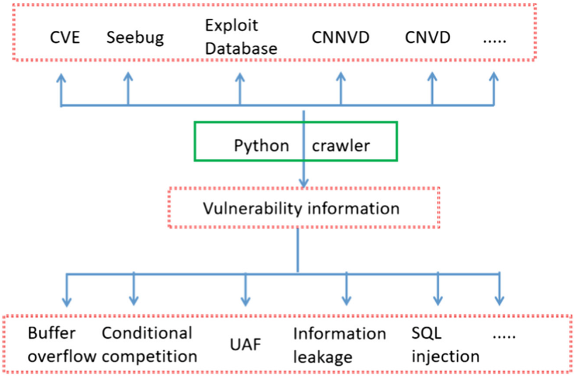


Fig. 1. Schematic diagram of vulnerability database construction

network security vulnerabilities known to the public. CVE is now the industry standard for vulnerabilities and exposed identifiers. More than 100,000 vulnerabilities are covered in CVE, and XML files are provided for users to download. All vulnerabilities in CVE are uniquely identified by the CVE number, which is compatible with other vulnerability databases.

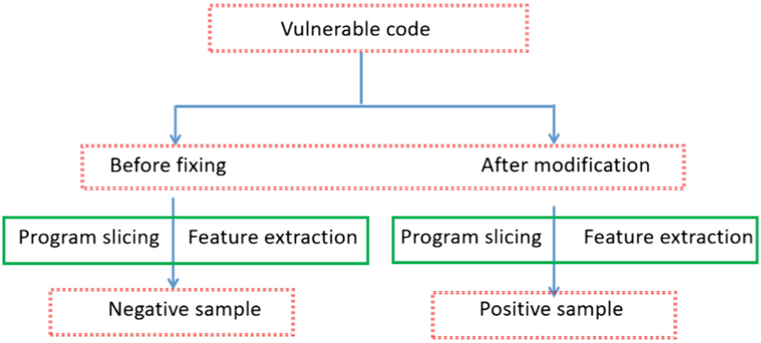
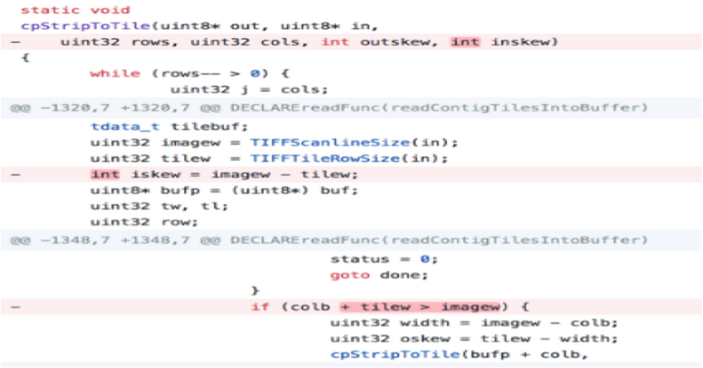


Fig. 2. Construction of positive and negative samples

According to the vulnerability classification, the vulnerability information and its POC are stored in the database to complete the preliminary construction of the vulnerability database. The construction of training positive and negative samples is shown in Fig. 2.

By analyzing the code before and after the modification of the vulnerable program, we can construct program slices through the statements before and after the modification (Fig. 3). Finally, the program slices are used as positive and negative samples for subsequent training.



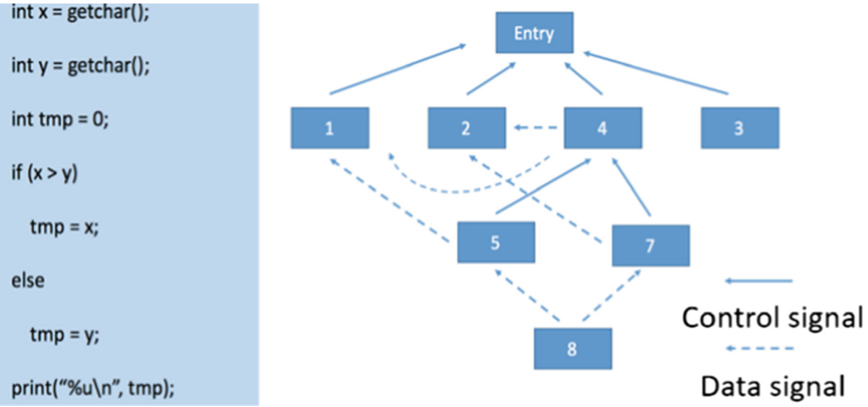
```
 static void
 cpStripToTile(uint8* out, uint8* in,
-    uint32 rows, uint32 cols, int outskew, int inskew)
 {
         while (rows-- > 0) {
                 uint32 j = cols;
@@ -1320,7 +1320,7 @@ DECLAREreadFunc(readContigTilesIntoBuffer)
         tdata_t tilebuf;
         uint32 imagew = TIFFScanlineSize(in);
         uint32 tilew  = TIFFTileRowSize(in);
-        int iskew = imagew - tilew;
         uint8* bufp = (uint8*) buf;
         uint32 tw, tl;
         uint32 row;
@@ -1348,7 +1348,7 @@ DECLAREreadFunc(readContigTilesIntoBuffer)
                                         status = 0;
                                         goto done;
                                 }
-                                if (colb + tilew > imagew) {
                                         uint32 width = imagew - colb;
                                         uint32 oskew = tilew - width;
                                         cpStripToTile(bufp + colb,
```

Fig. 3. Before and after modification of the vulnerable program

3.2 Structural Modeling of Vulnerable Code

(1) Program slice
The code in the vulnerable code library is usually large in scale, and it is necessary to simplify the code with the help of program slicing technology to track the processing of input variables. On the basis of program fragmentation, code modeling can reduce very large amount of calculation and redundant information. This paper adopts the program slicing method based on graph reachability algorithm. The program code is a sequence composed of computer operating instructions in a certain order. Based on this sequence, two types of information can be directly obtained, control flow information and data flow information. In the final analysis, these two types of information are the program execution sequence relationship between the basic blocks of the program and the definition-reference relationship of different statements in the program to the same variable. These two types of relationships are essentially dependencies between the two sentences. Here, the dependency between the two is defined as the control dependency and the data dependency. Control dependence refers to the dependence of the two basic blocks of the program on the program flow. Let $\boldsymbol{G}$ be the control flow graph of the program, where $\boldsymbol{a}$ and $\boldsymbol{b}$ are two nodes in $\boldsymbol{G}$. When $\boldsymbol{a}$ and $\boldsymbol{b}$ meet the following two conditions, then $\boldsymbol{b \to a\_cd}$, which means that $\boldsymbol{b}$ control depends on $\boldsymbol{a}$ (Fig. 4).
① There is an executable path from $\boldsymbol{a}$ to $\boldsymbol{b}$. For all nodes on this path except $\boldsymbol{a}$ and $\boldsymbol{b}$, node $\boldsymbol{b}$ is a necessary node thereafter.
② Node b is not a necessary node of $\boldsymbol{a}$.

By controlling the dependency relationship, the control dependency graph $\boldsymbol{G\_c = (V, C)}$ can be defined. Where $\boldsymbol{V}$ is the combination of all statements in the code, and $\boldsymbol{C}$ is the edge set of the control dependency graph. If there is $\boldsymbol{b}$ control that depends on $\boldsymbol{a}$, then the edges from $\boldsymbol{a}$ to $\boldsymbol{b}$ are added to the edge set. The attributes of the control flow graph refer to the attributes inside the flowchart nodes and the attributes between nodes. The specific parameters are shown in Table 1:



```
int x = getchar();

int y = getchar();

int tmp = 0;

if (x > y)

  tmp = x;

else

  tmp = y;

print(“%u\n”, tmp);
```

Fig. 4. Schematic diagram of program slice

Table 1. Control flow graph properties

Type	Attribute name
Properties inside the node	String constants
	Numeric constants
	No. of transfer instructions
	No. of calls
	No. of instructions
	No. of arithmetic instructions
Attributes between nodes	No. of offspring
	Betweenness

4 Conclusion

In summary, this paper builds a vulnerability database through various means and methods, which can provide a reference for vulnerability rules for preventing a new round of attacks. This paper relies on CVE, Exploit Database (vulnerability database website) and other platforms to automatically grab information on the vulnerability platform through Python crawlers and scripts to obtain all vulnerability information with POC. At the same time, we take the code before and after the modification given by the vulnerability platform as positive and negative samples, and locate the modified position. According to the classification standard of CWE (Common Weakness Enumeration), vulnerabilities are classified into buffer overflow, conditional competition, UAF, information leakage, XSS, SQL injection, CSRF, etc. In order to build a database of vulnerability samples for the study of malicious attacks.

Acknowledgments. This work was supported by State Grid Gansu Electric Power Research Institute Project-Intelligent Recognition and Defense of Intrusion Behavior of Electric Power Information and Physical Fusion System in Cyber Attack Environment (No. 52272219000E).

References

1. Sargolzaei, A., Yen, K., Abdelghani, M.N.: Delayed inputs attack on load frequency control in smart grid. In: Innovative Smart Grid Technologies Conference (ISGT), 2014 PES: IEEE (2014)
2. Sridhar, S., Hahn, A., Govindarasu, M.: Cyber-physical system security for the electric power grid. Proc. IEEE **100**(1), 210–224 (2012)
3. Liu, X., et al.: A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. IEEE Trans. Smart Grid **6**(5), 2435–2443 (2015)
4. NVD: https://nvd.nist.gov/
5. Exploit-Database: https://www.exploit-db.com/
6. OSVDB: http://osvdb.org/
7. Xie, L., Lin, M., Sinopoli, B.: Integrity data attacks in power market operations. IEEE Trans. Smart Grid **2**(4), 659–666 (2011)
8. SARD: https://samate.nist.gov/SRD/index.php
9. Ding, J., Mu, D.: Research on Security Vulnerability Hazard Assessment and Design and Implementation of Standard Vulnerability Library. Xidian University (2016)
10. Zhao, J.X., Guo, S., Mu, D.: DouBiGRU-A: software defect detection algorithm based on attention mechanism and double BiGRU. Comput. Secur. **111**, 102459 (2021)
11. Zhao, J.X., Zhang, X.: Exploring the optimum proactive defense strategy for the power systems from an attack perspective. Secur. Commun. Netw. **2021**, 1–8 (2021)

An Essential Vigilance Analysis on Security of Web Applications

Bin Hu[1], Sohail M. Noman[2](✉), and Muhammad Irshad[3]

[1] Changsha Normal University, Changsha, China
[2] Computer Science Department, Yanshan University, Qinhuangdao, Hebei, China
mn.sohail@hotmail.com
[3] Information Engineering Department, Chang'an University, Xi'an, China

Abstract. Modern web applications are heavily influenced by security advancements. Protecting open web applications is a common term for these programs, which are often referred to as the protection project. A mechanism for establishing security cooperation would be: When providing services through the internet, this is what you'd use. According to a recent study, millions of online services and applications produced using digital technology would be utilized by millions of websites and people every day. They want to adopt a safe method of building web applications that are used by people and people together.

Keywords: Web application · Internet security · Technology management

1 Introduction

Advances in web technology and a changing market climate mean web application in corporate, public, and government agencies are becoming more prevalent today. While web applications can be convenient and effective, there are various kinds of safety threats that can pose significant risks to an Information Technology (IT) infrastructure if not properly managed. The exponential growth in the deployment of web applications has made it more dynamic and distributed. More difficult to protect and manage IT infrastructures. Web applications rely on network-perimeter protection mechanisms, for example, firewalls, to secure IT infrastructure, in one way or another, over more than a decade. In the process of creating web apps, such as injection, more and more attacks target security vulnerabilities, conventional network security measures are not enough to defend applications against new dangers. Threats often arise from untrusted users, non-session protocols, the dynamic design of web technologies, and vulnerabilities in network layers [1–3]. Customer software typically cannot be managed by the owner of the application for web applications. There is also no absolute confidence and processing of the user's feedback from a program running the client. An attacker may create an identity that looks like a lawful client, reproduces an identity of a user, or creates fraudulent messages and cookies. A web-based application may be described as a web browser-based application. It can also be described as a message on the website that would be used to process the data in a simple word processor or table. The web application or

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 92–97, 2022.
https://doi.org/10.1007/978-981-19-3486-5_11

software referencing the person using the application or that is used in the client/server environment, may also be represented as a client-server application. The creators of the web application will be responsible for the development of a client with a particular type of device, which can also be used as a computer system and which will operate on IBM machines or any other user-willing operating system. The browsers used to create a web application which includes Internet Explorer, Firefox, Google Chrome, or a special form of browser that would allow the development developer to access the server-side script combination using languages such as, ASP, ASP.Net, PHP, etc. [3–5].

In the creation of the Web application, the client of the program should concentrate on the information the client receives from the server-side script, which is used as information passed on to another computer from one computer to the next. You may push the application in various ways. Modern technology uses e-mail services from providers including Gmail, Yahoo, Hotmail, etc., which are also known as e-mail customers and allow users to connect via the internet. The users' main concern is that the protection they want is maintained because they want to communicate personal data over the internet and that application providers need to ensure safety in any way that data is protected. [6].

In the production and integration process of the design and the entire application cycle, web application protection should be included. It's a given that the application's final product is a significant component. Safety testing for online applications and testing of new products go hand in hand. Even though web application tools and processes rely heavily on technology features, the human factor is important to their success. As a management team, we must guarantee that stakeholders and contractors as well as project managers and developers are well-informed on the game. [5, 6].

Told the general management team and related risks associated with web security applications, some proposals still impede complete comprehension and take the right decision for an environmental protection network. Some suppliers of security solutions and the willingness on the part of the network professionals to ensure customers and to explain their views to the network's public safety networks help with a range of misconceptions, such as web security applications. Conversely, the particular steps implemented can include sensitive data applications and solutions, credibility, and faults. What does any request have and more technology was initially created to make the details fully free to use, and, unlike web-based applications, there are no built-in authentication systems, management tools, and vulnerabilities in access control. Pirates typically only detect and take advantage of vulnerabilities by a simple web browser authentication. To help you avoid confidential data, you can build SSL technology such as payment details in plain text on the web. SSL site logo for the commercial certificate. Once e-commerce begins, the media are optimistic and the browser locks on the status bar are familiar to consumers. The source of the (faulty) SSL certificate must be readily accessible and safeguarded. [7–12].

Assessment of the papers focused on network creation and network protection and their own mistake based on the analysis studies. The programmers perform all factors of the Internet application. For the following reasons: access to external expertise, save time, cut costs. Rethinking the above scenario may be applied in whole or in part.

2 Security Threats Reviews

1) An attacker injects malicious code into a database or web server from web applications and systems. By tracking the outbound pages such as references to information leaks, businesses can use the Web Application Firewall.
2) It is like an injection attack as well. Malicious scripts were inserted into legitimate websites in cross-site scripting attacks. The development of policies should be focused on the appropriate organizations addressing the issue of input validation.
3) Password improvements and recovery activities, including solid authentication credentials for bad cause management practices. Good authentication and session administration organizations should strive to establish a collection of controls.
4) If the data is not encrypted and the data objects may be exposed through the application, which is called a device design flaw. For example, Uniform Resource Locator (URL), drop list box, Java applications, and JavaScript's are available.
5) A secret zone, including an unexpected token, is suggested to prevent Cross Site Request Forgery (CSRF) from being part of the transaction. At least one token must be unique to each user session on request.
6) A security disorder exists if the device is improperly designed to compromise a Web server, application server, or web application. To lower the effort to create a healthy environment, the mechanism should be automated.
7) To ensure that the risk environment is assessed by organizations and confidential information should be secured. It should also be stored off-site support arranged and encrypted with various keys.
8) The safeguarding of communication programs that often fail to encrypt user information is very important. Even if they can do so, expired or invalid certificates should be checked. To prevent non- Secure Socket Layer (SSL) page requests from SSL Pages, some pages need to be redirected to SSL.
9) The open web framework guides users to malicious websites and transmits them to them. Unsecure data should be forwarded and victims can be sent to malicious websites by the hacker.

3 Evaluation and Critical Reviews

Evaluation and critical analysis include threat modeling, spoofing, denial of services (DDoS), and tampering. [13–19].

1) Security of software now has a significant role to play in the reliability of the systems. Hackers employ various methods to use the software programs for the device and features. The challenges faced by software developers are that they are more concerned first of all with the functionalities and functionality. This approach to development leads to devise manipulation and a hacker may attack. The developer needs to concentrate on the threats listed briefly below to build a safe web app.
2) A spoofing attack happens in a way where the attacker embodies the authentication of identity and attempts to connect with the recipient. To transport fraud on the Internet, it uses bogus websites and emails. An attack happens if the attacker creates

a fake website close to the original website and uses emails to lure the user to the site. If you enter all of your important data, such as your username and password, the hacker stole all information. This technique used by hackers is not known to immature users.

3) The keyway the hackers are using MSN, QQ is to send malicious website links using the chat tool (Ali Wangwang). Marketing campaigns use their customers to connect them to our websites. Emails are transmitted to the phishing site for bank password recovery while all information is transmitted to the hacker account when the user enters his/her correct information. The user must take great care in entering URL, when the user is transferred to a fishery website as if he/she mistakenly types facebok.com, hotmal.com, etc.
4) Spoofing can also be a method in that the hacker can render it impossible by accessing the person's device and attempting to use his credentials to personalize himself from a user's point of view. From a broader point of view, we may say that the individual might recognize the fraud and try to collect the data utilizing cookies and affect all the modification.
5) A distributed denial-of-service (DDoS) attack is enabled to take place in an application where a hacker compromising communication ports is used, which directly affects the data on bandwidth and computers. The application will find the solution in open port mode to protect an attack on the communication port while the application is in the DoS attack mode. We can also make a shift by hopping the app and synchronizing the solution and understanding the protocol between the customer and the server. The harbor and the dos assault might pursue the attacker himself, would be in a vulnerable position.
6) In creating web apps, safety plays a major role in disrupting one of the securities threats the device could obtain, which could be converted into that which could modify/delete the resource without the person's permission. A platform where a user enters the website and wants to modify the files, for example. In other words, the user attempts to use a way that is specifically influenced by the script or the website coding.
7) The use of a connection would be disguised by the user or malicious user and the data would be manipulated. The program will also have the minimum right of even a database affected by the malicious user.

4 Conclusion

Security implementation is just part of the solution. Vigilance is also an essential factor. Even if your system has several safety assurances, you need to track it carefully: monitor the event logs of your system. See if your device is constantly logged into or unnecessary requests are made on your web server. Keep your application server constantly up to date with the most recent security patches or other data sources you might use. It is imperative that upstream Web applications are protected. Customer security requirements and records should be made clear to them, so they don't have any doubts. These issues are critical for consultants. In this case, the supplier argues that the security architects and frameworks of the file security architecture and the security of web applications are following its developers and that the Developer Guide is dedicated and that the guarantee of paying the writing of code or components contained in (OPEN) during the application life cycle has to be made.

Acknowledgment. This paper is funded by the research project of Changsha Normal University (CSSY202109).

References

1. Huang, Y.W., Huang, S.K., Lin, T.P., Tsai, C.H.: Web application security assessment by fault injection and behavior monitoring. In: Proceedings of the 12th international conference on World Wide Web, WWW 2003, New York, USA. ACM Press, pp. 148–59 (2003). https://doi.org/10.1145/775152.775174
2. Nguyen-Tuong, A., Guarnieri, S., Greene, D., Shirley, J., Evans, D.: Automatically Hardening Web Applications Using Precise Tainting. In: Sasaki, R., Qing, S., Okamoto, E., Yoshiura, H. (eds.) SEC 2005. IAICT, vol. 181, pp. 295–307. Springer, Boston, MA (2005). https://doi.org/10.1007/0-387-25660-1_20
3. Gollmann, D.: Securing web applications. Inf. Secur. Tech. Rep. **13**, 1–9 (2008). https://doi.org/10.1016/j.istr.2008.02.002
4. Rafique, S., Humayun, M., Hamid, B., Abbas, A., Akhtar, M., Iqbal, K.: Web application security vulnerabilities detection approaches: a systematic mapping study. In: 2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing SNPD 2015 - Proceedings of the Institute of Electrical and Electronics Engineers Inc. (2015). https://doi.org/10.1109/SNPD.2015.7176244
5. Tripp, O., Pistoia, M., Cousot, P., Cousot, R., Guarnieri, S.: Andromeda: Accurate and Scalable Security Analysis of Web Applications. In: Cortellessa, V., Varró, D. (eds.) FASE 2013. LNCS, vol. 7793, pp. 210–225. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-37057-1_15
6. Sadqi, Y., Maleh, Y.: A systematic review and taxonomy of web applications threats. Inf. Secur. J. (2021). https://doi.org/10.1080/19393555.2020.1853855
7. Attaallah, A., Algarni, A.M., Ahmad Khan, R., Algarni, A.: Managing security-risks for improving security-durability of institutional web-applications: design perspective secure e-transaction view project managing software security risk: a design metrics perspective view project managing security-risks for improving security-durability of institutional web-applications: design perspective. Comput. Mater. Contin. **66**, 1849–65 (2020). https://doi.org/10.32604/cmc.2020.013854
8. Monika, V.: DPLOOP: detection and prevention of loopholes in web application security. In: Gao, X.Z., Tiwari, S., Trivedi, M., Mishra, K. (eds.) Advances in Computational Intelligence and Communication Technology: Proceedings of CICT 2019, pp. 161–172. Springer, Singapore (2021). https://doi.org/10.1007/978-981-15-1275-9_14
9. Łuczak, P., Poniszewska-Maranda, A., Karovič, V.: The process of creating web applications in ruby on rails. In: Kryvinska, N., Greguš, M. (eds.) Developments in Information & Knowledge Management For Business Applications. SSDC, vol. 330, pp. 371–401. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-62151-3_9
10. Sherin, S., Iqbal, M.Z., Khan, M.U., Jilani, A.A.: Comparing coverage criteria for dynamic web application: an empirical evaluation. Comput. Stand. Interfaces **73**,(2021)

11. Shahriar, H., Zhang, C., Talukder, M.A., Islam, S.: Mobile application security using static and dynamic analysis. In: Maleh, Y., Shojafar, M., Alazab, M., Baddi, Y. (eds.) Machine Intelligence and Big Data Analytics for Cybersecurity Applications. Studies in Computational Intelligence, vol. 919, pp. 443–459. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-57024-8_20
12. Zheng, R., Ma, H., Wang, Q., Fu, J., Jiang, Z.: Assessing the security of campus networks: the case of seven universities. Sensors **21**, 312 (2021). https://doi.org/10.3390/s21010306
13. Jan, S., Bin Tauqeer, O., Qudus Khan, F., Tsaramirsis, G., Ahmad, A., Ahmad, I., et al.: A framework for systematic classification of assets for security testing software product line engineering view project DSR project view project a framework for systematic classification of assets for security testing. Comput. Mater. Contin. **66**, 631–645 (2020). https://doi.org/10.32604/cmc.2020.012831
14. Kumar, R., Khan, A.I., Abushark, Y.B., Alam, M.M., Agrawal, A., Khan, R.A.: A knowledge-based integrated system of hesitant fuzzy set, AHP and TOPSIS for evaluating security-durability of web applications. IEEE Access **8**, 48870–48885 (2020). https://doi.org/10.1109/ACCESS.2020.2978038
15. Kumar, R., Irshad Khan, A., Abushark, Y.B., Alam, M.M., Agrawal, A., Khan, R.A.: An integrated approach of fuzzy logic, AHP and TOPSIS for estimating usable-security of web applications. IEEE Access **8**, 50944–50957 (2020). https://doi.org/10.1109/ACCESS.2020.2970245
16. Andrian, R., Fauzi, A.: Security scanner for web applications case study: learning management system. J. Online Inform. **4**(2), 63–68 (2020)
17. Durai, K.N., Subha, R., Haldorai, A.: A novel method to detect and prevent SQLIA using ontology to cloud web security. Wireless Pers. Commun. **117**(4), 2995–3014 (2020). https://doi.org/10.1007/s11277-020-07243-z
18. Goyal, P., Sahoo, A.K., Sharma, T.K., Singh, P.K.: Internet of things: applications, security and privacy: a survey. Mater. Today Proc. (2020). https://doi.org/10.1016/j.matpr.2020.04.737
19. Alenezi, M., Agrawal, A., Kumar, R., Khan, R.A.: Evaluating performance of web application security through a fuzzy based hybrid multi-criteria decision-making approach: design tactics perspective. IEEE Access **8**, 25543–25556 (2020). https://doi.org/10.1109/ACCESS.2020.2970784

A Retrospective Sustainable Glimpse to Improve Project Management via ICT

Bin Hu[1], Sohail M. Noman[2](✉), and Muhammad Irshad[3]

[1] Changsha Normal University, Changsha, China
[2] Computer Science Department, Yanshan University, Qinhuangdao, Hebei, China
mn.sohail@hotmail.com
[3] Information Engineering Department, Chang'an University, Xi'an, China

Abstract. In IT, projects have become more complex as technologies rapidly change and end-users demand greater ease-of-use and flexibility. The most common today's challenging competitive landscape by ensuring that all your technology projects and operations are led by effective digital strategies. But there is complexities and interdependencies of large-scale, long-term, diverse IT projects are among the most challenging issues of IT projects. Effective technology portfolio, program and project management enables clients to see how technology assets are performing, and ensure they're aligned to business strategies. It maximizes the value of your assets, reduce any potential exposure to risk and ensure technology project is delivered on time and within budget.

Keywords: Project management · ICT · Digital strategies · Effective technology

1 Introduction

The management of the projects is a means for preparing, coordinating, encouraging, and managing resources to reach desired objectives [1]. Due to the review of the programs, two separate methods are presented to work together. The entire project life cycle demonstrates the work done to describe, create and produce the product. The project life cycle varies from the lifetime of some goods and services. Project management involves the use of expertise, experience, resources, and strategies in projects to fulfill the project specifications, usually on time and on budget. The development and incorporation of the project management systems, grouped in five separate phases (also called process groups), leads to Project Management including conception, planning, execution, performance, and closing of the project [2].

1) The idea accepted for the project is carefully analyzed to decide whether or not it is useful for the company. The correct decision-making team of the project thus determines the viability of completing either project.
2) The work should be performed in writing for the project definition and preparation to detail the work to be carried out. A proper project team can prioritize the project as well as calculate the projected estimate budget and schedule.

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 98–103, 2022.
https://doi.org/10.1007/978-981-19-3486-5_12

3) All the tasks are initially distributed in the team during the start of the project and the team is aware of the tasks. The important details relating to project management should be a good time to note.
4) The project manager is dependent on the actual schedule to verify the status and success of the project. The project manager must check and change the schedule to ensure that the project is on track in this process.
5) When the project is done. The customer must enjoy the results. To this end, it is important to assess the progress of the project and the study project.

Project management and project management systems differ between organizations. As there are several project components. The ultimate purpose of offering a product and improving a method or solving a problem to ensure that the business continues to benefit. In public administrations, however, the Information and Communication Technology (ICT) [3–5] project management does not employ the full range of procedures, resources, and strategies for project management [6–9]. This is because the contractor is responsible for particular procedures and the project manager of the company is solely interested in quality management and/or approval. Furthermore, there may be project management procedures that are the responsibility of the contractor and do not yield structured project outcomes. They may therefore be regarded as internal to the project management methodology of the contracting company and do not need the attention or involvement of the project manager of the organization. Its knowledge area includes integration, scope, time, cost, quality, communication, risks, and procurement.

1) Integration Management comprises activities and processes which include the various components. Where the project management process is typically specified, organized, and combined
2) Scope management requires a mechanism that determines the job criteria for the project and only the project completion requirement.
3) Time Management covers all procedures relevant to the project's completion time.
4) Cost management requires all procedures involved in project planning and budgeting to be performed in a given budget.
5) Quality control requires responsibility for the project to fulfill its needs and objectives.
6) Communications Management encompasses the mechanism that concerns project information with time, storage, compilation, and final disposal.
7) Risk management consists of a mechanism that deals with the state of project risk management
8) Procurement accounting covers procurement, operation, and management systems results and contracts.

2 Critical Analysis and Future Perspectives

Promoting an improvement culture is an intrinsic and ongoing processing solution that is easy to pay off quickly as this mentality does not only increase the efficiency of individual projects/programs but can also quickly contribute to the overall results [10–14]. The approach to achieving greater success during the entire project life cycle could be improved by critical best practices. But the improvement of the output begins from above. Some further perspective and analysis include: the education of executives, fund seeking, retain the right talent, be realistic, and harmonize the resources.

1) Management recognizes that every day the ICT project manager cannot understand the way good projects are handled at an early age. To educate top management at the same level of project management, it seems that priesthood would have an effect and advantage on small businesses or medium-sized businesses and value consumer concerns and increased Return on Investment (ROI).
2) If you can purchase funds to enhance the management of your project, useful and appropriate value-added solutions, such as training and testing, are essential for the next step. Learning has never been successful in helping training efforts, but it can also help boost long-term returns on investment from the post-evaluation guide. Future learning in your company reveals that a well-trained project manager will potentially make a better decision [15].
3) We have found that even the best ideas always go wrong, without the right people in the right positions or places of work. Does it give a better chance to find a new way, but also to acquire the best talent and improve skills? Four out of five Information Technology (IT) professionals say they would need to quit their jobs to find a higher level, and in their operator, it is doing so in an organized manner according to the research weekly computer.
4) Project management is a long-term objective in horizontal maturity. According to the annual Project Management Office (PMO) by Engineering System International (ESI), the sophistication of project management is a primary predictor of five programmer's/project management officers using only portfolio management. Is a fact when setting improvement goals to better control the standards of the organization on all levels. Moreover, the key problem is that most organizations do not want to use any maturity model to recognize how advanced their project management levels [16]. In reality, the company's plan is seldom formally contacted. But how can an individual be told that the organization does not have the right ideas? Using appropriate modeling; suitable maturity programs instigated in line with company budgets and goals can be used. The main factor is to choose a certain approach to increase maturity and to obtain rapid deliveries.
5) There is still a lot of light in the resources of your company, needing a smart assailant or a balance between them. To focus on the company-wide system, talent, tools, and processes and to build and design project management plans. Can this supply a company? Can it be removed? With business priorities, the business knowledge and maturity can be optimized and cost reduction while increasing efficiency.
6) It is to believe that every project management cycle shall have five phases of development as shown in the Fig. 1 namely project initiation which includes mission, vision, scope, risk and resources; project planning which includes budget statements and road maps; project execution which includes problem management; project control and monitoring; and project closure.

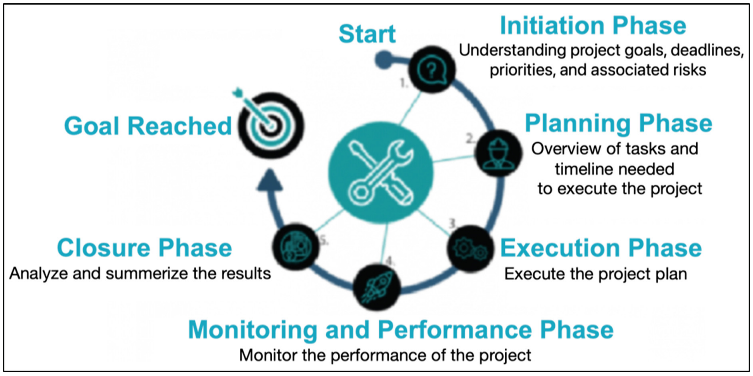

Start
Initiation Phase
Understanding project goals, deadlines, priorities, and associated risks
Planning Phase
Overview of tasks and timeline needed to execute the project
Execution Phase
Execute the project plan
Monitoring and Performance Phase
Monitor the performance of the project
Closure Phase
Analyze and summerize the results
Goal Reached
1.
2.
3.
4.
5.

Fig. 1. The key elements involve in project management cycle.

3 Discussion and Conclusion

Most businesses have shown a variety of advantages of introducing ICTs for project managers as well as a wide range of information to support information flows, simple, fast, and enhanced communication. ICT promotes collaborative events, too. To better prepare for the potential adoption of ICT applications and concerns for the slow acceptance of ICT needs, efficient use or distribution of ICT by organizations must be handled. Due to the diverse perspectives of project team members, challenges may be technological, management, cultural, social, and political. At the business, organization, and people level, holistic studies are required. This is more applicable to the use of ICT in the industry because it has proven difficult for the company to obtain quantity benefits for project management from ICT adoption. However, still some principles need to be concern further for ICT projects to be successful, such as participation, ownership policies, development of capacity, technology involvement, partnerships, alignments, leaderships, competitive environment, sustainability, and consideration of risks.

1) Individuals involved in the project should take part in any stage from the initial monitoring of needs. Participation and demand-driven approach to the increase in ICT activities.
2) They must be locally owned, along with human and organizational capacity growth programs for sustainable development. Only efficient ICT access and use of the elements are effective. Physical access. Local ownership and capacity building can ensure that individuals, communities, and organizations can use and sustain IT structures and use them to increase their income.
3) Technology choices can depend largely on the context. Further exploration is needed for the relationship between the consumer or public and the particular media. By taking the necessary technical decisions to assess the potential of ICTs for the benefit of the disadvantaged.
4) The use of ICT can have spillover effects across agencies and services, which will dramatically increase advocacy and distribution of resources. The need for more

capital and the fact that developing is a matter for all sectors of society, multi-stakeholder collaborations are the difficulty of the challenge, multi-level interaction, and effective response.

5) ICT activities are likely to have greater benefits for the poor, especially those linked to efforts to reduce poverty. more demand-driven development partners have.
6) It is very important to feel owned and led by partner agencies. Although the Pilot Program often provides individuals with successful ICT technology, the initiative needs to be extended institutionally so that coverage and number of participants are increased.
7) A comprehensive information and communication technology infrastructure specifications, including the final mile in investment for service growth, including local content, as well as Open-Source solutions, including freedom of speech, diversity, or the free flow of information.
8) The economy should from the beginning of the planning phase be able to accomplish sustainable projects, with all possible costs and revenue. The problems of social sustainability and the set local ownership and capacity building are also of equal importance. Social and financial security must be considered.
9) The possible and unintended consequences, including how to benefit from ICTs can be unevenly distributed and have even their desired impact, that of raising the economic, social, and cultural split ratio to poverty reduction, must be considered and carefully monitored to encourage interventions.

Acknowledgement. This paper is funded by the scientific research project of Hunan Provincial Department of Education (21C1632).

References

1. Jacoby, M., Usländer, T.: Digital twin and internet of things—current standards landscape. Appl. Sci. **10**(18), 6519 (2020). https://doi.org/10.3390/app10186519
2. Sarkar, D., Patel, H., Dave, B.: Development of integrated cloud-based Internet of Things (IoT) platform for asset management of elevated metro rail projects, Int. J. Constr. Manag. 1–10 (2020).https://doi.org/10.1080/15623599.2020.1762035
3. Hu, B., et al.: A pilot study of global ICT strategy applications in sustainable continuing education. Procedia Comput. Sci. **183**, 849–855 (2021). https://doi.org/10.1016/j.procs.2021.03.009
4. Irshad, M., Liu, W., Wang, L., Khalil, M.U.R.: Cogent machine learning algorithm for indoor and underwater localization using visible light spectrum. Wireless Pers. Commun. **116**(2), 993–1008 (2019). https://doi.org/10.1007/s11277-019-06631-4
5. Akram, A., et al.: A pilot study on survivability of networking based on the mobile communication agents. Int. J. Netw. Secur. **23**(2), 220–228 (2021). https://doi.org/10.6633/IJNS.202103_23(2).04
6. Jamaluddin, R., Chin, C.M.M., Lee, C.W.: Understanding the requirements for project management maturity models: awareness of the ICT industry in Malaysia. In: IEEM 2010-IEEE International Conference on Industrial Engineering and Engineering Management (2010), pp. 1573–1577. https://doi.org/10.1109/IEEM.2010.5674174

7. Piraquive, F.N.D., García, V.H.M., Crespo, R.G.:. Crespo, ICT as a means of generating knowledge for project management. In: The 8th International Conference on Knowledge Management in Organizations (2014), pp. 617–629. https://doi.org/10.1007/978-94-007-7287-8_50
8. Hussein, B., Ngereja, B., Hafseld, K.H.J., Mikhridinova, N.: Insights on using project-based learning to create an authentic learning experience of digitalization projects (2020). https://doi.org/10.1109/E-TEMS46250.2020.9111829
9. Ben Omran, E.E., Pandey, R.K.: Application of ICT in resource management on construction projects in india. Int. J. Adv. Res. Eng. Technol. **11**(9), 687–696 (2020)
10. Huo, C., Hameed, J., Ul, I., Noman, S.M., Chohan, S.R.: The impact of artificial and non-artificial intelligence on production and operation of new products-an emerging market analysis of technological advancements a managerial perspective. Rev. Argentina Clínica Psicológica **29**(5), 69–82 (2020). https://doi.org/10.24205/03276716.2020.1008
11. Hu, B., Irshad, M., Noman, S.M., Tang, X., Awais, M., Muhammad, M.U.: An Economical Design of Rain Water Harvesting and Preservation System via Sensors and Buzzers. In: Proceedings 3rd International Conference on Information Technologies and Electrical Engineering (2020). https://doi.org/10.1145/3452940
12. Waqas Sadiq, M., Hameed, J., Albasher, G., Alqahtani, W., Ibrahim Abdullah, M., Noman, S.M.: Service innovations in social media & blogging websites: enhancing customer's psychological engagement towards online environment friendly products, XXIX, 677–696 (2020). https://doi.org/10.24205/03276716.2020.873
13. Sohail, N., Jiadong, R., Bilal, M., Iqbal, W., Akbar, U., Rizwan, T.: Why only data mining? a pilot study on inadequacy and domination of data mining technology, Int. J. Recent Sci. Res. **9**(10B), 29066–29073 (2018). https://doi.org/10.24327/ijrsr.2018.0910.2787
14. Shah, S., et al.: A Quantum spatial graph convolutional network for text classification. Comput. Syst. Sci. Eng. **36**(2), 369–382 (2021). https://doi.org/10.32604/csse.2021.014234
15. Bin, H., et al.: A pilot study of global ICT strategy applications in sustainable continuing education. Procedia Comput. Sci. **183**, 849–855 (2021). https://doi.org/10.1016/j.procs.2021.03.009
16. Kurniawan, R., Budiastuti, D., Hamsal, M., Kosasih, W.: The impact of balanced agile project management on firm performance: the mediating role of market orientation and strategic agility. Rev. Int. Bus. Strateg. **30**(4), 457–490 (2020). https://doi.org/10.1108/RIBS-03-2020-0022

Research on the Construction of University Data Platform Based on Hybrid Architecture

Jun Zhang, Fenfen Wang(✉), and Jiang Zhou

Hunan Railway Professional Technology College, Zhuzhou 412001, Hunan, China
nnzhang309@foxmail.com

Abstract. With the development of information technology in Colleges and universities, the traditional data integration scheme has been unable to meet the needs of colleges and universities in dealing with massive unstructured and semi-structured data and various types of structured data integration and fusion analysis. Based on this, this paper uses MPP and Hadoop to build university data platform, which can not only meet the needs of deep analysis, complex query and rapid response of structured data, but also meet the performance requirements of massive unstructured data in storage, loading, conversion and other aspects. At last, the paper selects the log data of a university's online behavior, carries out data storage, preprocessing and analysis query, verifies the performance advantages of the platform in massive data processing, and provides a new idea and method for the construction of university data platform.

Keywords: Hadoop · MPP database · Hybrid architecture · Data analysis

1 Introduction

With the rapid development of Internet, cloud computing and Internet of things technologies, the era of big data has come [1]. After years of development, educational informatization has experienced the construction from digital campus to smart campus. After years of construction, colleges and universities have relatively complete management information systems and accumulated a large amount of structured data such as teaching, scientific research, office and assets. In addition, a large amount of unstructured data such as video, audio, images and documents are also distributed in different digital resource management systems such as resource base, knowledge base and archives, There are also a large number of semi-structured data such as log documents, behavior records and location information generated by mobile Internet and Internet of things related systems. These data are the precious wealth of colleges and universities, but these data also have the characteristics of diverse forms, heterogeneous and complex. How to integrate and use these data with high quality and efficiency has become an important problem to be solved in the current information construction of colleges and universities.

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 104–111, 2022.
https://doi.org/10.1007/978-981-19-3486-5_13

2 General Thought

At present, most colleges and universities have established data integration systems for data storage, data exchange and data sharing to varying degrees. The data integration system can collect the structured data in the databases of various business systems in Colleges and universities, integrate and process the data, and provide data exchange and sharing services. However, in the big data environment, the massive non relational data generated by the Internet of things and mobile Internet environment is increasing day by day. When dealing with these massive semi-structured and unstructured data, the traditional data integration solutions can not effectively deal with them [2]. Combined with Hadoop and MPP (massive parallel processor) technology, this paper uses Hadoop and MPP mixed mode to design and implement the university data platform system. Hadoop ecosystem has very superior performance in massive data processing. Therefore, for unstructured and semi-structured data with low value density and huge amount of data, HDFS (Hadoop distributed file system) and MapReduce of Hadoop technology system are used to complete storage and calculation [3], The structured data with high value density of the source business system and requiring frequent reading and writing can be processed by MPP relational database system. Compared with Hadoop, MPP database has obvious advantages in flexible query, complex association summary and in-depth analysis. It is suitable for complex logic processing scenarios such as data mining, self-service analysis and data association in data platform application scenarios. Moreover, MPP database can respond to small-scale queries faster, so as to provide higher throughput. At the same time, the unified Structured Query Language (SQL) provided by MPP database has obvious advantages [4], and there is no need for customized development like Hadoop. It can effectively reduce the migration of original SQL applications and the development cost of new SQL applications. Using hybrid architecture to build university data platform can effectively meet the new needs of university data services. It can not only ensure the migration cost and processing efficiency of the original structured data applications, but also take into account the storage and calculation of massive unstructured and semi-structured data. See Fig. 1 for MPP and Hadoop technology positioning.

3 Architecture Design

The university data platform based on hybrid architecture combines the advantages of Hadoop and MPP and adopts a three-tier structure, including source data layer, data processing layer and data application layer.

(1) Source data layer: this layer is the original data of each system. According to the different data generation mechanisms of the system, the data structure is mainly divided into three categories, namely, the structured data from the traditional business system database and the massive unstructured and semi-structured data (such as security log, Internet behavior data, etc.) generated by various network devices and security devices (Systems) [5].

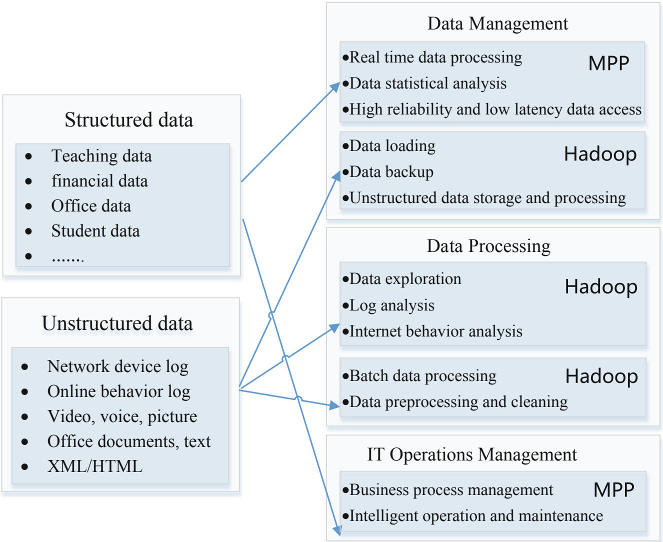


Fig. 1. MPP and Hadoop technology positioning

(2) Data processing layer: this layer is the core layer of the whole data platform, mainly including data ETL processing module, Hadoop data storage and processing module, MPP database module, unified data encapsulation and sharing module. The data ETL processing module extracts data from the source data layer, performs data conversion, loading, association and other operations according to the actual needs, completes data cleaning, removes noise data, generates standard data, and then stores the standard data in HDFS and MPP database of Hadoop respectively. At the same time, the data in Hadoop is calculated and aggregated to form structured data with high value density, and then integrated with the relevant data in MPP database. The results are stored in MPP data to complete the basic data processing process.

(3) Data application layer: in the application scenario of big data, conventional data statistics and data analysis can no longer meet the actual needs of colleges and universities. The data application layer can not only provide routine data query, data report, chart display and other functions, but also meet the needs of colleges and universities for data mining and online analysis. It can cope with different types of users and provide different data services.

(4) Data quality control: metadata is the basic data of the platform. It describes the structure and construction method of data stored in the data platform. With the increase of data, the association and flow of different types of data can easily lead to data confusion. Paying attention to and establishing metadata management can effectively ensure the quality of data integration and processing efficiency. Combine metadata management and data life cycle management, establish and improve data monitoring and data operation and maintenance management, and realize the whole process control of university data quality [6].

4 Data Processing Flow

After using Hadoop and MPP database to build university data platform, the processing of unstructured and semi-structured data has become a key problem to be solved by the platform. In Colleges and universities, the main source of unstructured data is the massive log data generated by network equipment such as network security equipment and Internet behavior management. The general process of processing these log data is: first upload the log data to the HDFS storage system, then use MapReduce to clean the original log data in HDFS, extract the data items concerned by users, and carry out standardized processing [7]; After that, Hive is used for statistical analysis of the cleaned data; According to the actual needs, the statistical results can be imported into the MPP database using the data interworking tool, and users can also view the data details with HBase.

Cleaning the original data with MapReduce is a key link in the processing flow. Firstly, the log data types and structures generated by different equipment or systems are different. If the equipment is replaced or added, new data types may appear, which requires that the MapReduce data preprocessing and cleaning of the university data platform can meet the needs of dynamic configuration. Regular expression has obvious advantages in text data processing. It is flexible, efficient and convenient to use. It is widely used in character search and program compilation. In this paper, different types of log data are described by regular expressions to form a maintainable regular expression rule set. In the process of MapReduce data preprocessing, we first need to determine the type of log data, find out the regular expression description rules in the configuration file according to the class information, then extract the rule, read the specific log data content in HDFS, and complete the matching and parsing of the log data by using the regular expression description rule. Then the parsed data are normalized and output. The processing process is shown in Fig. 2.

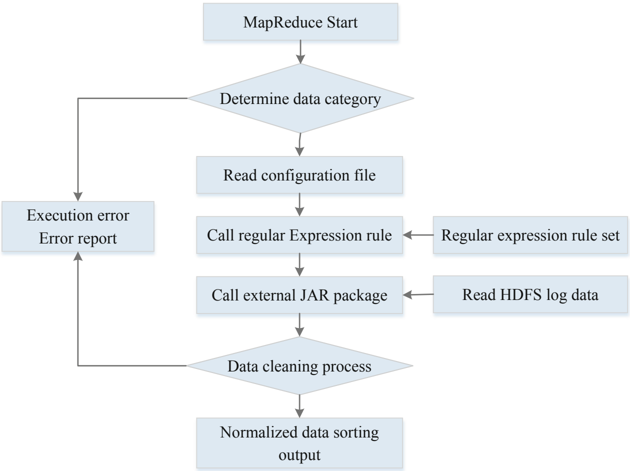


Fig. 2. MapReduce data preprocessing process

MapReduce data preprocessing separates the regular expression describing log data from specific data parsing and cleaning through the configuration file, and carries out unified maintenance and management in the maintainable regular expression rule set. When the log data type changes due to device changes, you only need to update the corresponding regular expression description in the rule set, The main program of MapReduce will not be affected, and there is no additional impact on the whole data preprocessing process. Data cleaning mainly realizes the verification, splitting and replacement of data strings in the target log using regular expressions. At present, most development languages provide good support for regular expressions, which are very convenient to use, and can greatly improve the development efficiency and quality.

5 Data Platform Implementation

A. Platform construction principles and Strategies

Based on the above analysis, the university data platform based on hybrid architecture is built by Hadoop + MPP. In the actual implementation process, different construction principles should be followed according to the different characteristics of MPP and Hadoop. The operation in MPP database is characterized by multi node concurrent calculation, during which there may be loading, data redistribution, replication or data broadcasting between nodes, and finally the result summary. Therefore, MPP database architecture has high requirements for the network quality between nodes, and it is necessary to ensure the point-to-point 10 Gigabit Ethernet bandwidth. In addition, disk capacity evaluation is also an important link in the construction of MPP database. The specific estimation steps are as follows:

(1) The file system space provided after the hard disk of each data node is formatted FD = L(raw disk space) − R (image loss space) − F (format loss space);
(2) Each data node removes the use space of operating system and application software DD = FD-O (operating system space and application software space);
(3) Considering the ratio of file system to database space (T), generally speaking, the two copies are 50%, and the final database space G = DD * T;

Comprehensive formula: G = (L-R-F-O)*T*U = K*KR/C;

In the case of two copies, compression is not considered. The ratio of raw disk space to available data space of MPP database is 3.4:1. If compression is considered, more data can be loaded, but the calculation of compression rate is very different due to different database products and stored data, so it needs to be measured.

A complete Hadoop cluster should contain three role nodes: client, master and slave. The client is deployed in the application node used to interact with Hadoop; The master node is used for cluster management. It mainly communicates with the client and allocates available slave nodes to the client. At the same time, the master will maintain each operation parameter reported by the slave node; Slave node is the executor in Hadoop. The main modules include datanode for storage and nodemanager for parallel computing. In terms of storage capacity estimation, compression ratio, number of copies and redundancy are the main factors affecting storage capacity. The reference estimation formula is: (business estimated data volume * compression ratio * number of copies)/redundancy. When the remaining space of HDFS is small, the performance will be affected. It is recommended to set the redundancy to 30%. The compression algorithms and characteristics that can be used in HDFS of Hadoop are shown in Table 1. However, high compression rate usually means long compression and decompression time, so different compression methods should be selected in different scenarios.

Table 1. Compression algorithm and its characteristics in HDFS

Tool	Algorithm	File extension	Multiple files	Severability	Compression ratio
snappy	snappy	.snappy	Y	Y	About 37%
gzip	DEFLATE	.gz	N	N	About 25%
zip	DEFLATE	.zip	Y	Y	About 22%
bzip2	bzip2	.bz2	N	Y	About 18%
lzop	LZO	.lzo	N	Y	About 35%

B. Platform construction and performance test

The platform is built with X86 physical architecture, and five nodes are allocated for Hadoop cluster, including one control node and four data nodes. The node hardware configuration is Intel Xeon CPU (4 cores), 8 GB memory and 100 g hard disk; The node software environment is CentOS 7 operating system, the Java environment is jdk-8u161-linux, and the Hadoop version is Hadoop 2.8.3. The MPP database is Greenplum 4.3.9.0, which is composed of one master node and four data nodes [8]. The RDBMS used for performance comparison is Oracle 11 g.

The data source selected in this paper is the online behavior log data of a university. There are 12000 students in the school, and the amount of online behavior log data per day is about 2.6 GB. Each log record includes client access IP, user ID, user, access time, request page, request status, size of returned file, jump source, browser, etc. Based on the log data format, you can write the regular expression matching the log as follows:

$$([\wedge]^{*})([\wedge]^{*})([\wedge]^{*})(\backslash[.^{*}\backslash])(\backslash''.^{*}?\backslash'')(-|[0-9]^{*})(-|[0-9]^{*})(\backslash''.^{*}?\backslash'')(\backslash''.^{*}?\backslash'')$$

Using this regular expression, each column of log data can be matched. By matching the log data of one day, a total of 1.26 million valid data records are obtained. The data is loaded into hive, and then the data is loaded into MPP database and Oracle database by means of external tables [9], At the same time, the performance of the three technical schemes in executing multi table Association query is tested and compared, and the results are shown in Table 2 .

From the comparison results of data loading and multi table associated query, the distributed structure has obvious advantages over the traditional database construction method. With the same number of processing nodes and hardware configuration, MPP database has certain performance advantages over Hadoop platform for the data level of millions of records. In general, Hadoop has advantages in processing unstructured data

Table 2. Comparison of data loading and query efficiency of different technical schemes

Technical scheme	Number of nodes	Loading time (seconds)	Query time (seconds)
Hive	5	118.67	45.89
MPP	5	80.019	27.103
Oracle	–	601	152.42

and semi-structured data, especially suitable for application requirements such as data storage and query (detailed order storage and query), data batch processing, unstructured data analysis (log analysis, text analysis), etc. MPP is suitable for replacing big data processing under the existing relational data structure, multi-dimensional data self-service analysis, data mart, etc. Therefore, building a hybrid architecture data platform can give full play to the advantages of MPP and Hadoop in massive data processing and analysis .

6 Conclusion

Use MPP database and Hadoop technology to build a university data platform, store all business data in a centralized way, and complete data cleaning, governance and integration.It effectively solves the problems of low processing efficiency, difficult fusion analysis and slow data loading faced by colleges and universities in the integrated processing of all kinds of heterogeneous data. The mixed construction of university data platform with MPP and Hadoop can not only ensure the analysis efficiency of traditional relational data, but also effectively ensure the storage and computing performance of non relational data, and provide more comprehensive data support for the rational allocation of university resources and scientific decision-making.

Acknowledgements. This work is supported by Industry-university-research Innovation Fund for Chinese Universities for the Science and technology development center of the Ministry of Education (Grant Nos. 2020ITA02058), the Scientific research project of Hunan Provincial Department of Education (Grant Nos. 18C1528).

References

1. Tang, Y., Liu, R.Q., Wang, P.: Design and implementation of college and university big data platform based on Hadoop. Inf. Technol. **24**(5), 105–109 (2019)
2. Deng, H.Y., Lu, S., Cheng, G.: Research on university data integration system based on MPP-Hadoop mixed architecture. Comput. Technol. Devel. **28**(8), 160–163,169(2018)
3. Koop, N.: The marriage of Hadoop and the data warehouse. http://ibmdatamag.com. Accessed 21 Nov 2018
4. Xin, H., Yi, X.H., Chen, Z.: Design of telecom operators' network data sharing platform based on Hadoop+MPP architecture. Telecommun. Sci. **30**(4), 135–145 (2014)
5. Shi, M., Lu, D.H., Qin, T.: Research on big data platform for college students analysis and service. Inf. Technol. **2**(2), 5–10 (2019)

6. Yu, P., Li, Y.: Research on university data governance under the perspective of big data. Mod. Educ. Technol. **28**(6), 60–66 (2018)
7. Ying, Y., Ren, K., Liu, Y.J.: Network log analysis technology based on big data. Comput. Sci. **45**(z2), 353–355 (2018)
8. Dai, Z.Y., Yi, T., Fan, W.F.: Exploration on the selection of enterprise MPP data warehouse China Manag. Informationization **21**(9), 45–47 (2018)

Pingan Campus Intelligent Security Monitoring System Design

Yan Xie[1] and Lang Pei[2](✉)

[1] School of Electronic Information, Hunan University of Information Technology, Changsha, China

[2] College of Computer Science, Wuhan Qingchuan University, Wuhan, China
11286978@qq.com

Abstract. Vigorously developing safe and civilized school construction is the requirement of constructing harmonious society. Under the severe social security situation, it is necessary to establish and perfect the safety and civilized school safety monitoring network system. How to solve the specific situation of campus security and build to meet the needs of the school security monitoring network system prevention function and reliability is an urgent task to be solved. The design of safe campus system should follow the principle of advanced technology, complete functions, stable performance and cost saving, and consider the maintenance and operation factors comprehensively, so as to leave more space for future development, expansion, transformation and other factors. Therefore, the system design content framework is complete, the design scheme is scientific and reasonable, with operability.

Keywords: Campus · Security · System design

1 Introduction

To effectively solve the existing problems of campus security and ensure campus security has become an important part of the work of creating a safe society. It is the goal of security prevention system to use advanced technology to alert possible intrusions in a certain area, to capture, process and record relevant images of alarm events in time, to automatically record the entry and exit of important departments, and to provide effective protection for important areas. According to the national standard of school safety construction, in line with the requirements of high standard and high quality, the intention of the builder is fully reflected in the design, and considering the user's future maintenance, in order to use conveniently, the planning and design of the safety monitoring system.

2 System Design Objectives

General image in the monitoring system can only be stored in the control room of the school, real-time images of the watch inside the school, only if an emergency need to

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 112–120, 2022.
https://doi.org/10.1007/978-981-19-3486-5_14

draw on, the public security department due to obtain first-hand information in the first time distance, therefore, need to establish a corresponding monitoring center in real time monitoring, emergency command, coordination, security management platform system deployed in the monitoring center, Realize unified equipment management, unified user scheduling and other functions, better serve the school management and emergency command. In the design of this system, a second-level monitoring screen is added, which can be assigned to each second-level college or functional department to provide monitoring video access on their office computers, and local videos can also be viewed through mobile APP to achieve the effect of quickly finding and solving problems.

3 Detailed System Design

The system includes five parts: front-end monitoring design, transmission network design, monitoring room design, monitoring center design and alarm system design.

3.1 Front-End Monitoring Design

The front-end monitoring effect is mainly determined by the positioning and selection of the front-end camera. The front-end camera is the original signal source of the entire security defense system and is mainly responsible for the collection of on-site video signals at each monitoring point and transmission to the video processing equipment. The basic requirements of the camera are: clear and true image, adapt to complex environment, easy installation and debugging. In addition, it is recommended that the camera be powered centrally by the UPS to ensure clean power supply and prevent crosstalks. There are also the following requirements in the front-end monitoring design:

3.1.1 Selection of Monitoring Points

Because of the video monitoring system is mainly composed of the front camera, need according to the different environment and application of site selection of different cameras, at entrances to choose the infrared camera and fast ball machine, infrared gun camera is set in the stairs and corridors, the perimeter can choose the infrared camera and fast ball machine, choose in campus outdoor open areas outside spherical camera, etc. Basic Settings and type selection should be determined as described below. As shown in the Fig. 1, the whole campus monitoring system can be divided into three lines of defense:

The first line of defense: campus perimeter, gate and entrance, this part mainly adopts the perimeter guard alarm + perimeter monitoring + entrance and exit monitoring to achieve.

The second line of defense: inside and outside the campus, including the playground and main intersections, this part mainly adopts outdoor fastball cameras.

The third line of defense: all teaching buildings, office buildings, dormitory rooms, etc., are monitored by different types of cameras such as infrared cameras installed at gates, entrances and exits, stairways and corridors.

The basic configuration of the school video surveillance system is shown in the following Table 1:

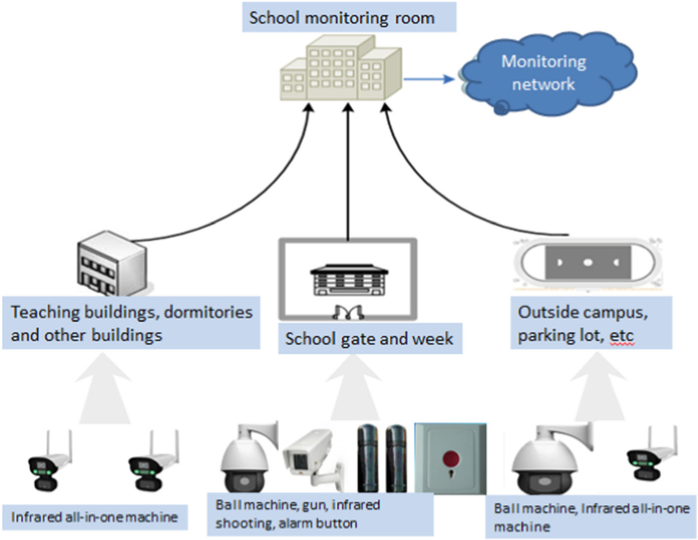

School monitoring room
Monitoring network
Teaching buildings, dormitories and other buildings
School gate and week
Outside campus, parking lot, etc
Infrared all-in-one machine
Ball machine, gun, infrared shooting, alarm button
Ball machine, Infrared all-in-one machine

Fig. 1. Layout of monitoring points

Table 1. Basic configuration table of school video surveillance system

Number	Installation area or coverage area	Type of equipment selected
1	School entrance	Hd camera, HD smart ball machine
2	School office	The alarm button
3	School perimeter	Infrared camera, intelligent ball machine, infrared shooting
4	Outside the campus	Smart ball machine
5	Entrance and exit of each building (including dormitory entrance)	Infrared camera
6	Stairway, corridor	Infrared camera
7	Parking lots, bicycle sheds	Infrared camera

3.1.2 School Entrance and Exit

Campus school of import and export, social workers are often through the school entrance breaking into the school, is the area of the campus security is important, in order to strengthen the management of campus in and out of the vehicle and personnel, should be set up at the gate of the each point, should be considered when installing the camera light dark of night, and asked each to see clear point to point in and out of the vehicle license plate and appearance of personnel, Provide factual basis for campus management. The system designed high-definition network camera and high-definition fastball machine, real-time record school entrance and exit information. The entrance is the first line of defense, should be as far as possible to intercept hidden dangers outside the first line of defense, so in the case of conditions allow (such as network bandwidth and other requirements), should choose high-definition network camera. Horizontal resolution up to 2 M (1600 × 1200), real-time image output, line by line scanning CCD; Capture motion image without sawtooth, using advanced video compression technology, high compression ratio, and processing is very flexible, support SD/SDHC card local storage. As shown in the Fig. 2:

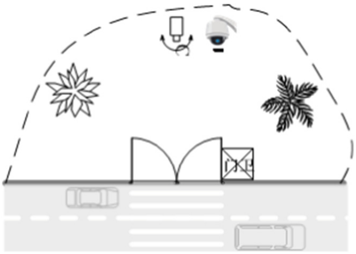


Fig. 2. School arrangement

3.1.3 Campus Perimeter

Most of the walls around the campus are polygonal, but the campus wall is the area with the weakest security protection, in the whole considering wall at night light is very poor, and each can monitor the large range of point to point, at the same time in order to achieve a good level of protection, this system adopt the fastball model camera and infrared camera to cooperate with each other to realize all-round, no blind spot monitoring of 24 h a day. The camera should be installed within the perimeter protection range without blind spots, as shown in the Fig. 3:

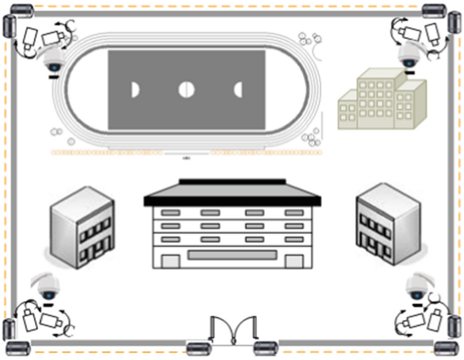


Fig. 3. Perimeter arrangement outside the campus

Due to the large amount of personnel activities outside the campus, it is also easy to have disputes. In serious cases, fights may occur, which seriously affects the normal management of the school. Therefore, it is necessary to set up a monitoring point here. as shown in the Fig. 4:

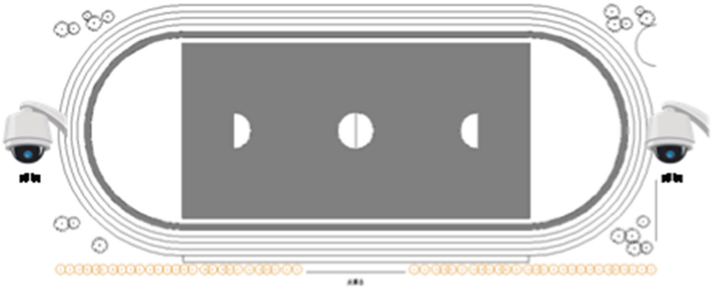


Fig. 4. Campus outdoor layout

Campus outdoor monitoring point design: due to the wide range of outdoor monitoring, it is necessary to adopt integrated intelligent high-speed ball for panoramic monitoring. This scheme adopts high speed intelligent ball machine.

3.1.4 Entrances and Exits of Each Building

The entire campus security is one of the key areas on campus import and export of various building, dormitory doorway, inward and outward quantity, personnel flow too much, in order to strengthen the management of the detached wing in and out of the personnel, should be set up at the gate of the detached wing area, point to point considering requirements can see clear in appearance, this region have all-weather work demand, so choose the infrared camera. as shown in the Fig. 5:

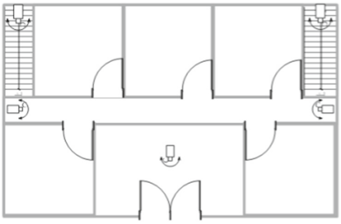


Fig. 5. Building entrance layout

3.1.5 Stairways and Corridors

Staircases and corridors are easy dead ends,In order to strengthen the floor channel management, reduce the labor intensity of the patrol, to monitor real-time monitoring to the floor channel situation, found that warning instance can be processed in a timely manner, to the teaching building floor channel locale monitoring points, to provide factual basis for safety management of the building, the requirements of this region have all-weather work, so choose the infrared camera. as shown in the Fig. 6:

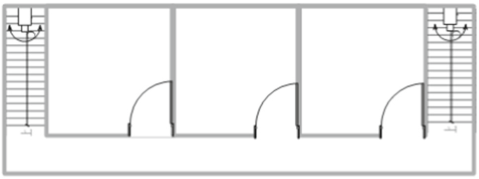


Fig. 6. Stairway, corridor layout

3.1.6 Parking Lots and Bicycle Sheds

The campus parking vehicle area is wide, is the weak link of the whole campus security prevention, in order to manage, reduce labor intensity, let the monitoring personnel real-time monitoring of the parking lot, single carport, found that the police situation can be handled in time. Set up monitoring points in the parking lot and single carport area and select infrared cameras.

3.2 Transport Network Design

In the monitoring system, the transmission of video signal is a very important part of the whole system. Although the cost of this part is small, it is related to the image quality and use effect of the whole monitoring system. Therefore, an economical and reasonable transmission mode should be selected. At present, the most commonly used transmission media in the monitoring system are coaxial cable, twisted-pair, optical fiber and so on. Different transmission modes should be selected for different occasions and different transmission distances.

3.3 Design of Monitoring Room

The monitoring room realizes the unified management and control of the monitoring and alarm system, including digital hard disk video recorder, display system, alarm host and management and network equipment.

3.4 Design of Monitoring Center

In order to realize system management, video storage and image display, the monitoring center arranges servers, storage devices, decoders and TV walls. The video flow direction is as shown in the Fig. 7:

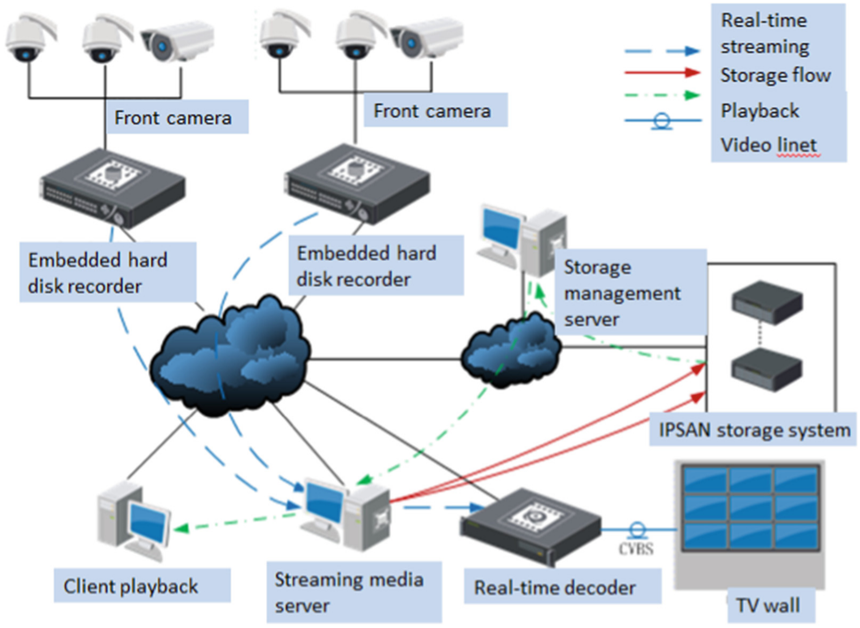


Fig. 7. Monitor central system flow

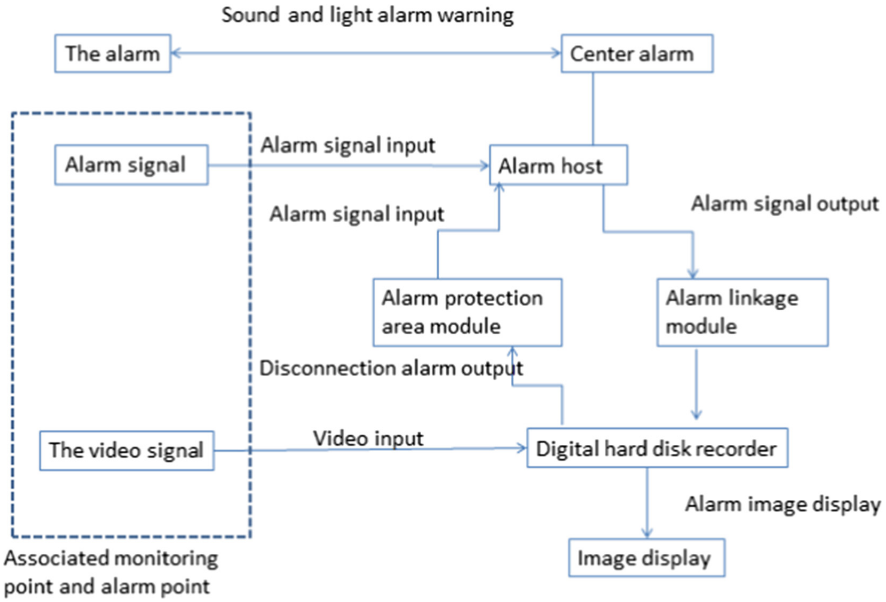


Fig. 8. Alarm linkage

3.5 Alarm System Design

Monitoring and alarm linkage: the alarm host is connected with the alarm input port of the digital hard disk recorder through the alarm linkage module, and the video image linkage through the semaphore. as shown in the Fig. 8:

When the detector detects abnormal conditions, the alarm signal will be transmitted to the alarm host. After receiving the alarm, on the one hand, the alarm host alarms through the sound and light integrated alarm number to notify the staff on duty room, and at the same time, the monitor jumps from the normal multi-screen browsing to the corresponding image of a camera. If it is a ball machine, it can immediately switch to the preset position. All the above actions are transmitted at the speed of current. There is no interval between the determination of alarm and the completion of all response actions, so as to achieve timely response. After the alarm is eliminated, the alarm host will automatically cut off the relay output and the system will return to normal working state.After submitted to the system startup, the secondary monitor screen (that is, the secondary school branch monitoring port) will have the bounce, according to the interface monitoring personnel can control the first time any endpoint security situation, at the same time, the administrator mobile terminal also can receive an alarm, to find and solve problems quickly, foolproof security prevention and control.

4 Conclusion

The system uses analog camera and hard disk video recorder combined with the front-end monitoring storage system, monitoring center centralized management and part of the storage technology route. The second level monitoring screen is added, which can be assigned to each second level college or functional department to provide monitoring video access on their office computers, and local videos can also be viewed through mobile APP to achieve the effect of quickly finding and solving problems. And other equipment specific hybrid DVR combined with hd network camera and analog camera mode of architecture, the system structure with local key protection, mature and reliable, good stability characteristics, using infrared camera and outdoor fastball, meet the requirements of 24-h monitoring, and according to the different parts of the security requirements, Different cameras are arranged to achieve the purpose of all-round monitoring; And the system can also access the anti-theft alarm system, access control system and the original construction of the monitoring system, can achieve unified management, alarm linkage, so as to achieve the purpose of unified coordination command, rapid emergency response.

Acknowledgements. 1. Research results of "Architecture Design and Application research of College Security System Based on Cloud Storage", Scientific research Plan guiding project of Hubei Education Department in 2021, Project number: B2021405.

2. Research results of "engineering ability-oriented software Engineering practice Education training model research", Hubei Province Higher Education Research project, Project number: 2020757

3. The core course "Unstructured database" curriculum reform results –Nosql.

References

1. Qing, G.: Application of modern security technology in library management. New Saf. East Fire Prot. **74** (2010)
2. Xin, C.: Design and analysis of archive security system. Intell. Build. 58–60 (2013)
3. Wong: Construction scheme of campus security system. Chin. Mod. Educ. Equip. **99** (2017)
4. Wang, J.: Application and development of automatic fire alarm monitoring network technology. Fire Technol. Prod. Inf. 5–11(2017)
5. Guangde, L.: A Design Method of Alarm System. Mach. Electron. 72–74 (2017)
6. Xdong, W.: Practical application of intelligent image enhancement technology in the field of security monitoring. Digit. Des. **215** (2019)

An Intelligent Patrol System Based on Edge Data Center Station

Hongbo Ma(✉), Peng Wang, Kaiyi Qiu, Jie Liu, and Zhengchao Zhang

State Grid Information and Telecommunication Co., Ltd., Beijing 100031, China
mahongbo2@sgitg.sgcc.com.cn

Abstract. A centralized intelligent patrol system based on edge data center stations is proposed. By building new digital infrastructures such as edge data center stations, the centralized management of brainy patrols of plant stations in various industry scenarios can be realized. The online intelligent patrol level of each plant and station is improved, and the work pressure of grassroots operation and maintenance personnel is reduced. This kind of system has lower cost, higher deployment efficiency, and better inspection task management than the independent deployment of inspection equipment at the factory site. The system gives full play to the advantages of edge computing technology, improves the level of centralized operation and management of plants and stations, and provides a new inspection mode for the construction of intelligent plant and station management systems.

Keywords: Edge data center · Intelligent inspection system · Factory management

1 Introduction

With the rapid development of industrial intelligence, traditional plant operation and maintenance management models are gradually challenging to adapt to the requirements of lean management. Various industries have vigorously developed a centralized management model based on factories in recent years. State Grid Corporation requires the implementation of the "Equipment-owner system" in 2020, and optimizes the local operation and maintenance mode of the substation due to local conditions, and implements the centralized monitoring operation mode of the substation [1]. As of June 3, 2020, Changqing Oilfield Improvement Eight Factory has completed 17 central stations and 110 unattended stations, achieving full coverage of the construction of the isolated station. The completion of these stations marks the official operation of the first rectification digital center station in Changqing Oilfield [2]. The implementation of centralized monitoring of plants and stations is conducive to improving the intensity of equipment monitoring, the fineness of operation and maintenance management, and the degree of management informatization of each plant and station, which significantly enhances the capability of equipment safety guarantee. At present, each factory station mainly realizes the intelligent inspection of each factory station through the independent deployment of inspection systems and intelligent perception hardware equipment [3, 4]. This model

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 121–128, 2022.
https://doi.org/10.1007/978-981-19-3486-5_15

does not fully consider the centralized management of various plants and stations within a specific range and often requires wise replacement of station-end equipment, which has problems such as low deployment efficiency and high investment costs.

This paper proposes an intelligent inspection system based on the edge data center station for the above problems. The system uses new digital infrastructure, such as edge data center stations, to centrally control remote inspection and station-side analysis services in various industries to solve the contradiction between the growth of different sectors and the shortage of personnel. The application of the system can comprehensively improve the intellectual level of centralized monitoring, operation, inspection, early warning, decision-making and field control. It can be effectively stored in the digital upgrade of the plant and lay a solid foundation for the centralized management of the plant construction.

2 System Architecture and Characteristics

2.1 Overall Structure

This paper proposes an intelligent patrol system based on an edge data center station, which takes dozens of plant stations (such as power plants, water plants, etc.) in different industry application scenarios as the unit. The system uses high-definition video cameras, infrared thermometers, and other sensing devices for production video surveillance installed in key patrol positions as front-end data acquisition nodes. Unlike the traditional construction mode of the intelligent patrol system, the system adds a new layer – an edge data center station on top of all the clusters. The edge data center station analyzes and processes the data collected at all stations, and manages the equipment at all stations in a centralized manner, to realize the intelligent centralized patrol of all subordinate stations and improve the intensive level of management. The system architecture diagram is shown in Fig. 1.

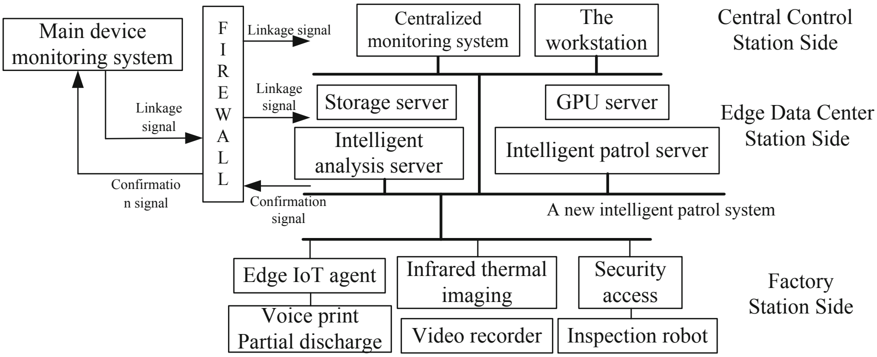


Fig. 1. System architecture diagram

The intelligent patrol system is deployed at the edge data center station, accesses the video data from each plant station in the system, and performs unified analysis of the video data; each plant station's superior centralized management system directly connects to the brainy patrol system.

Each factory station deploys a front-end data-acquisition device, including various perception terminals such as cloud cameras, ball cameras, fixed cameras, micro-cameras and infrared temperature measuring instruments. The video image data is directly transmitted to the edge data center station. By deploying hardware devices such as disk array, database server, application server, online intelligent patrol server and streaming media server and equipped with remote smart patrol system of edge data center station, video data of all stations can be processed, analyzed, displayed and applied in a unified manner.

2.2 Data Architecture

The traditional inspection system is deployed and installed at each station. The storage and analysis process of multi-source data generated by each station is completed at each site. There is a lack of information interaction and linkage between each station in this mode, and effective centralized management cannot be formed. According to the proposed intelligent patrol system architecture and tradition, the difference of the patrol system, this system all stations within the deployment of the terminal equipment of multi-source data are stored in the stations, all without having to upload, edge side patrol demand, intelligent patrol system according to the actual stand side to stand end data acquisition, from station end data analysis, And according to the station inspection results of the intelligent decision, at the same time store the calculation results, and the corresponding result data feedback to the superior centralized management system.

2.3 Disposition Process

The edge intelligent patrol system proposed in this paper can realize the information linkage between operation and maintenance teams, stations and strategies, and effectively improve stations' operation and maintenance management level due to the advantages of architecture and agile information interaction. When the edge data center makes intelligent analysis on the video or sensor data of the station and finds abnormalities, the abnormal data will be transmitted synchronously to the superior centralized management system and the corresponding operation and maintenance team. The excellent centralized management system will further process the anomalous data and issue the task work order to the corresponding operation and maintenance team. At the same time, the operation and maintenance team can first judge the abnormal information based on experience to improve the initiative and flexibility of the fault handling process. When the operation and maintenance team formally receives the task work order or discovers the abnormality after preliminary judgment, it enters the plant to handle the fault and completes the information filing. Such a fault warning disposal process can respond to the fault warning from two aspects of the team and a superior centralized management system, significantly improving the flexibility and reliability of centralized management operation and maintenance of plant and station.

3 Edge Data Center Station

The construction of edge data center station can realize “localization” of computing and storage business of intelligent patrol of each station and has the characteristics of low delay, small scale, physical dispersion, and logical unification [5–7]. In addition, after the completion of multiple edge data center stations, the interconnection between edge data center stations can realize large-scale unified management and resource reuse. The innovative patrol system is deployed in the edge data center station and can realize the remote smart patrol and browse and view the patrol results through the system workstation. The brainy patrol system mainly consists of platform software and a communication protocol stack.

3.1 Platform Software

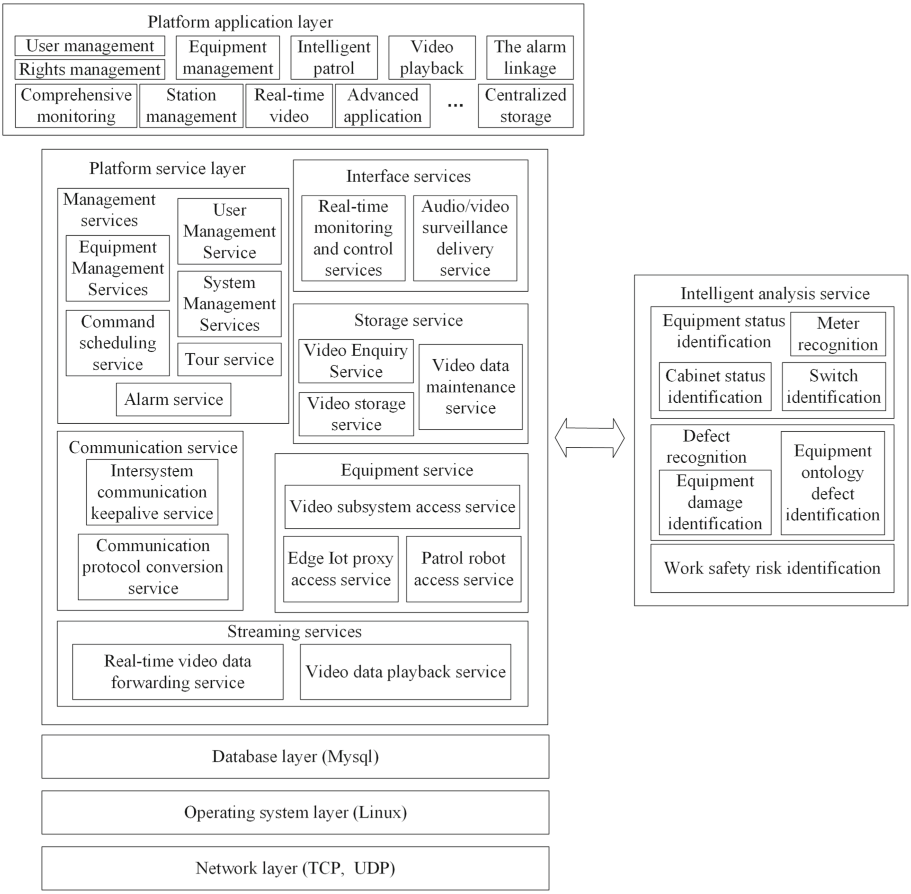

Platform application layer
User management
Rights management
Equipment management
Intelligent patrol
Video playback
The alarm linkage
Comprehensive monitoring
Station management
Real-time video
Advanced application
...
Centralized storage
Platform service layer
Management services
Equipment Management Services
User Management Service
System Management Services
Command scheduling service
Tour service
Alarm service
Interface services
Real-time monitoring and control services
Audio/video surveillance delivery service
Storage service
Video Enquiry Service
Video storage service
Video data maintenance service
Communication service
Intersystem communication keepalive service
Communication protocol conversion service
Equipment service
Video subsystem access service
Edge Iot proxy access service
Patrol robot access service
Streaming services
Real-time video data forwarding service
Video data playback service
Database layer (Mysql)
Operating system layer (Linux)
Network layer (TCP, UDP)
Intelligent analysis service
Equipment status identification
Meter recognition
Cabinet status identification
Switch identification
Defect recognition
Equipment damage identification
Equipment ontology defect identification
Work safety risk identification

Fig. 2. Platform software architecture diagram of edge data center station

The platform software adopts advanced Adaptive Communication Environment (ACE) communication architecture, mainly divided into the network, operating system, data, platform service, and platform application layers. The network layer uses Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) protocols to connect to other systems, the functional system layer uses the Linux system, and the database layer uses the Mysql database. The platform software architecture diagram of edge data center station is shown in Fig. 2.

The platform service layer communicates internally with patrol service and intelligent analysis services to realize the philosophical analysis of patrol video. The device service layer is responsible for interaction with other systems and devices. Communication service realizes communication protocol conversion and survival function; Streaming media service can discover real-time video data forwarding, video playback, video distribution control and other parts. Storage services can realize video query, video storage, video data maintenance and other functions. Interface service can recognize real-time monitoring and control, audio and video monitoring and upload functions; The management service implements device management, command scheduling, user management, system management, patrol management, and alarm management.

The software of this system platform adopts the architecture of "micro-core + plug-in" and supports container technology. All function modules adopt the way of the plug-in to make the core program lightweight. How plug-ins and core programs are automatically assembled into complete applications by containers makes the architecture more open and flexible. The replacement and modification of any functional plug-ins will not affect the core programs and available plug-ins running stably. They can solve the core technology of system customized development and upgrade expansion. Based on the advanced platform architecture and modular software structure, it is convenient to carry out secondary outcomes when implementing future equipment data acquisition applications.

3.2 Platform Software Communication Protocol Stack

The platform software protocol stack is defined as five layers according to the Internet Protocol Address (IP) network, including application, transmission, network, link, and physical layers. The application layer is divided into four parts by function: network management, file and data transmission, signaling, and media transmission, which correspond to different applications. The physical layer defines several possible access modes between subsystems in the system, such as Synchronous Digital Hierarchy (SDH), Ethemet, Token Ring, Fiber Distributed Data Interface (FDDI), World Interoperability for Microwave Access (WIMAX), 3rd Generation Partnership Project (3GPP), and Wide Area Network (WAN), which can select one or more of these modes based on actual requirements. The link-layer protocol consists of Point to Point Protocol (PPP), Point-to-Point Protocol Over Ethernet (PPPOE) and Media Access Control. The network layer includes Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP), IP, Reverse Address Resolution Protocol (RARP), Address Resolution Protocol (ARP), etc. The transport layer includes Stream Control Transmission Protocol (SCTP), TCP, and UDP.

4 System Functions

The new intelligent patrol system can achieve the following functions through the construction of the edge data center station:

(1) Multi-factory station patrol equipment centralized management: The centralized management of multiple plant inspection equipment, including the defect record, operation, and maintenance information, account information, etc. of various plant inspection equipment, which makes it easy for the operation and maintenance personnel to master the critical data of inspection equipment.
(2) Patrol task customized: The system supports the unity of multi-plant inspection tasks and the storage, return, and process unified configuration of the inspection data. The operations team is flexible according to the work demand, timely changes in the inspection plan.
(3) Hidden trouble timely processing and analysis: when a hidden crisis occurs, the edge patrol system will send the fault message to the operation and maintenance management personnel of the plant and station for the first time for timely processing and scheduling and can check the processing progress through the system, grasp the key work in real-time, prevent hidden trouble in the future, and improve the operation and maintenance management level of the plant and station.

4.1 Comprehensive Monitoring

The intelligent patrol system based on the edge data center proposed in this paper can centrally display the overall state of each station in the system. This function mainly includes patrol statistics, equipment statistics, alarm statistics, station micro weather, real-time alarm prompts, and other aspects. This function module can realize centralized statistics and display operation and maintenance status information of different plant and station equipment, and discover more advanced applications based on this function module. Through this function, operation and maintenance personnel in various industries can improve the management level of inspection equipment at each station and improve the overall management efficiency of enterprises.

4.2 Intelligent Patrol

This function can automatically complete the patrol task by automatically calling the preset bit of the station-side patrol device. Through the graphics analysis module in the intelligent analysis application, the patrol picture can be analyzed automatically, and the patrol status can be automatically judged to achieve the goal of camera patrol instead of manual patrol. This function displays the inspection status, inspection task execution, and inspection task display. In addition, it can automatically collect and record the inspection data of various devices and generate inspection reports. The inspection reports include routine inspection, off-light inspection, special inspection, special inspection, and custom inspection reports.

4.3 Device Alarm Linkage

According to the configured linkage scheme, after receiving the device fault signal, the system can automatically link the High Definition (HD) video camera and turn the preset bit to enable linkage recording and intelligent video analysis. According to the above functions, each station's automatic identification of equipment status is realized, and linkage records are saved for inquiry and traceability. In addition, the system provides the alarm management function, which provides unified management of different types of alarm information, facilitating operation and maintenance (O&M) personnel to view alarm information intuitively.

4.4 State Tracking

The system provides the status tracking function for monitored devices. You can discover the faults of devices that need special attention promptly. This function allows you to set the tracking time range for the device that requires status tracking. Within this time range, the preset bits of all cameras belonging to the device must be set as the watch bits, and the video recording subject is the device when viewing the video. In addition, this function accelerates the inspection frequency of analysis items and collects data associated with virtual machines, and stores the collected data.

4.5 Operation Control

This part of the function provides the supervision function of safe operation in the operation area of the station. The camera can be set in the operation area to automatically analyze whether there is an illegal operation in the operation area, improving the security of on-site operation and maintenance. Including but not limited to the following functions:

(1) support through face recognition, automatic control of access control station, launch the door opening action;
(2) Record the information of incoming vehicles through license plate recognition.
(3) Support visual access control through the door to identify visitors and manually open the door remotely.

5 Conclusion

This paper presents an intelligent inspection system based on edge computing technology. In this system, the edge data center station is built on the upper layer of the station in different industry scenarios to realize the intelligent patrol and centralized management of the equipment in other scale stations. Through the innovative architecture, the fault handling pass in each station is moved forward, which supports the operation and maintenance personnel's rapid and timely response and improves the station's operation and maintenance management level.

In the future, based on the edge data center stations in the system mentioned above, the establishment of the critical nodes of the edge computing cluster at the station level can further give play to the advantage of the "key connection" of the edge data center.

References

1. Zeng, Z.: Studage and value exploration of “equipment master system” in the leafily management of substation equipment. Low Carbon World (2019)
2. Yu, Y.: Realistic bone. China Petrol. (2020)
3. Cai, J., Chen, F., Chen, L.: Design of substation intelligent patrol system for automatic update of model. Henan Sci. Technol. (2021)
4. Shen, H.P., Yao, N., Huang, X.L.: Intelligent inspection of substation equipment status based on intelligent vision. Mod. Electron. Tech. (2017)
5. Guo, L.: Key Technology and development trend of edge data center. Inf. Commun. Technol. Policy (2019)
6. Meng, C., Liu, W.L., Yang, Q., Zhao, Y.R., Guo, Y.Y.: Research on operation optimization of edge data center under the background of “multi-station fusion”. Eng. Sci. Technol. **52**, 49–55 (2020)
7. Zhu, X.Y.: Edge Data center: the future of data center under edge computing. Inf. Commun. Technol. Policy (2019)

Alternative BIM Format for Facilitating Substation 3D Design

Xuebin Jiang, Bing Wu(✉), and Jiangqian Huang

Economic Research Institute of State Grid Zhejiang Electrical Power Company,
Hangzhou 310000, China
wu_bing_jyy@sgcc.com.cn

Abstract. Substations are key nodes in the power grid used to change voltage levels between higher voltage and lower voltage for power distribution. Compared with general industrial buildings, substations often have more complex systems of equipment and automatic control and relatively simple building structures. Although the Industry Foundation Class (IFC) has become the prevailing standard for Building Information Modeling (BIM) in many industrial trades, the power distribution companies in China recently seek alternative approaches for recording BIM data in order to improve sharing information across organizations, and a series of domestic industry standard, called Grid Information Modeling (GIM) standards, have been published. This study first summarizes the application of these GIM standards, and then presents the challenges of applying the GIM format in communication and collaboration with other trade in the context of City Information Modeling (CIM). Accordingly, the method of converting the GIM data to the IFC format has been developed. Finally, a case of a real design case of a substation in Zhejiang province has been studied to validate the feasibility of the data format conversion method.

Keywords: Substation · Preliminary design · Building Information Modeling · Industry Foundation Class · Grid Information Modeling

1 Introduction

More stringent requirements have been put forward for power production and distribution. The substation are key nodes of a power grid to realize change of multiple levels of voltage. Most of the newly developed substations are smart substations. A smart substation is a typical smart building [1] that integrated the building system of physical components with the production/automaton system. While the structure and enclosure system establish functional space within an industrial building, various types production systems are allocated in such functional spaces, and also continuously monitored, controlled, diagnosed, and protected by a collection of complex automation systems.

Moreover, compared with commercial or residential buildings, substations often possess more complex systems of production equipment and automation device and relatively simpler building structures. Accordingly, such production equipment as transformers, switchgear, circuit breaker, and lightning arrester as well as various types of

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 129–138, 2022.
https://doi.org/10.1007/978-981-19-3486-5_16

cubicles for automation devices, account for the majority of investment of a typical smart substation. This means that the production and automation systems are the focuses of 3D design modeling of a substation. Furthermore, the design models contribute a major part of information or knowledge shared by the downstream construction, operation and maintenance trades.

The design of smart substations is often a complex and also collaborative process with exchange of rich information among many project participants. An effective approach to deal with the modeling data exchange among multiple engineering disciplines is to utilize the Building Information Modeling (BIM) technology. In this way, BIM plays a crucial role in data exchange and information sharing along the lifecycle of a smart building [2]. The power industry experienced many successful cases along the lifecycle of smart substations. In addition, a number of data exchange protocols, like SV, GOOSE [3], BACnet [4, 5], LonWorks [5], and KNX [6], have been developed for defining the communication networks in the smart buildings.

The information modeling is process restricted by the business process and rules. Specifically, the equipment types cannot be determined in the preliminary design stage since the equipment contracting cannot be executed before the finalization of preliminary design which provide the key criteria of equipment configuration. Although the detailed product models can be acquired from equipment manufactures during the preliminary design stage, such equipment should be represented and evaluated. The 3D model of a production equipment, like a high-voltage transformer, are often used for layout evaluation and collision detection, and its relationships with architectural and structural elements and automation systems should also be abstracted for validation of electromagnetic field effect, fire protection, signal transmission, and monitoring/maintenance space. Therefore, a series of typical production equipment model should be developed and shared by the member companies in the State Grid. This is different from the BIM application of general commercial or residential buildings.

Although a number of previous studies have explored for the incorporation of production/automation system into smart buildings for such purposes as design optimization [7], operation management [8], and fault detection [9]. Later, some research attempted to connect the 2D drawings of building automation system and IFC database [10], but these studies touch very little on the interoperability issue of the Intelligent Electrical Devices (IED) in substation automation systems. The system design of the automation part of substation production system should follow the IEC 61850 standard in order to realize the interoperability of IEDs. The power grid industry experienced a lot of difficulties in using the IFC format to share production equipment models. Nevertheless, little research was carried out into alternative and economic information modeling approaches of the production systems for the preliminary design of a smart substation.

Therefore, the China State Grid seek an alternative information modeling method for the digitalization of its smart infrastructures. This study first briefs the key barriers of applying IFC in the power distribution industry, and then presents the Grid Information Modeling data format, alternative file format for BIM models of production system of smart substations. Moreover, the advantages of GIM application is introduced, and the conversion method from GIM to IFC is also developed to fulfill the data exchange requirement in the broader context of digital twins.

2 Challenges of Applying IFC for Production System of Smart Substation

IFC is initially designed as an exchange format mainly used by software developers for realizing interoperability among various BIM software. The IFC format is an open and neutral file format specification that has been widely accepted by the Architectural, Engineering and Construction (AEC) community. Nearly all BIM software has IFC import and export functions. Therefore, the BIM design of substations utilize IFC as its data exchange format for the architecture, structure, pipe, ventilation, and fire designs. Unfortunately, there are a number of application barriers to meet the need of modeling production and automation system of a substation.

(1) Multiple representation schema of complex equipment

A production equipment in a substation, for example a high-voltage transformer, may require thousands of 3D generic shapes, which are organized in a hierarchy of layers. The seemingly identical model in the CAD viewport can have multiple IFC representation, and the black-box export functions of different BIM modeling software exacerbate the difficulties for the generation of IFC file. This flexible nature of IFC representation make it difficult to consistently represent a complex equipment for the viewpoint of sharing typical equipment models. Meanwhile, the design standard of substation should follow some system decomposition rules that are not abstracted in the existing IFC storage standards. For example, the F1 to F4 levels of system decomposition criteria. In this regard, a strict and one-to-one mapping between the information model and data file representation can really help the exchange flow of equipment model.

(2) Scattered data for one component

The reference between lines of data in an IFC file is very flexible, not requiring sequence or continuity of data lines. Such flexibility for data representation simultaneously increases the cost of sharing typical models, especially when a part of model should be shared and evaluated among a number of parties. The representation of parts or components are often scattered in the IFC file exported by the prevailing BIM modeling software, which make it costly and difficult to combine the parts for sharing partial data of an equipment model. So, an alternative model representation with ease segmentation of equipment model is desired.

(3) Difficult integration of 3D models and 2D schematic drawings

The current BIM design seldom consider the collaboration between the 3D BIM models and the 2D schematic drawings, which is crucial for collaborative design of both production and automation systems of a smart substation. Most of existing schematic design for automation system are presented by 2D drawings data tables with using 2D CAD tools, like AutoCAD and Excel [11]. The focus of 3D BIM design is often layout evaluation and collision detection, while the focus of production and automation design is process flow, information flow, and control logics. Therefore, a protocol of model integration between those two systems should be developed for saving the designers from manual linkage works.

3 Format of Grid Information Modeling

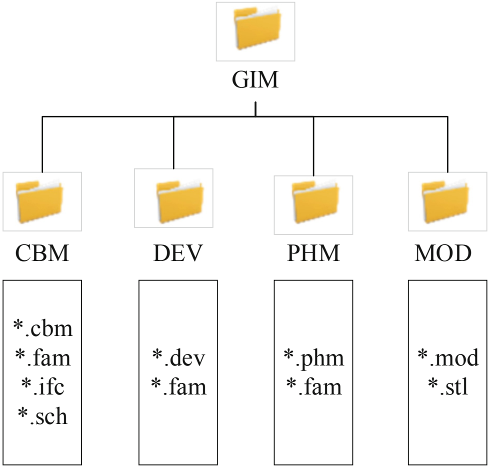


Fig. 1. Structure of a zipped .GIM file

Figure 1 shows the organization structure of. GIM file the three-dimensional design model of the substation project. A .GIM file is essentially a compression file containing of a collection of XML files in hierarchical folders [12]. In the top level, there are four folders, i.e. CBM, DEV, PHM, and MOD. In each folder, there are a number of files of different formats.

The CBM folder, containing files of four formats, i.e. ifc, cbm, sch, fam, describe the different types of systems. The design of architectural, structural, pipe, ventilation, and air conditioning system are represented using the existing IFC2X3 format. At the same time, a cbm file is used to describe a production system of a substation with specific function(s). In the power industry, such production systems are often called primary systems. The fam file comprises a list of key value pairs, each of which defines a single property. Either a cbm or dev or phm file can has an associated fam file with the same name to describe the physical, functional and performance properties of the system element.

Meanwhile, the sch file, itself being a zipped file, describes the logic model, instead of the physical model, of the automation systems that is often called secondary systems in substation design. The sch file contains both spcd file and scd files. The logic model of the secondary system mainly describes a collection of graphic symbols for system node (of representing devices, components, parts ports, and pins) the linkage edges for depicting the connection among those nodes. Moreover, the connection between the primary and secondary system are also defined by the GIM predefined coding rules.

Subsequently, the DEV folder contains dev and fam files for representing an equipment of its constituent sub-devices, while the PHM folder contains phm and fam files for describing the components or parts of a device/sub-device. Lastly, the MOD folder contains files of both mod and stl formats, for depicting the 3D shape of a system element. A mod file represents the parametric model of a shape, while a stl file defines the triangulated boundary of a complex shape. The stl file format has been used in a lot of 3D modeling applications, for example, game and 3d printing. In GIM, the stl format is used for representing complex shapes like NURBS surfaces, and such files can be easily exported from the prevailing CAD software.

In this way, the data size of the GIM is greatly reduced compared with equivalent IFC files, and the segmentation of a GIM file is also much more easier due to its file organization structure.

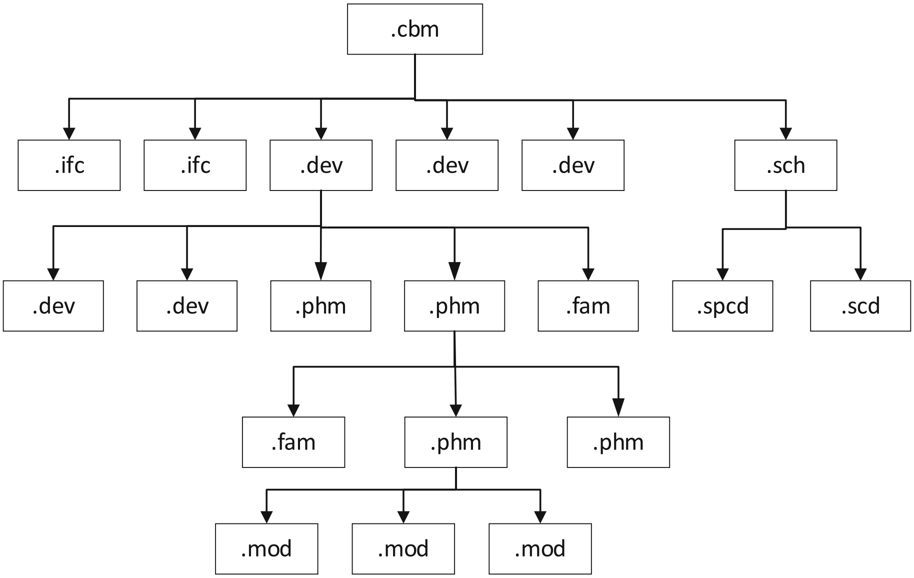


Fig. 2. Reference relationships between Files in GIM

The reference relationships between the files of the aforementioned format are illustrated in Fig. 2. Each cbm file contains a list of dev files, which describe the manufactured devices in the production system. Each dev file describes a device with its detailed composition in terms of its constituent components (phm files) or sub-devices. Those constituent components/parts are depicted by phm files. In this way, the details of a complex device can be hierarchically described. Furthermore, a phm file record a collection of mod files and stl files to describe its 3D shapes.

In addition, either cbm or dev or phm file allows recursive reference. In other word, a high-level cmb file can reference a set of low-level cbm files. Likewise, a high-level dev or phm file can also recursively reference low-level files. In this way, the complex decomposition structure of a production equipment can be modeled with multiple decomposition layers.

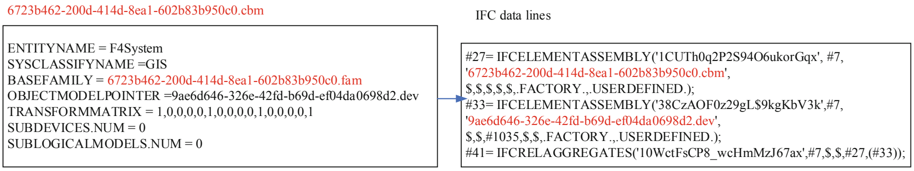
Due to its stricter requirements for predefined system decomposition hierarchy, limited 3D shape definition, and compulsory engineering property assignment, the State

Grid proposes the Grid Information Modeling approach, and until the submission of this study, the development of the GRID has not completed. In particular, the model representation schema of substation secondary (automation) system and its connection with the production system are still in the progress of development. A series of standards for 3D modeling of the primary (production) system have been published in the recent years. Now the GIM format acts as the de facto data exchange protocol for preliminary designs of substations, applied by nearly all the member companies of the China State Grid.

4 Conversion from GIM to IFC

On one hand, application of the GIM format simplifies and enhances the BIM data production, and accordingly improve the data exchange flow among the participants along the project lifecycle. It can significantly save the time and effort of designers and engineers. On the other hand, the GIM data should be converted to the prevailing IFC data format in order to deliver modeling data to the other industries other than the power grid since these companies may not invest the parser or CAD software that can view and evaluate GIM models. Therefore, a series of templates have been developed for the conversion from GIM to IFC.

In the following, the GIM file of a group of three GIS-5000/63 is used for illustrating the conversion template.



6723b462-200d-414d-8ea1-602b83b950c0.cbm

```
ENTITYNAME = F4System
SYSCLASSIFYNAME =GIS
BASEFAMILY = 6723b462-200d-414d-8ea1-602b83b950c0.fam
OBJECTMODELPOINTER =9ae6d646-326e-42fd-b69d-ef04da0698d2.dev
TRANSFORMMATRIX = 1,0,0,0,0,1,0,0,0,0,1,0,0,0,0,1
SUBDEVICES.NUM = 0
SUBLOGICALMODELS.NUM = 0
```

IFC data lines

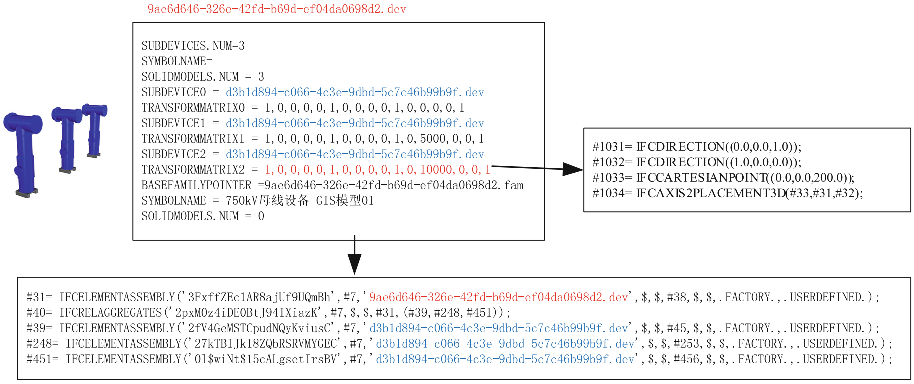
```
#27= IFCELEMENTASSEMBLY('1CUTh0q2P2S94O6ukorGqx', #7,
'6723b462-200d-414d-8ea1-602b83b950c0.cbm',
$,$,$,$,$,.FACTORY.,.USERDEFINED.);
#33= IFCELEMENTASSEMBLY('38CzAOF0z29gL$9kgKbV3k',#7,
'9ae6d646-326e-42fd-b69d-ef04da0698d2.dev',
$,$,#1035,$,$,.FACTORY.,.USERDEFINED.);
#41= IFCRELAGGREGATES('10WctFsCP8_wcHmMzJ67ax',#7,$,$,#27,(#33));
```

Fig. 3. Conversion template for cbm

Figure 3 shows the conversion template by which the cbm can be converted into the partial ifc file. The line #27 in the IFC file indicates the Gas Insulated Switchgear (GIS) (F4 System level) comprises one device represented by the data line #33. The former is represented by the "6723b462-200d-414d-8ea1-602b83b950c0.cbm" file, while the latter 9ae6d646-326e-42fd-b69d-ef04da0698d2.dev. At the same time, the transformation matrix defined in the cbm file is converted into four IFC data lines.

Figure 4 shows the template for integrating three identical integrating three identical GIS-5000/63 devices, respectively for A, B, and C phases, respectively, into one device group represented by the 9ae6d646-326e-42fd-b69d-ef04da0698d2.dev, which is referenced by the cbm file illustrated in Fig. 3. The system decomposition is represented by the IFC class IFCELEMENTASSEMBLY. Figure 4 shows that the 3 sub-device reference the same dev file d3b1d894-c066-4c3e-9dbd-5c7c46b99b9f.dev.

The data line #1034 uses the IFCAXIS2PLACEMENT3D entity to depict a 3D placement coordinate. In detail, the line of #1031, #1032, and #1033 denotes the Z axis,



9ae6d646-326e-42fd-b69d-ef04da0698d2.dev

```
SUBDEVICES.NUM=3
SYMBOLNAME=
SOLIDMODELS.NUM = 3
SUBDEVICE0 = d3b1d894-c066-4c3e-9dbd-5c7c46b99b9f.dev
TRANSFORMMATRIX0 = 1,0,0,0,0,1,0,0,0,0,1,0,0,0,0,1
SUBDEVICE1 = d3b1d894-c066-4c3e-9dbd-5c7c46b99b9f.dev
TRANSFORMMATRIX1 = 1,0,0,0,0,1,0,0,0,0,1,0,5000,0,0,1
SUBDEVICE2 = d3b1d894-c066-4c3e-9dbd-5c7c46b99b9f.dev
TRANSFORMMATRIX2 = 1,0,0,0,0,1,0,0,0,0,1,0,10000,0,0,1
BASEFAMILYPOINTER =9ae6d646-326e-42fd-b69d-ef04da0698d2.fam
SYMBOLNAME = 750kV母线设备 GIS模型01
SOLIDMODELS.NUM = 0
```

```
#1031= IFCDIRECTION((0.0,0.0,1.0));
#1032= IFCDIRECTION((1.0,0.0,0.0));
#1033= IFCCARTESIANPOINT((0.0,0.0,200.0));
#1034= IFCAXIS2PLACEMENT3D(#33,#31,#32);
```

```
#31= IFCELEMENTASSEMBLY('3FxffZEc1AR8ajUf9UQmBh',#7,'9ae6d646-326e-42fd-b69d-ef04da0698d2.dev',$,$,#38,$,$,.FACTORY.,.USERDEFINED.);
#40= IFCRELAGGREGATES('2pxM0z4iDE0BtJ94IXiazK',#7,$,$,#31,(#39,#248,#451));
#39= IFCELEMENTASSEMBLY('2fV4GeMSTCpudNQyKviusC',#7,'d3b1d894-c066-4c3e-9dbd-5c7c46b99b9f.dev',$,$,#45,$,$,.FACTORY.,.USERDEFINED.);
#248= IFCELEMENTASSEMBLY('27kTBIJk18ZQbRSRVMYGEC',#7,'d3b1d894-c066-4c3e-9dbd-5c7c46b99b9f.dev',$,$,#253,$,$,.FACTORY.,.USERDEFINED.);
#451= IFCELEMENTASSEMBLY('01$wiNt$15cALgsetIrsBV',#7,'d3b1d894-c066-4c3e-9dbd-5c7c46b99b9f.dev',$,$,#456,$,$,.FACTORY.,.USERDEFINED.);
```

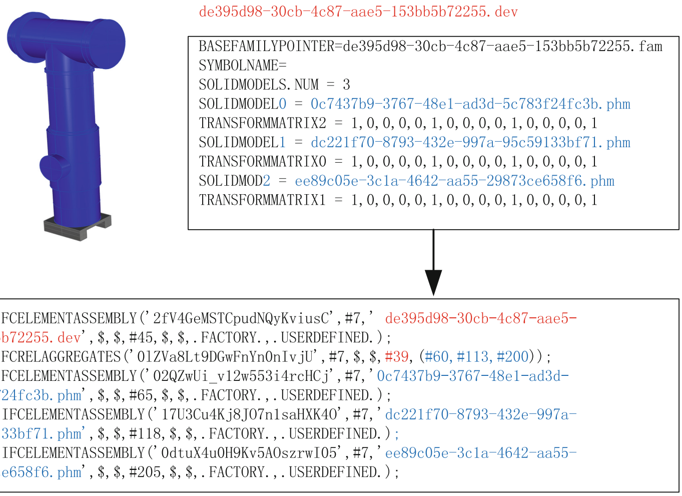
Fig. 4. Template for aggregation of sub-devices

x axis, and origin of the aforementioned 3D coordination. The Y axis is not defined in the IFC file since it can be derived from the Z and X axes.

For the transformation matrix 2 in Fig. 4, its equivalent IFC coordinate can be calculated by the following formula:

$$S_{3\times 4} = \begin{bmatrix} 0\,0\,0\,1 \\ 0\,0\,1\,0 \\ 1\,0\,0\,0 \end{bmatrix} * \begin{bmatrix} 1 & 0\,0\,0 \\ 0 & 1\,0\,0 \\ 0 & 0\,1\,0 \\ 10000 & 0\,0\,1 \end{bmatrix} = \begin{bmatrix} 10000 & 0\,0\,1 \\ 0 & 0\,1\,0 \\ 1 & 0\,0\,0 \end{bmatrix} \qquad (1)$$

The first row in the resultant matrix indicates the origin of the newly 3D coordination derived from the transformation matrix in the mod file. The second row defines the Z axis, and the third row X axis.



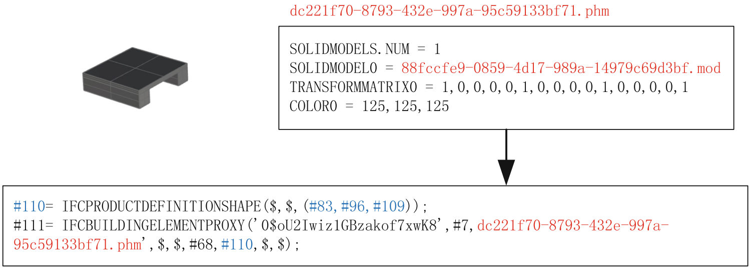
de395d98-30cb-4c87-aae5-153bb5b72255.dev

```
BASEFAMILYPOINTER=de395d98-30cb-4c87-aae5-153bb5b72255.fam
SYMBOLNAME=
SOLIDMODELS.NUM = 3
SOLIDMODEL0 = 0c7437b9-3767-48e1-ad3d-5c783f24fc3b.phm
TRANSFORMMATRIX2 = 1,0,0,0,0,1,0,0,0,0,1,0,0,0,0,1
SOLIDMODEL1 = dc221f70-8793-432e-997a-95c59133bf71.phm
TRANSFORMMATRIX0 = 1,0,0,0,0,1,0,0,0,0,1,0,0,0,0,1
SOLIDMOD2 = ee89c05e-3c1a-4642-aa55-29873ce658f6.phm
TRANSFORMMATRIX1 = 1,0,0,0,0,1,0,0,0,0,1,0,0,0,0,1
```

```
#39= IFCELEMENTASSEMBLY('2fV4GeMSTCpudNQyKviusC',#7,' de395d98-30cb-4c87-aae5-
153bb5b72255.dev',$,$,#45,$,$,.FACTORY.,.USERDEFINED.);
#59= IFCRELAGGREGATES('01ZVa8Lt9DGwFnYn0nIvjU',#7,$,$,#39,(#60,#113,#200));
#60= IFCELEMENTASSEMBLY('02QZwUi_v12w553i4rcHCj',#7,'0c7437b9-3767-48e1-ad3d-
5c783f24fc3b.phm',$,$,#65,$,$,.FACTORY.,.USERDEFINED.);
#113= IFCELEMENTASSEMBLY('17U3Cu4Kj8J07n1saHXK40',#7,'dc221f70-8793-432e-997a-
95c59133bf71.phm',$,$,#118,$,$,.FACTORY.,.USERDEFINED.);
#200= IFCELEMENTASSEMBLY('0dtuX4u0H9Kv5A0szrwI05',#7,'ee89c05e-3c1a-4642-aa55-
29873ce658f6.phm',$,$,#205,$,$,.FACTORY.,.USERDEFINED.);
```

Fig. 5. Conversion template for dev

Subsequently, the a single GIS device is illustrated in Fig. 5 that presents the template for converting a dev file into the equivalent IFC codes. There are three parts composed in the GIS device, represented by three phm files.



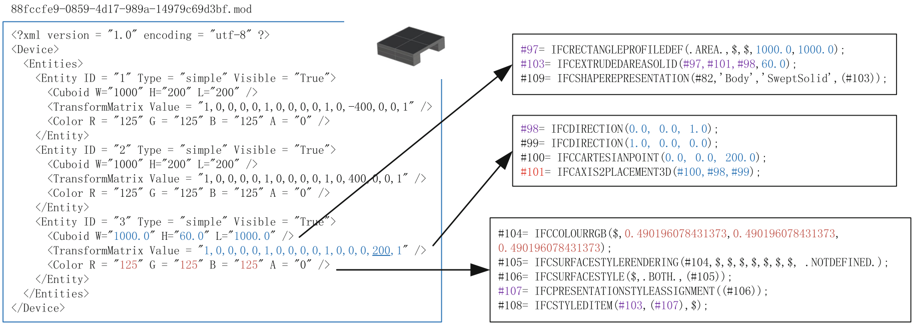
dc221f70-8793-432e-997a-95c59133bf71.phm

```
SOLIDMODELS.NUM = 1
SOLIDMODEL0 = 88fccfe9-0859-4d17-989a-14979c69d3bf.mod
TRANSFORMMATRIX0 = 1,0,0,0,0,1,0,0,0,0,1,0,0,0,0,1
COLOR0 = 125,125,125
```

```
#110= IFCPRODUCTDEFINITIONSHAPE($,$,(#83,#96,#109));
#111= IFCBUILDINGELEMENTPROXY('0$oU2Iwiz1GBzakof7xwK8',#7,dc221f70-8793-432e-997a-
95c59133bf71.phm',$,$,#68,#110,$,$);
```

Fig. 6. Conversion template for phm

Figure 6 illustrates the template for converting a phm file to the corresponding IFC data lines. The line #111 indicates that a phm file can be represented by the IfcBuildingElementProxy, which is a subclass of the IfcBuildingElement. All building elements are derived from the IfcBuildingElement. The 7th attribute of the IfcBuildingElementProxy is the shape description of the building element (the base of the GIS device), and this shape is further represented by the IfcProductionDefinationShape entity, which references three boxes described by #83, #96, and #109, respectively.



88fccfe9-0859-4d17-989a-14979c69d3bf.mod

```
<?xml version = "1.0" encoding = "utf-8" ?>
<Device>
  <Entities>
    <Entity ID = "1" Type = "simple" Visible = "True">
      <Cuboid W="1000" H="200" L="200" />
      <TransformMatrix Value = "1,0,0,0,0,1,0,0,0,0,1,0,-400,0,0,1" />
      <Color R = "125" G = "125" B = "125" A = "0" />
    </Entity>
    <Entity ID = "2" Type = "simple" Visible = "True">
      <Cuboid W="1000" H="200" L="200" />
      <TransformMatrix Value = "1,0,0,0,0,1,0,0,0,0,1,0,400,0,0,1" />
      <Color R = "125" G = "125" B = "125" A = "0" />
    </Entity>
    <Entity ID = "3" Type = "simple" Visible = "True">
      <Cuboid W="1000.0" H="60.0" L="1000.0" />
      <TransformMatrix Value = "1,0,0,0,0,1,0,0,0,0,1,0,0,0,200,1" />
      <Color R = "125" G = "125" B = "125" A = "0" />
    </Entity>
  </Entities>
</Device>
```

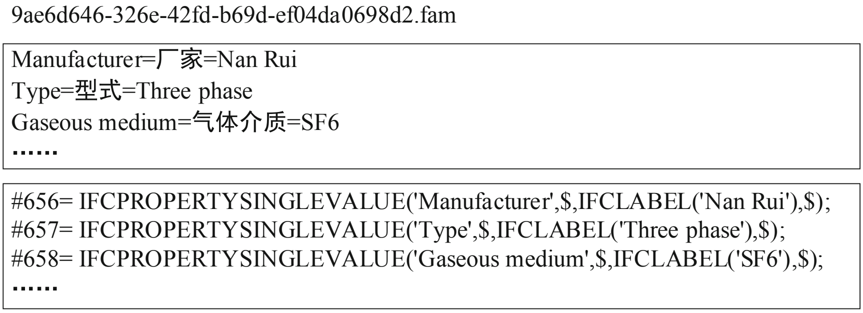
```
#97= IFCRECTANGLEPROFILEDEF(.AREA.,$,$,1000.0,1000.0);
#103= IFCEXTRUDEDAREASOLID(#97,#101,#98,60.0);
#109= IFCSHAPEREPRESENTATION(#82,'Body','SweptSolid',(#103));
```

```
#98= IFCDIRECTION(0.0, 0.0, 1.0);
#99= IFCDIRECTION(1.0, 0.0, 0.0);
#100= IFCCARTESIANPOINT(0.0, 0.0, 200.0);
#101= IFCAXIS2PLACEMENT3D(#100,#98,#99);
```

```
#104= IFCCOLOURRGB($,0.490196078431373,0.490196078431373,
0.490196078431373);
#105= IFCSURFACESTYLERENDERING(#104,$,$,$,$,$,$,$, .NOTDEFINED.);
#106= IFCSURFACESTYLE($,.BOTH.,(#105));
#107= IFCPRESENTATIONSTYLEASSIGNMENT((#106));
#108= IFCSTYLEDITEM(#103,(#107),$);
```

Fig. 7. Conversion template for mod

Figure 7 provides the template for converting the mod file into IFC data lines. The mod file in figure includes three cuboid shapes for the base. Using the top slab as an example, the Lines #97, #103 and #109 defines the box 1000 mm * 1000 mm * 60 mm. In particular, the line #103 employs the IfcExtrudedSolid entity for extruding the rectangle profile 1000 mm * 1000 mm, and the extrusion direction is defined by #98, and height, 60mm, is defined by the 4th attribute of the IfcExtrudedSolid entity. The shape is finally defined by #109 IfcShapeRepresentation entity for further reference by IfcBuildingElementProxy entities (See Fig. 6). In addition, the conversion of transformation matrix and color is also presented in Fig. 7. Due to the limited writing space, the conversion process is not elaborated here.



```
9ae6d646-326e-42fd-b69d-ef04da0698d2.fam

Manufacturer=厂家=Nan Rui
Type=型式=Three phase
Gaseous medium=气体介质=SF6
……

#656= IFCPROPERTYSINGLEVALUE('Manufacturer',$,IFCLABEL('Nan Rui'),$);
#657= IFCPROPERTYSINGLEVALUE('Type',$,IFCLABEL('Three phase'),$);
#658= IFCPROPERTYSINGLEVALUE('Gaseous medium',$,IFCLABEL('SF6'),$);
……
```

Fig. 8. Conversion template for fam

Figure 8 illustrate the template for converting fam into IFC data lines. Each line of the fam file has three items splited by "=". The first two item are property name in both English and Chinese, while the third item is the value of the property. IfcPropertySinglеValue entities are used for representing those properties. For example, the word "厂家" is the Chinese translation of the English word "Manufacture". Similarly, "型式" is the Chinese translation of "Type", and "气体介质" is the Chinese translation of "gaseous medium".

5 Conclusions

Compared with general industrial buildings, substations often have more complex production and automation systems and relatively simple building structures. Although the Industry Foundation Class (IFC) has become the prevailing BIM standard for commercial and residential buildings, the power grid companies in China met several challenges in applying IFC for describing the production and automation equipment for smart substations. So they recently developed the GIM file format as an alternative BIM format for storing the BIM design results of production and automation devices. Meanwhile, the template for converting the GIM to the IFC format has been developed with case studies. Finally, a case of a real design of a substation in Zhejiang province has been studied to validate the feasibility of the data format conversion method. The real case study indicates that the GIM format can greatly reduce the size of 3D design model and improve the data exchange among the project participants.

Acknowledgments. This research was supported by Research on Key Technologies for 3D design and engineering data based on new generation power system (Grant No. 5200-201956106A-0-0-00). We thank Dr. Yuanbin Song from Shanghai Jiao Tong University who provided insight comments that greatly assisted the writing of this paper.

References

1. Bolchini, C., Geronazzo, A., Quintarell, E.: Smart buildings: a monitoring and data analysis methodological framework. Build. Environ. **121**, 93–105 (2017). https://doi.org/10.1016/j.buildenv.2017.05.014
2. Aram, S., Eastman, C.: Integration of PLM solutions and BIM systems for the AEC industry, In: Proceedings of the International Symposium on Automation and Robotics in Construction, vol. 30, p. 1. IAARC Publications (2013). https://doi.org/10.22260/isarc2013/0115
3. Grid T&D: What is GOOSE Messaging?. https://www.igrid-td.com/smartguide/iec61850/goose-messaging/#:~:text=GOOSE%20(IEC%2061850). Accessed 01 June2021
4. American Society of Heating, Refrigerating and Air-Conditioning Engineers, BACnet - The New Standard Protocol. http://www.bacnet.org/Bibliography/EC-9-97/EC-9-97.html. Accessed 01 June 2021
5. Phongchit N.: What is the difference between BACnet, Modbus and LonWorks? https://www.setra.com/blog/what-is-the-difference-between-bacnet-modbus-and-lonworks. Accessed 01 June 2021
6. KNX: A brief introduction to KNX. https://www.knx.org/knx-en/for-professionals/What-is-KNX/A-brief-introduction/. Accessed 01 June 2021
7. Oti, A.H., Kurul, E., Cheung, F., Tah, J.H.M.: A framework for the utilization of building management system data in building information models for building design and operation. Autom. Constr. **72**, 195–210 (2016). https://doi.org/10.1016/j.autcon.2016.08.043
8. Gao, X., Pishdad-Bozorgi, P.: BIM-enabled facilities operation and maintenance: a review. Adv. Eng. Inform. **39**, 227–247 (2019). https://doi.org/10.1016/j.aei.2019.01.005
9. Dong, B., O'Neill, Z., Li, Z.: A BIM-enabled information infrastructure for building energy fault detection and diagnostics. Autom. Constr. **44**, 97–211 (2014)
10. Tang, S., Shelden, D., Eastman, C., Pishdad-Bozorgi, P., Gao, X.: BIM assisted building automation system information exchange using BACnet and IFC. Autom. Constr. **110**, 103049 (2020)
11. Zhang, J., Seet, B.C., Lie, T.: Building information modelling for smart built environments. Buildings **5**(January), 100–115 (2015). https://doi.org/10.3390/buildings501010026
12. China Electricity Council: Interactive specification for the three-dimensional design model of power transmission and transformation project (2020)

Research on Digital Twin Modeling for Virtual Power Plant

Bingsen Xia[1], Yuanchun Tang[1], Zhimin He[2,3](✉), and WenQin Lin[1]

[1] State Grid Fujian Economic Research Institute, Xiamen 361000, China
[2] Global Energy Interconnection Research Institute Co., Ltd., Nanjing 210003, Jiangsu, China
825097034@qq.com
[3] State Grid Key Laboratory of Information & Network Security, Beiqijia, Beijing 100000, China

Abstract. In recent years, distributed photovoltaics, decentralized wind power, new types of loads, electric vehicles, etc. have been connected to the power grid on a large scale, and the distribution network has become more active, with strong volatility, and large peak-valley differences. The management and coordination of distributed resources has become more prominent. Interaction puts forward higher requirements. This paper first investigates the main requirements of virtual power plants for the access of various new energy sources on the load side; then based on the virtual power plant resource aggregation access requirements and the key technologies of the power Internet of Things, the virtual power plant access layer system architecture is proposed; in order to further realize the power flow, The integration of information flow and business flow, optimize the allocation of power resources, improve the quality of service, build a communication network with a hierarchical control architecture based on the intelligent decision-making needs of virtual power plants, and establish a cloud-side-end integrated digital twin model, thereby integrating the digital twin The technology is highly integrated with the physical power grid to provide a means for real-time control of the adjustable resources of the virtual power plant.

Keywords: Virtual power plant · Digital twin · Resource aggregation

1 Introduction

1.1 Research Background

Driven by the strategy of clean replacement and electric energy replacement, distributed photovoltaics, decentralized wind power, new types of loads, electric vehicles, etc. are connected to the grid in a wide range [1]. As of the end of 2020, there have been 1.69 million distributed photovoltaic power stations nationwide with a total capacity of more than 40 million kilowatts connected to low-voltage stations [2]. At the same time, electric vehicles and charging facilities have entered a stage of rapid development, and the transition from 120–180 kW (300 A) fast charging to 350–400 kW (400 A) high-power charging. The characteristics of active distribution network, strong volatility,

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 139–146, 2022.
https://doi.org/10.1007/978-981-19-3486-5_17

and large peak-valley difference are becoming more prominent, which puts forward higher requirements for the management and coordination and interaction of distributed resources.

As an effective means to solve the problem of multiple distributed power grid connection, virtual power plant uses advanced control, metering, communication and other technologies to aggregate distributed power sources, energy storage systems, controllable loads, electric vehicles and other different types of distributed energy sources [3]. It realizes the coordinated and optimized operation of multiple distributed energy sources through a higher-level software architecture. It can aggregate distributed power sources outside the scope of the microgrid, and is more conducive to the rational and optimized allocation and utilization of resources, and realizes the integration and distribution of resources. It gradually participates in the operation of distributed energy in the wholesale electricity market as an aggregate entity, and is a smart grid. It is an important way to achieve interaction and intelligence on the energy supply and demand side.

In recent years, with the increasing acceleration of the intelligentization process, in order to realize the interaction and integration of the physical world and the information world, the concept of "digital twin" has emerged at the historic moment, and has continued to evolve and develop rapidly, which has greatly promoted many industries [4]. In the process of continuous improvement and development of the concept of digital twins, researchers have mainly carried out research on digital twin modeling, physical information fusion and service applications, focusing on analyzing the relationship between digital twins and related industries, establishing virtual models, and relying on twin data Convergence analysis, service application guidelines, etc. The connotation of the digital twin is to construct a digital twin. Its final form is a complete and accurate digital description of the physical entity, which can be used to simulate, monitor, diagnose, predict and control the physical entity. Although digital twins are currently less used in the power industry, learning from their applications in aerospace, automobile manufacturing, oil and gas pipelines and other industries will help promote the construction and development of the energy Internet.

1.2 Purpose and Significance

With the rapid development of power substitution on the user side, there are more and more flexible resource types, wider geographical distribution, more frequent information interaction, and control and protection extending to the terminal. However, due to the lack of simulation analysis and evaluation tools for flexible resource aggregation and regulation capabilities At the same time, there are problems such as difficulty in controlling on-demand time delay of dispatching communication network, difficulty in precise adjustment of users and difficulty in coordinated output, resulting in insufficient capabilities such as dynamic scalability of virtual power supply capacity, real-time power control or fast frequency modulation response, and it is difficult to meet the needs of new power systems, adjust the power supply's multiple time and space scales and flexible backup requirements.

1.3 Research Level at Home and Abroad

The development of virtual power plants is divided into three stages: the first stage is an invitation-based stage. In the absence of an electricity market, the government department or dispatching agency will lead the organization, and various aggregators will participate to jointly complete the invitation, response and incentive process; The second stage is a market-based stage. After the electric energy spot market, ancillary service market and capacity market are completed, aggregators will participate in these markets in a similar manner to physical power plants to obtain revenue; the third stage is a cross-space autonomous dispatch virtual power plant, Adopting "cloud edge collaboration + Internet of Things technology + AI + digital twin" technology to aggregate more diverse, more environmentally friendly and adjustable resources on the user side, presenting a wider and wider geographical distribution, more frequent information interaction, and extended control to the end. Situation, with the characteristics of dynamic expansion of energy grid, software definition of information network, plug-and-play of terminal resources, intelligent and credible power transaction, operation control elimination and coordination, and strengthen the ability of fast, accurate and flexible frequency modulation, and the business form is more diverse. Become an important configuration form of the energy Internet of large cities in the future.

In fact, there have been many cases of research on virtual power plants in Western countries. Each country has its own characteristics. Japan and Germany use energy storage and distributed power as the main body of virtual power plants, while the United States focuses on controllable loads, and the scale has accounted for more than 5% of peak loads.

The construction of virtual power plants in China is in a stage of rapid development. The State Grid Hai Power, Jibei Power, and Jiangsu Power have implemented virtual power plant technology demonstration applications around demand-side response, clean energy consumption, and friendly interaction between source and grid.

2 Key Technology Research

The core of the virtual power plant is the integration of source, network, load, storage, sales, and service. The power source can be traditional thermal power, or emerging wind power, photovoltaic, and biomass power generation; it can be either large-scale centralized power generation or Distributed scattered power generation can also be other forms of energy such as cold, heat, energy storage, and controllable load. Virtual power plants connect them in series, based on the Internet and big data, cloud computing, artificial intelligence, digital twins and other technologies to realize self-regulation of power generation and electricity consumption and maintain an instantaneous balance. Digital twin, as an indispensable technical means in the research of large-scale and flexible resource aggregation control simulation technology and platform research and development, is a key technology to promote the digital construction of power grids and an important measure for the digital transformation of the State Grid. The company is concerned. At present, some provincial companies have started exploring digital twin-related projects in substations and other scenes, collecting sensor data in real time, monitoring the operating status of the system, deducing the operating situation of the equipment system, and providing decision-making solutions for feedback control. Digital twin technology is used in virtual power plants, which can assist virtual power plants to effectively aggregate distributed power generation, controllable loads, energy storage systems, electric vehicles and other resources scattered in a large area of the city, and realize the interconnection and sharing of various distributed resources. Better play to its economy and flexibility in the energy market.

2.1 Business Needs Analysis

The main requirement of the virtual power plant for the access of various new energy sources on the load side is to build an intelligent network system with intelligent judgment and adaptive adjustment capabilities for unified access to the grid and distributed management of multiple energy sources. Real-time monitoring and collection, and adopting the most economical and safest transmission and distribution method to deliver electric energy to end users to realize the optimal configuration and utilization of electric energy, and improve the reliability of grid operation and energy utilization efficiency. It needs to integrate the core technology of the Internet of Things, integrate the data in the system, and optimize the operation and management on the basis of an open system and a shared information model.

In addition, the construction of virtual power plants must achieve a high degree of integration of power flow, information flow, and business flow while meeting the overall requirements of smart grids that are strong, reliable, cost-effective and efficient. Virtual power plants have a large number of rich and diverse applications on the business side, and different applications have different requirements for information. Therefore, application middleware is needed to adapt between the diversity of virtual power plant applications and the versatility of the bearer platform to perform intelligent information processing such as data filtering, data mining, and decision support. At the same time, the virtual power plant needs to have strict user identification, verification, and authentication systems for user access so that different users can enjoy different levels of Internet of Things services. Finally, because the virtual power plant directly participates in the grid operation business, it greatly affects the safe and stable operation of the power system, which requires the virtual power plant to have extremely high safety and reliability.

In addition, in terms of architecture, the existing virtual power plant architecture generally uses chimney-style independent business access, which cannot meet the needs of data sharing and unified management and control in the new form. In order to cope with the changes in smart grid terminal access and business requirements, it is urgent to conduct further research on this basis, build a virtual power plant terminal integrated access network architecture based on the aggregate communication gateway, and realize the "integrated access, edge intelligence, and unified construction of the terminal". Model, safety protection".

2.2 Access Layer Architecture

The access layer architecture is divided into four sub-layers from the bottom to the top: on-site collection components, the business terminals, on-site communication network and aggregation communication gateway.

1) On-site collection components include various sensors, sensor components and on-site collection terminals.
2) The business terminals include various components, operating systems and hardware chips.
3) On-site communication network includes power communication network, such as: industrial Ethernet, EPON, etc., 2G/3G/4G/5G, wireless local area network, wireless wide area network, etc.
4) The aggregation communication gateway layer is composed of a software layer and a hardware layer. It is used to connect the service terminal and the platform layer to realize various functions such as data collection, edge computing, encryption, and transmission of the terminal. Among them, the software layer includes service terminal open interfaces, security, unified model adaptation, edge computing, data processing and other modules, provides standard communication protocol adaptation, and provides standardized communication interfaces to support the flexible access of multiple service terminals. The security module considers four aspects of data, business, network, and equipment, and provides security guarantees based on technologies such as abnormal traffic analysis, equipment evaluation, and channel intrusion detection.

At the same time, the convergent communication gateway has multi-source data fusion computing capabilities, protocol analysis capabilities, and behavior analysis capabilities. It supports the implementation of the SG-CIM interface of the State Grid standard, and communicates with the platform layer through interfaces such as Restful and Web Service; the hardware layer includes computing storage The hardware resource layer such as hardware and the communication adaptation layer that provides standardized wired and wireless communication interfaces, and can flexibly adapt to local, remote, wired, wireless, public network, private network and other network communication channels according to business needs. The converged communication gateway is the “hub” between the field communication network and the wide area communication network. It is used to connect the service terminal and the platform layer. It mainly realizes “unified access, edge intelligence, multi-dimensional perception, unified modeling, security protection, resource Orchestration”. The various business terminals deployed on site are connected to the aggregated communication gateway through the on-site communication network, and finally connected to the aggregated control platform of the virtual power plant.

2.3 Cloud-Side Collaborative Digital Twin Model

On the load side of the virtual power plant, renewable energy services, building energy efficiency services, supply-demand interactive services, smart electricity services, and low-carbon transportation services all put forward a higher level of diversified information collection capabilities and flexible network access capabilities [5]. The high-performance communication network can interconnect a large number of distributed energy harvesting devices, energy storage devices, and various types of loads and other energy nodes, and needs to provide wireless ubiquitous access to the energy Internet client side; in the field of regulation, the collection of communication network carried

For business and control services, the requirements for communication are "high reliability, high speed, and low latency", and it requires the complete state monitoring of the power grid generation, transmission, distribution and DC system within 60 ms; the defense control of important disturbances and faults within 300 ms, With load classification control and equipment-level precise adjustment capabilities. Therefore, from the perspective of the communication network, both the access side and the backbone network side have put forward higher performance requirements for the communication network.

The overall functional architecture of the virtual power plant aggregation control communication network layer includes: access network, transmission network, data communication network, business network, synchronization network, etc. The communication network layer connects the aggregate communication gateway of the terminal layer downwards, and connects the virtual power plant control platform of the platform layer upwards. It mainly realizes the functional goals of "wide coverage and large connection, low latency and high reliability, heterogeneous network integration, and network customization". Construct a "space, space, and ground" coordinated and integrated ubiquitous communication network, and finally form a "network as a service" power communication network, which fully meets the goal of "full-time-space communication coverage", and provides multi-source access, low-latency control, and high-speed communication for virtual power plants. Bandwidth transmission provides support.

The digital twin model of the cooperative operation and control system superimposed on the network transmission characteristics is shown in Fig. 1. The physical part of the semi-physical simulation model consists of analog fans, energy storage cabinets, load cabinets, electric heaters, inverter air conditioners, fixed frequency air conditioners, etc. The energy storage cabinet is used to simulate nodes with charging and discharging characteristics such as batteries and electric vehicles, and the load cabinet is used to simulate loads such as lighting loads. The physical objects are equipped with an information collection unit and an energy collection unit. The information collection unit is used to exchange data with the virtual power plant's digital twin. The energy collection unit is used to collect the energy change curve of a single component, and then aggregate large-scale controllable resources to obtain. The electromechanical controllability of the virtual power plant.

The core of the cloud-side digital twin model is the information flow transmission and energy deployment of the digital twin of the virtual power plant. Through actual components for information collection and energy collection, the virtual power plant digital twin interacts with the actual components and the digital world in two-way data, which can realize analog distributed power, storage batteries, super capacitors, analog loads, electric vehicles, lighting loads, variable frequency/fixed frequency The interconnection and expansion of various primary equipment such as air conditioners controls the transmission, distribution, load management and power of the power system through modeling and simulation analysis, combined with large-scale and flexible resource aggregation to control network communication transmission, and realizes the overall system data monitoring of the virtual power plant, Data collection, equipment management, power control, power quality monitoring, energy efficiency evaluation, power plan setting, economic analysis, etc.

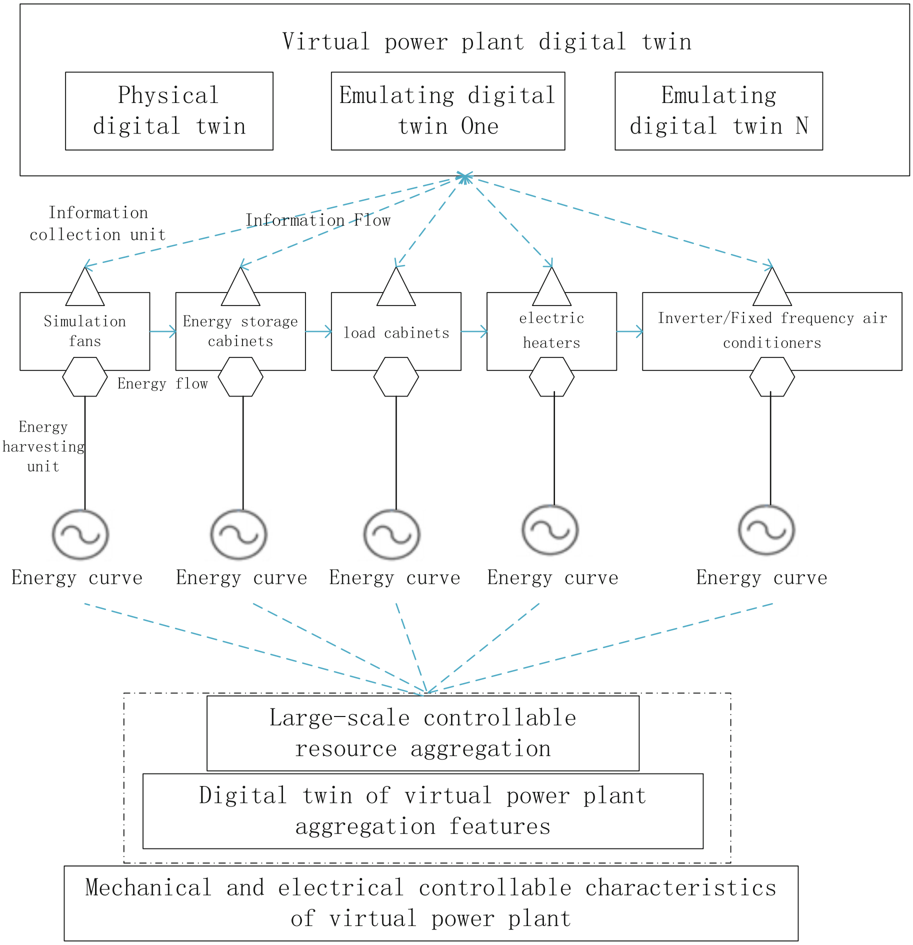

Virtual power plant digital twin
Physical digital twin
Emulating digital twin One
Emulating digital twin N
Information collection unit
Information Flow
Simulation fans
Energy storage cabinets
load cabinets
electric heaters
Inverter/Fixed frequency air conditioners
Energy flow
Energy harvesting unit
Energy curve
Energy curve
Energy curve
Energy curve
Energy curve
Large-scale controllable resource aggregation
Digital twin of virtual power plant aggregation features
Mechanical and electrical controllable characteristics of virtual power plant

Fig. 1. System digital win model.

3 Conclusion

The communication network is an important support for the aggregation and regulation of virtual power plants, which can ensure the real-time and accurate acquisition of massive electricity/non-electricity information of the smart grid, provide a comprehensive high-speed transmission channel for cloud computing and big data, and provide diverse and reliable mobile applications Data and network support. Therefore, the communication network is crucial to the development of virtual power plants.

This paper first investigates the main requirements of virtual power plants for the access of various new energy sources on the load side; then based on the virtual power plant resource aggregation access requirements and the key technologies of the power Internet of Things, the virtual power plant access layer system architecture is proposed; in order to further realize the power flow, the integration of information flow and business flow, optimize the allocation of power resources, improve the quality of service, build a communication network with a hierarchical control architecture based on the intelligent decision-making needs of virtual power plants, and establish a cloud-side-end integrated digital twin model, Therefore, digital twin technology is integrated, which is highly integrated with physical power grid, providing a means for real-time control of adjustable resources of virtual power plant.

Acknowledgments. This work is supported by Science and Technology Project of State Grid Corporation of China (Research on key technologies of virtual power plant based on digital twin, No. B3130N2100V).

References

1. National Energy Administration's 13th Five-Year Plan for Electric Power Development 2016–2020. http://fjb.nea.gov.cn/news_view.aspx?id=27538(2016)
2. Cheng, Y., An, S.: Analysis of active load's interaction response behavior. Autom. Electric Power Syst. **37**(20), 63–70 (2013)
3. Yavuz, L., Önen, A., Muyeen, S.M., et al.: Transformation of microgrid to virtual power plant - a comprehensive review. IET Gener. Transm. Distrib. **13**(11), 1994–2005 (2019)
4. Fan, H.D.: Research on architecture and system deployment of intelligent power plant based on digital twin. Chin. J. Intell. Sci. Technol. **1**(3), 241–248 (2019)
5. Wei, X., Pan, S.G., Wang, B., Sun, H.B., Guo, Q.L.: Review on virtual power plant resource aggregation and collaborative regulation using cloud-tube-edge-end architecture. J. Glob. Energy Interconnect. **3**(6), 539–551 (2020)

Research on Construction Scheme of Coastal Water Transportation and Communication Network Based on 5G Technology

Fuzhai Wang, Shanshan Wang(✉), Zhongli Yi, Jinyu Zhao, and Rong Sun

Transport Planning and Research Institute of MOT, Beijing 100020, China
949095839@qq.com

Abstract. From the perspective of user demand, 4G/5G network can meet the construction needs of coastal traffic communication network at present and in a certain period. Therefore, based on mobile (broadband) communication system, this paper proposes two construction schemes of coastal water traffic communication network, namely public-private combination scheme and self-building private network scheme. The two schemes are compared and analyzed from the perspectives of convention, technical characteristics, investment scale, Op generation and maintenance and resource control. Finally, this paper puts forward that public-private combination scheme is better than self-building private Net-work Scheme.

Keywords: Coastal water · Communication network · 5G technology

1 Introduction

Fifth generation mobile communication system (5G) is an upgrade of 4G. As a new generation mobile communication system being vigorously promoted by the state, it is a high integration of new wireless access technology and existing wireless access technology. The main application scenarios of 5G include enhanced mobile broadband, large-scale machine communication and high reliability and low delay communication [1–3]. Its main performance indicators are shown in Table 1.

Compared with 4G system, 5G technology has the following advantages:

- The transmission rate is large, 10–100 times that of 4G, up to 10 Gbps.
- The network capacity is large, and the number of devices that can be connected is 1000 times higher than that of 4G.
- The end-to-end delay is small and can reach the millisecond level.
- The spectrum efficiency is high, which is 5 to 10 times higher than that of 4G in the same bandwidth.
- Wider frequency band.

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 147–154, 2022.
https://doi.org/10.1007/978-981-19-3486-5_18

Table 1. Main performance indexes of 5G system

Performance index	Value
User experience rate	0.1–1 Gbps
Connection number density	10^6/km^2
End-to-end delay	1 ms
Mobility	500 km/h
Peak rate	20 Gbps
Flow density	10 Mbps/m^2

4G/5G networks can meet the construction needs of coastal transportation and communication networks at present and in a certain period, and various communication equipment and terminals are very rich, which can effectively control the network construction investment at this stage [4–6]. In addition, 4G will exist in parallel with 5G for a long time in the future. Users can reasonably choose the network system according to their actual needs.

Coastal water area (broadband) communication network is a new construction field. Considering the coverage of 4G and 5G technology, link bandwidth, technology development trend and macro environment, 5G technology is recommended to build coastal water area traffic communication network in this paper.

2 System Architecture

Based on the state-of-the-art 5G communication technology, this paper proposes a mobile (broadband) communication network architecture, which is divided into four layers: wireless access layer, access layer, switching layer and business application layer. The flat structure shortens the time delay of the user interface, reduces the complexity of the system, reduces the interface types, and reduces the corresponding interactive operations within the system. The contents and functions of each layer are as follows.

2.1 Wireless Access Layer

The wireless access layer, also known as the sensing layer, mainly includes various terminals and acquisition devices used by users.

2.2 Access Layer

The access layer mainly includes building base band unit, remote radio unit, antenna and other equipment, which mainly provides base station and user end signal access in the signal access system. Specifically, in order to achieve good coverage, base station equipment usually needs to be deployed on islands and reefs. The base station on the island and reef can relate to the shore-based network by microwave communication, and the land interworking can be realized through point-to-point transmission. The main coverage scenario is to extend the network coverage along the coast (Island) line. Ships in this area can be interconnected with the shore end in real time to maintain voice and video communication and ensure the fluency and real-time of communication. When the maritime law enforcement personnel perform the boarding inspection task around the ship, they complete the voice and video communication in the on-site workflow.

2.3 Switching Layer

The switching layer mainly includes EPC core network, OMC network management and HSS user signing server to complete user management, authentication access, routing transmission of user data, and effective transmission of terminal data and audio and video services in the system.

2.4 Business Application Layer

The business application layer is the highest layer in the system, which is closest to the user. It mainly includes multimedia cluster dispatching equipment, monitoring display equipment (encoding and decoding, audio and video matrix, etc.), geographic location information auxiliary equipment (BeiDou Navigation Satellite System, Global Positioning System, etc.) and audio and video storage equipment.

3 System Composition

Coastal mobile (broadband) communication system is mainly composed of core network subsystem, transmission subsystem, base station subsystem and user terminal subsystem. The core network realizes the overall control of the transmission operation of the whole network. The user terminal accesses to the core network through the wireless base station and transmission line, and then realizes communication connection and information interaction with other devices. Figure 1 shows the overall composition of the system.

3.1 Core Network Subsystem

The core network subsystem mainly realizes the functions of network core management, service scheduling processing and network management. It is the core service processing part of mobile (broadband) communication system. Firstly, the core network management functions include cluster user management, cluster services, data services, public services and so on. Secondly, the service scheduling processing function can realize the real-time display of the current state of each terminal. The dispatcher can conveniently carry out various scheduling operations and realize the communication and scheduling of voice, instruction and video. Finally, the network management function is used to realize the management of relevant network layer equipment. Its physical structure includes server, operation and maintenance terminal, alarm terminal, operation terminal, alarm box, management console and some networking equipment.

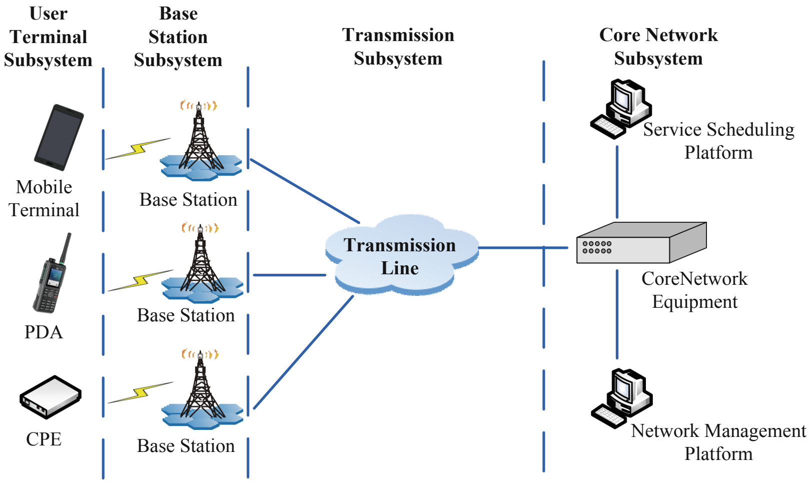


Fig. 1. Composition diagram of mobile (broadband) communication system.

3.2 Transmission Subsystem

The transmission line is used to realize the interactive transmission of data between the base station and the core network. Generally, in order to achieve longer distance coverage, mobile (broadband) communication base stations often need to be built on islands without network conditions, and microwave transmission mode needs to be adopted.

3.3 Base Station Subsystem

The base station subsystem is the front end of the mobile (broadband) communication system. Its main function is to realize the communication connection with the user terminal in the specified frequency band, and connect it through the standard interface and core network to meet the professional cluster, high-speed data and other business needs of the user terminal.

3.4 User Terminal Subsystem

User terminal subsystem refers to various terminals for users to access mobile (broadband) communication system, including a variety of devices, such as Personal digital assistant (PDA), Customer premise equipment (CPE), etc.

In addition, in order to better perform the water distress and safety communication guarantee work under the jurisdiction, timely handle the water emergency communication and special communication guarantee tasks, and provide sea related users with navigation information services, Hydrometeorological Information Services, alarm services, industry supervision and other functions.

4 Construction Scheme

This section aims to detail two construction modes of mobile (broadband) communication system. First, the public-private combination scheme relies on the infrastructure, equipment and frequency point resources of the operator's existing core network, transmission network and wireless network to build a mobile (broadband) communication system to meet the communication needs of coastal traffic. Second, the self-building private network scheme relies on the existing communication transmission network and other infrastructure and equipment resources of coastal transportation departments, applies for private network frequency point resources, and independently constructs mobile (broadband) communication system. Each part is described as follows in detail.

4.1 Public-Private Combination Scheme (Scheme I)

This scheme is mainly based on the operator's existing network architecture and communication resources. Special core network equipment is arranged in the transportation management department to be responsible for the relevant businesses of private network users. Figure 2 is presenting network structure of scheme I.

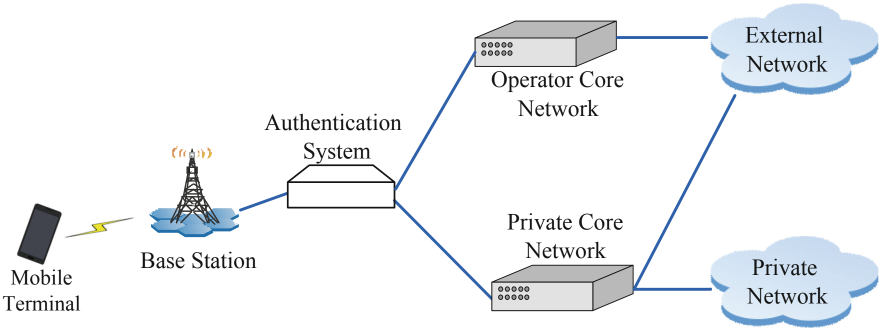


Fig. 2. Structure diagram of scheme I.

The wireless base station in the area covered by the private network can provide shared access for private network users and ordinary users. The authentication system is responsible for distinguishing the types of users, guiding the private network users to the private network core network to establish bearer, and guiding the ordinary users to the operator core network to establish bearer. In addition, private network users can carry out various services of the private network platform under the control of the private network core network, and can also access the external network. Concurrently, ordinary users can establish connections with private network users under the core network and license and control of the private network.

4.2 Self-building Private Network Scheme (Scheme II)

The wireless base station in the area covered by the private network only provides access to the private network terminal, which is established and carried by the private network core network to realize the development of various services of the private network platform. In this scheme, two sets of core network equipment shall be configured, one set is mainly used for internal network service bearer and one set is mainly used for external service bearer. At the same time, the two sets of equipment can be backed up to each other. Private network users can carry out intranet and extranet applications through corresponding core network equipment. External users can also connect to private network users through gateway and switching equipment. Figure 3 is presenting network structure of scheme II.

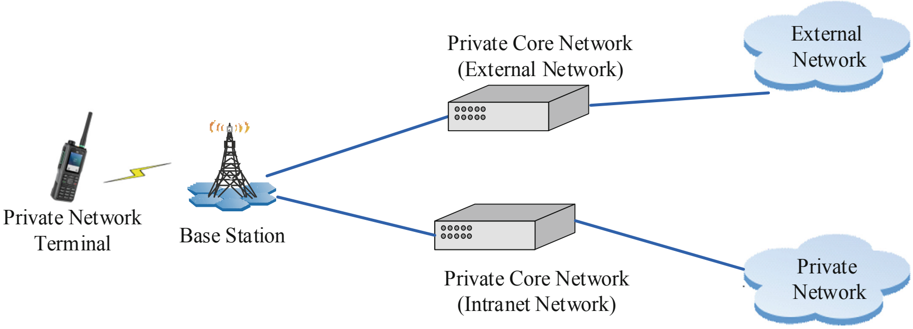


Fig. 3. Structure diagram of scheme II.

5 Comparison and Analysis

At present, there are three most commonly used communication means for ships in coastal waters, namely public communication network (mobile phone), VHF radio communication and satellite communication. VHF communication bandwidth is limited and the cost of satellite communication is expensive. Most of the information exchange is through the public communication network, but the coverage of the public mobile communication network is very limited. Both scheme I and scheme II proposed in this paper are due to the current communication mode in coastal waters.

This part mainly compares and analyzes the public-private combination scheme (scheme I) and the self-building private network scheme (scheme II) from the perspectives of convenience, technical characteristics, investment scale, operation and maintenance and resource control.

5.1 Convenience

In scheme I, users do not need to purchase special communication terminals, but only need to open the corresponding section services, so that they can use mobile phones and other communication terminals to access the ship shore broadband transmission private network and enjoy various business services. Scheme II requires a dedicated communication terminal to access the private network. Therefore, scheme I has better convenience and universality, and is easier to promote and use among social users.

5.2 Technical Characteristics

Both scheme I and scheme II are based on 4G/5G technology system, and can carry out various services under 4G/5G network conditions. Specifically, scheme I makes use of the operator's private network core network and has the conditions for smooth transition to a comprehensive 5G communication network. Besides, in scheme II, because the communication frequency band is limited to 1.4 ghz/1.8 ghz, the number of base stations is limited and the spacing is too large, the construction cost of complete transition to 5G communication network is large. Therefore, scheme I will have better scalability than scheme II.

5.3 Investment Scale

Scheme I relies on the mature and large-scale industrial chain of operators, and the construction cost of a single station is much lower than that of a private network base station. Therefore, the total investment of scheme I is lower. Furthermore, scheme I does not need to configure special communication terminals, and various general communication terminal equipment widely exist in the market, and the configuration cost is much lower than that of scheme II. Therefore, compared with scheme II, scheme I has economic advantages in construction cost and future operation and promotion.

5.4 Operation and Maintenance

For the operation and maintenance of relevant equipment and facilities in scheme I, the operator can be entrusted to provide corresponding services uniformly without the construction unit bearing relevant costs. Moreover, it can provide more high-quality operation and maintenance services for the private network and save a lot of operation and maintenance workload of the construction unit. In scheme II, the operation and maintenance management of equipment and facilities and network system in the later stage of the private network shall be undertaken by the construction unit. With the continuous expansion of the construction scale, the difficulty of private network operation and maintenance will continue to increase. Therefore, in terms of operation and maintenance, scheme I is better.

5.5 Resource Control

Most of the towers in scheme I belong to operators. Once the operators adjust the tower layout scheme, it will directly affect the system base station layout. Meanwhile, if the operator does not maintain some towers, it will increase the difficulty of system base station maintenance. On the contrary, the base station infrastructure in scheme II belongs to the construction unit, and the resource control is significantly better than that in scheme I.

After comprehensive analysis, the construction of coastal mobile (broadband) communication network by scheme I has more advantages in engineering construction, such as convenience, technical characteristics, investment scale, operation and maintenance, etc.

References

1. Zheng, S.: Application of 5G technology in mobile communication network. Wirel. Internet Technol. **8**(16), 1–2 (2017)
2. Calabrò, E., Magazù, S.: Non-resonant frequencies in mobile wireless 5g communication networks. Wirel. Pers. Commun. **115**(2), 1387–1399 (2020). https://doi.org/10.1007/s11277-020-07633-3
3. Sultana, A., Woungang, I., Anpalagan, A., et al.: Efficient resource allocation in SCMA-enabled device-to-device communication for 5G networks. IEEE Trans. Veh. Technol. **99**, 1 (2020)
4. Yi, Z., Wang, F., Wang, S., et al.: Design of high frequency digital transceiver in coastal radio station and shipborne. J. Phys: Conf. Ser. **1920**(1), 1–5 (2021)
5. Ali, M.F., Jayakody, D.N.K., Chursin, Y.A., Affes, S., Dmitry, S.: Recent advances and future directions on underwater wireless communications. Arch. Comput. Methods Eng. **27**(5), 1379–1412 (2019). https://doi.org/10.1007/s11831-019-09354-8
6. Ye, L., Wang, J., Zhang, S., et al.: Efficient coastal communications with sparse network coding. IEEE Netw. **4**, 1–7 (2018)

A CNN-Based Information Network Attack Detection Algorithm

Lei Di, Hongzhong Ma, Yi Luo(✉), and Zhiru Li

State Grid Gansu Electric Power Research Institute, Lanzhou 730070, China
1812685961@qq.com

Abstract. At the information network level, many researchers use techniques such as intrusion detection and traffic analysis to discover malicious behaviors of attackers. However, the above methods face many challenges when applied to smart grids. This paper is based on the vulnerability sample data set, and studies how to extract features for abstract modeling. The first is to extract the characteristics of the vulnerability samples by transforming the model into a learning vector and using artificial intelligence methods such as deep learning. The second is to learn and train the characteristics of vulnerabilities to form a prototype of the automatic detection principle of vulnerabilities. Finally, through the above two steps, the discovery ability and analysis efficiency of software high-threat security vulnerabilities are improved.

Keywords: CNN-based · Information network · Attack detection algorithm · Malicious behaviors

1 Introduction

Since 2018, attacks of different scales have increased exponentially, and medium-sized DDoS attacks (10–50 Gbps) have increased by an astonishing 293.44%. The growth rate of very large attacks (above 600 Gbps) has also reached 93.33%. On the contrary, the number of resources that can be used to launch attacks has decreased compared with last year, and the stability has gradually decreased. The above data has increasingly verified that the cost of attacks is gradually decreasing. Attackers can launch DDoS attacks with huge traffic and produce powerful destructive power with only a few resources. The above examples only reflect a specific attack. In reality, there are endless attack methods, all based on diversified vulnerabilities. Software vulnerability mining refers to the analysis of the source code or executable code of the software to detect whether it has defects that may be exploited. These flaws are exploited by attackers, which may cause program crashes and even threaten the security of the entire computer system.

The relatively mature vulnerability mining technologies currently developed include: manual detection, Fuzz technology, binary comparison, static analysis and dynamic analysis. In a real engineering environment, vulnerability mining relies heavily on the experience of engineers, and many vulnerabilities are discovered based on the experience of engineers. Therefore, traditional loophole mining has the problems of inability to

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 155–161, 2022.
https://doi.org/10.1007/978-981-19-3486-5_19

operate in batches and poor sustainability. Unable to operate in batches means that engineers cannot detect multiple codes at once, but can only do so in sequence. Each piece of code needs to be analyzed separately and cannot be carried out uniformly, and the detection efficiency is difficult to keep up with the explosive growth rate of the code volume. Poor sustainability refers to the consistency of the engineer's approach to code testing. Usually a code inspection can only be done by one engineer, and it is difficult to achieve collaboration. If a safety engineer interrupts work, it will be difficult for the successor to keep up with the predecessor's thinking and continue. Unlike code development, traditional vulnerability detection cannot form a modular division of labor, so the mode of vulnerability detection needs to be changed and innovated.

Smart grid is a typical power Internet of Things, and it is the part of the modern power grid that has the widest distribution, the most complexity, the most types of equipment, and the closest contact with users. These characteristics make it easy to access and difficult to monitor, making it the most vulnerable part of the power grid. With the introduction of the concept of ubiquitous power Internet of Things, while advancing the in-depth integration of information resources and physical resources, and improving the quality and efficiency of the power grid, more heterogeneous terminals have also been spawned. This leads to a wider exposure of the power grid system, giving attackers more angles of attack. At the same time, distribution network automation has become the core content of the development of power grids around the world. Cyber attacks may cause serious security risks to unattended, highly information-based smart grids. And network security supervision is one of the main ways to ensure the safe operation of large power grids. At present, the work is mainly carried out by means of manual on-site inspection and verification. The existing various safety detection technologies are not completely suitable for new applications such as electric power industrial control systems and "big cloud, moving intelligence" and so on. These technologies also cannot effectively discover and verify the existence of security flaws, vulnerabilities, malicious code, security vulnerabilities and other hidden dangers.

2 Related Research

At the information network level, many researchers use techniques such as intrusion detection and traffic analysis to discover malicious behaviors of attackers. Fadlullah et al. used probabilistic models to analyze power grid communication traffic and behaviors to detect and locate malicious behaviors in smart grids [1]. Zhang et al. used Support Vector Machine (SVM) and Artificial Immune System (Artificial Immune System) to identify malicious data injection attacks in the smart grid, and studied a distributed intrusion detection system [2]. Mitchell et al. proposed an intrusion detection system based on behavior rules, and detected specific behaviors according to behavior rules. In this system, the behavioral rules originate from the control loop linking intrusion detection and business process, and do not rely on system operation or other tracking data. Ten et al. used the description method of attack tree to evaluate the security of the information system of the SCADA system [3]. In contrast, the physical-information attack model of the smart grid constructed by Chen et al. using Petri nets can better characterize and discover coordinated attack events [4]. Liu et al. designed an intrusion detection method for smart meters and used Colored Petri net to describe the data flow and command flow inside the smart meters. Through spying domain to protect the internal data of the smart meter, an attack detection mechanism against the AMI network is constructed [5]. Zhao et al. conducted a lot of research on the active defense of the power grid, and provided new ideas for the defense of the power grid [6–8]. However, the above methods face many challenges when applied to smart grids:

1) The higher real-time requirements of the power grid make the delay caused by the existing authentication mechanism, attack detection and other methods affect the operation of the power grid;
2) The power system has high standards for availability and safety, and it is difficult for the existing technology to meet the demand for false positives and false negatives at the same time;
3) The network topology of the smart grid is complex, and the equipment types are diverse, which puts forward higher requirements for the compatibility and scalability of safety technologies.

Therefore, it is necessary to study information network attack detection methods suitable for smart grids based on a full understanding of the operating characteristics and requirements of smart grids.

This paper is based on the vulnerability sample data set to study how to extract features for abstract modeling. The first is to transform the research model into a learning vector, and use artificial intelligence methods such as deep learning to extract the characteristics of the vulnerability samples. The second is to learn and train the characteristics of vulnerabilities to form a prototype of the automatic detection principle of vulnerabilities. Finally, through the above two methods, the discovery ability and analysis efficiency of software high-threat security vulnerabilities are improved.

3 Vulnerability Detection Model Based on CNN Method

3.1 Analysis of Similarity of Graph Isomorphism Based on MLP

Multilayer Perceptron (MLP) is the most basic multilayer neural network, that is, the hidden layer has multiple layers. Its main feature is that the signal is transmitted in the forward direction, and the error is transmitted in the backward direction. By continuously adjusting the network weight value, the final output of the network is as close as possible to the expected output to achieve the purpose of training, as shown in Fig. 1.

In this paper, the code to be tested is compared with a code database with known vulnerabilities one by one, and similar codes that may trigger exceptions are found. The MLP neural network of the training network used for similarity comparison performs cosine operation on the vector transformed by the structure2vec algorithm. If the code is similar, output 1 and output -1 if the code is different. The specific method of cosine operation is shown in formula (1), where ***g*** represents the control flow graph, and ***∅(g)*** represents the structure2vec algorithm. In the training process, through error back propagation, the function that needs to be continuously optimized is shown in formula (2). The

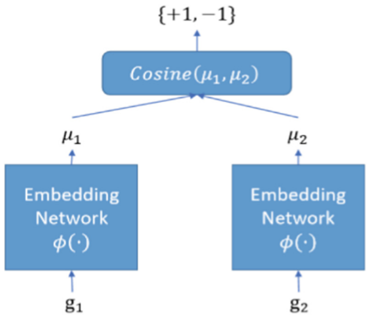


Fig. 1. Code similarity analysis based on multilayer perceptron

MLP neural network of the training network used for similarity comparison is shown in the figure.

$$\mathrm{Sim}(g, g) = \cos(\varnothing(g), \varnothing(g)) = \frac{\langle \varnothing(g), \varnothing(g) \rangle}{\|\varnothing(g)\| \cdot \|\varnothing(g)\|} \tag{1}$$

$$\min_{W_1, P_1, \ldots, W_n, P_n} \sum\nolimits_{i=1}^{K} (\mathrm{Sim}(g, g) - y_i)^2 \tag{2}$$

3.2 Code Flow Graph Analysis Based on Convolutional Neural Network

Convolutional Neural Network (CNN) is often used in the image field. The difference between a convolutional neural network and an ordinary neural network is that the convolutional neural network contains a feature extractor composed of a convolutional layer and a pooling layer. In the convolutional layer of a convolutional neural network, a neuron is only connected to some neighboring neurons. In a convolutional layer, it usually contains several feature planes (Feature Map). Each feature plane is composed of some neurons arranged in a rectangle, and the neurons of the same feature plane share weights. The weight shared here is the convolution kernel. The convolution kernel is generally initialized in the form of a random decimal matrix, and the convolution kernel will learn reasonable weights during the network training process. The direct benefit of sharing weights (convolution kernels) is to reduce the connection between the various layers of the network, and at the same time reduce the risk of overfitting. The pooling layer will further simplify and compress the feature plane, thereby reducing parameters and speeding up calculations. At the same time, this approach reduces the possibility of overfitting, and there are usually two forms of mean pooling and maximum pooling. In this paper, for the control flow graph and data flow graph of the code to be tested, the structure graph is transformed into a one-dimensional vector according to the structure2vec algorithm. Then the vector corresponding to each node is filled into a two-dimensional vector and combined into an “image”. After being transformed into an image, the deep convolutional network can be used to learn the features in the image and detect the code under test.

3.3 Function-Level Code Text Analysis Based on Deep Recursive Network

Recurrent Neural Network (RNN) is often used in the text field. Different from multilayer perceptrons and convolutional neural networks, recurrent neural networks have obvious advantages in processing sequences with obvious contextual features. From the structural point of view, the hidden layer of the recurrent neural network has an additional closed loop pointing to itself. That is, the output at the current moment will be used as the input to the next moment, so as to pass the sequence characteristics down. The model structure diagram of RNN is shown in Fig. 2, Where: x_t is a vector that represents the value of the input layer. h_t is a vector that represents the value of the hidden layer. U is the weight matrix from the input layer to the hidden layer. O_t is also a vector, which represents the value of the output layer. V is the weight matrix from the hidden layer to the output layer:

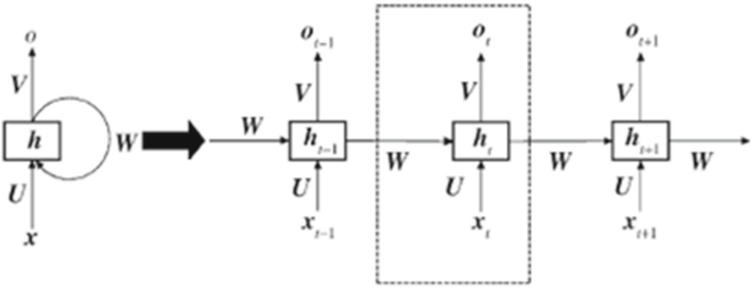


Fig. 2. Traditional recurrent neural network structure diagram

The traditional recurrent neural network model has the defect of gradient explosion, that is, when the length is too long, the training ability of the model decreases. In a training text, if two words with relevance are far apart in the text, the model cannot find the relevance. This problem is also known as the long-term dependency problem. The LSTM model is an improved model based on the RNN model to solve the gradient explosion problem in the RNN model. LSTM adds the concept of a "gate" to the RNN model, and uses the "gate" to control whether to forget or remember previous information. So as to solve the problem of gradient explosion caused by long text. The model structure of LSTM is shown in Fig. 3:

Considering that the code text is generally long, even if the network structure of LSTM is used, there is no guarantee that it can be accurately correlated. Therefore, the code is divided into functions, and text analysis is performed for each function. Each function builds an abstract syntax tree (AST), and then traverses the AST according to a depth-first search strategy. Thereby, irrelevant symbols are filtered out and new code text is generated.

The deep recurrent neural network learns and trains the newly generated code text, aiming to find high-risk function vulnerabilities.

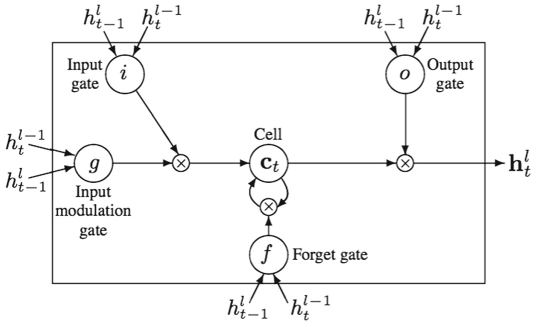


Fig. 3. Structure diagram of the adjusted LSTM

3.4 Vulnerability Detection and Verification

Based on the above principles, we have tested and verified the proposed detection method by developing a prototype of the vulnerability detection principle. The prototype of the vulnerability detection principle detects the code under test from the above three perspectives (ie, similarity comparison, flow graph feature recognition, and text feature recognition). Generate logs for detected suspicious codes and submit them for manual further testing or use dynamic detection methods for further verification. The main function of static vulnerability mining based on artificial intelligence is to serve as an auxiliary means to discover vulnerabilities. The most critical point is to automatically discover potential vulnerabilities in the code through the machine, and to determine the security of the code. This paper not only uses a multi-layer perceptron in the traditional code similarity analysis, but also uses a recurrent neural network to directly detect the code text. Furthermore, by establishing the control flow graph and data flow graph of the code, and transforming the flow graph into an image, the convolutional neural network is used for feature learning and judgment.

4 Conclusion

In short, we have proposed a CNN-based information network attack detection algorithm, which can abstract the features of the code from a higher level and establish a feature library of the vulnerable code. Compared with traditional static analysis, the feature library obtained through high-level abstraction is more complete. Traditional static analysis can only find local suspicious vulnerabilities based on static vulnerability signature libraries, but cannot fully grasp the correlation between large sections of code, which causes a large number of false positives. In this paper, through deep learning, we can find the potential features and the context of the code, the features are more complete, and the false alarm rate is reduced.

Acknowledgments. This work was supported by State Grid Gansu Electric Power Research Institute Project-Intelligent Recognition and Defense of Intrusion Behavior of Electric Power Information and Physical Fusion System in Cyber Attack Environment (No. 52272219000E).

References

1. Fadlullah, Z.M., et al.: An early warning system against malicious activities for smart grid communications. IEEE Netw. **25**(5), 50–55 (2011)
2. Zhang, Y., et al.: Distributed intrusion detection system in a multi-layer network architecture of smart grids. IEEE Trans. Smart Grid **2**(4), 796–808 (2011)
3. Ten, C.W., Liu, C.C., Govindarasu, M.: Vulnerability assessment of cybersecurity for SCADA systems using attack trees. In: Power Engineering Society General Meeting. (2007)
4. Chen, T.M., Sanchez-Aarnoutse, J.C., Buford, J.: Petri net modeling of cyber-physical attacks on smart grid. IEEE Trans. Smart Grid **2**(4), 741–749 (2011)
5. Liu, X., et al.: A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. IEEE Trans. Smart Grid **6**(5), 2435–2443 (2015)
6. Zhao, J.X., Guo, S., Mu, D.: DouBiGRU-A: software defect detection algorithm based on attention mechanism and double BiGRU. Comput. Secur. **111**, 102459 (2011)
7. Zhao, J.X., Zhang, X.: Exploring the optimum proactive defense strategy for the power systems from an attack perspective. Secur. Commun. Netw. **2021**, 1–8 (2021)
8. Xie, L., Yi, M., Sinopoli, B.: integrity data attacks in power market operations. IEEE Trans. Smart Grid **2**(4), 659–666 (2011)

Information Extraction for Knowledge Graph of ISO 19650 Standards

Bing Wu[1](✉), Yuanbin Song[2](✉), Junyi Chu[2], and Jinhao Cao[2]

[1] Economic Research Institute of State Grid Zhejiang Electrical Power Company,
Hangzhou 310000, China
wu_bing_jyy@sgcc.com.cn

[2] School of Naval Architecture, Ocean and Civil Engineering, Shanghai Jiao Tong University,
Shanghai 200240, China
ybsong@sjtu.edu.cn

Abstract. Engineering project development requires all participants timely communicate explicit information. Besides the IFC file format, they also need an information management framework to support their collaboration. ISO 19650 standard series provide such a framework to establish a reliable information source. Since the 5-part ISO 19650 series constitute a complex system, the AEC community expect a knowledge graph to capture the key concepts and rules in those standards in order to facilitate the application of the collaborative management framework. Unfortunately, manual development of ISO 19650 knowledge graph is costly and time consuming. Therefore, a NLP-based information extraction method has been specifically developed for automatic construction of the ISO 19650 knowledge graph. In particular, the difficulty arising from the lack of corpus is greatly overcome by reasoning out domain semantic relationships from the syntactic relationships with the mapping rules specifically developed in this study. Finally, the experiment verified the feasibility and usefulness of the developed information extraction method.

Keywords: Collaboration framework · Building Information Modeling · Knowledge graph · Natural Language Processing

1 Introduction

In the past decade, more and more companies in the Architecture/Engineering/Construction (AEC) industry have accepted and incorporated the Building Information Modeling (BIM) approach in their information management transactions. From the perspective of a digital model, BIM is the digital representation of physical and functional characteristics of a facility during its lifecycle [1]. Many designs and As-built drawings of buildings are recently delivered in the Industry Foundation Class (IFC) file format [2], which is the international standard of BIM data storage for describing the 3D geometrical, engineering, and functional characteristics of either building components or subsystems. On the other hand, BIM also refers to a set of information processes or transactions, which concern the explicit sharing of information

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 162–172, 2022.
https://doi.org/10.1007/978-981-19-3486-5_20

requirement about production, usage, updating, and exchange of the digital representation of an engineering infrastructure in order to form a reliable basis for decision making [3].

Although the IFC and other alternative file formats help the AEC industry to achieve interoperability among various design and engineering analysis software, multiple project participants still face up with the challenge of information collaboration. In particular, there is frequently information gap among trades, leading to no party being responsible for delivery of crucial information or delayed integration of drawings and as-built data. These problems have become more serious in an international project with a number of participants who come from different countries with diverse cultures of project management. In this regard, ISO 19650 standard series [4–7] have been published to assist the AEC industry to smooth their information collaboration with a set of concepts and guidelines.

The ISO 19650 standard series provide a unified framework of information management for all the project participants to follow. In this way, they can save a lot of time on communicating their information requirements and aligning their expectation within the same framework. In detail, a series of standard items categorize the information management transactions along the lifecycle of a project, and in each typical transaction, a collection of activities is formally modeled with the required production, usage and exchange as well as security of the BIM data. Accordingly, the implementation of the afore-mentioned framework often results in a series of templates or schemata of data, which should be agreed by the corresponding participants at different project stages.

Unfortunately, the 5-part ISO 19650 series constitutes a complex system, which is beyond the manual management of project stakeholders. Meanwhile, these standard documents are written in natural language, and therefore it is a great challenge for computer to understand or draw inference from the unstructured text. In this regard, it may be meaningful to utilize knowledge graph for representing the key information residing in the unstructured standard, which can further assist computer reasoning.

The concept of knowledge graph was originally proposed by Google as a knowledge representation method to improve internet searching. Recently, a dozen of applications using knowledge graph have been developed in various domains. Unfortunately, manual construction of a knowledge graph for a specific domain, like the ISO 19650 standards, is often a time-consuming and costly. So, this study attempts to automatically convert the ISO 19650 documents into a computer-understandable knowledge graph with the assistance of Natural Language Processing (NLP) tools. A number of deep-learning-based NLP methods have been utilized to facilitate the construction of knowledge graph [8–10]. The difficulty of utilizing the NLP approach lies in the lack of corpus to train the language model to recognize the named entities or concepts used in ISO 19650 standards for many core concepts are just only coined for these standards.

Meanwhile, knowledge reasoning has recently been studied with the combination of deep learning [11]. One typical difficulty of knowledge reasoning is that the meaning of a name entity depends on its semantic relationships with other entities. In other word, Different relationships connected to entities can represent different entities [12, 13], and this greatly infects the accuracy of filtering candidate entities in the graph. Although some research propose approach to improve the accuracy of filtering entities [14], such approaches are sometimes inadequate for inferring large-scale knowledge graphs, like the one for ISO standard series.

2 Preprocessing of the ISO 19650 Documents

Figure 1 illustrate the preprocessing flow to segment sentences in the ISO 19650 standard series into tokens for further processing. The original standards in English version are first translated into Chinese, stored in the Microsoft docx format. Then the preprocessing program as illustrated in Fig. 1 is applied to extract all the sentences in each part of the ISO standard.

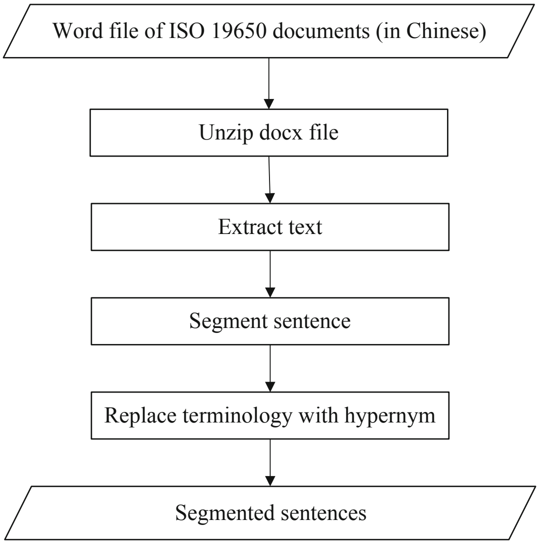

Word file of ISO 19650 documents (in Chinese)
Unzip docx file
Extract text
Segment sentence
Replace terminology with hypernym
Segmented sentences

Fig. 1. Preprocessing of Word documents of ISO 19650

The docx. file is actually a compressed package of a collection of XML files that contains both the textual content and the markup tags for its for formatting or typesetting definition. The.docx file is unzip into a collection of XML files using the open source ZLib library, and then the text content of the standards are extracted from those unzipped files with removal of all the font and paragraph typesetting. In this way, the program generates a plain text file with a list of sentences.

In general, knowledge can be divided into common knowledge and domain knowledge from the viewpoint of its content. The former often focuses on capturing common sense with generally used words in literature, textbook, journal, news and daily communication, while the latter, for instance the ISO standards, should formally represent the domain-specific concepts, rules and models with the necessary usage of a dozen of terminologies. It is these special terminologies that exacerbate the difficulty of segmentation of Chinese sentence. Different from an English sentence, a Chinese sentence has no space to split the characters into words, resulting in difficulties for evaluating relationships between words.

The Jieba library is used to segment each sentence in the ISO 19650 standard documents into an array of words, each of which contains one or more Chinese characters. Moreover, since Jieba has limited capacity to identify new word, a database of bilingual ISO vocabulary has been specifically developed to enhance Jieba's capacity of identifying new words. For example, without using the ISO 19650 vocabulary, the word "公共数据环境"(Common Data Environment, CDE) is often segmented into three items "公共"(Common), "数据"(Data)", "环境"(Environment), which is not the expected result. So, the terminology "公共数据环境" is incorporated into the Jieba's special dictionary in order to enhance its segmentation capacity.

3 Evaluation of Syntactical Relationships

The structure of a sentence can be reasoned out by the dependency parsing, a process that labels each word as a token and simultaneously determines its links to other constituent words in the sentence. Dependency parsing aims to annotate sentences into a dependency tree which is designed to be easy for humans and computers alike to understand. In this study, the open source Baidu Dependency Parser (DDParser) [10] is utilized for examining the dependencies among an array of words segmented from a sentence in the preprocessing procedure. Dependency parsing provides a useful means for computer to understand the syntactical relationships or grammatical structure of a sentence.

The DDParser is an extension of the graph-based biaffine parser [15] in order to deal with the Chinese characteristics in the training dataset DuCTB. The input vector of the *ith* word e_i is the concatenation of both its embedding vector $e^{word}{}_i$ and its character-level LSTM vector *charLSTM*(w_i), as shown in the following formula:

$$\mathrm{e_i} = \mathrm{e_i^{word}} \oplus \mathrm{chrLSTM(w_i)} \quad (1)$$

where $\mathrm{chrLSTM(w_i)}$ is the concatenated vectors resulting from sequentially feeding each character in the *ith* word into a BiLSTM layer.

Then, each e_i is input into the 3-layer BiLSTM that produces the high-dimension vector r_i. Subsequently, the dimension of each r_i vector is reduced by the Multiple-Layer Perception (MLP). This reduction of dimension can screen the information that contribute little to the dependency between words [15]. For applying deep biaffine attention, each word can be regarded as either a head or a dependent, and the deep biaffine attention method is utilized for both in dependency arc classifier and relation classifier. Accordingly, the dimension reduction results from the $\mathrm{MLP^{(arc)}}$ are denoted by h_i^{h-arc} and h_i^{d-arc}, while $\mathrm{MLP^{(rel)}}$ h_i^{h-rel} and h_i^{d-rel}. Then with the pairwise strategy, the $\mathrm{i^{th}}$ word and the $\mathrm{j^{th}}$ word are input into the biaffine attention for calculating the scores for dependency arc and relationship. Due to the limitation of writing space, the details of biaffine attention is not elaborated herein, and interested readers can refer the literature [15]. The biaffine attention is utilized to identify both dependency and its syntactic relationship. By the highest dependency score of $\mathrm{S^{arc}}$, the corresponding syntactical relationship can be determined. For the example in Fig. 2, the syntactical relationship between "Is" and "Information source" is derived as Verb-Object (VOB).

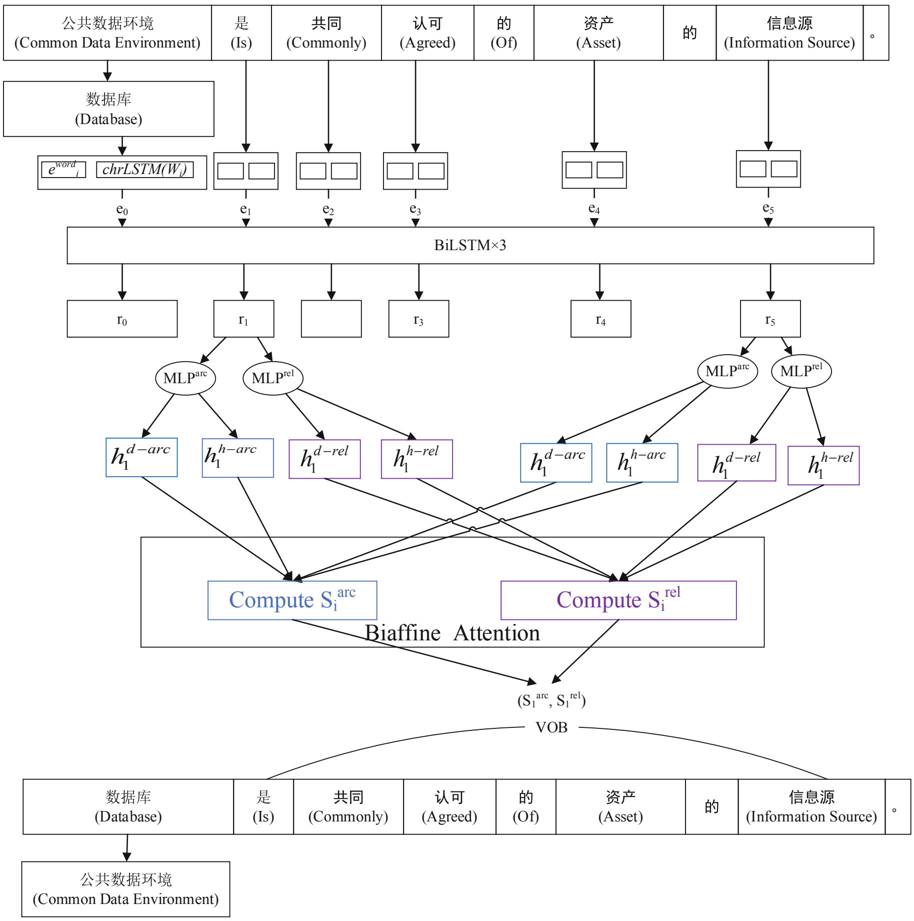


Fig. 2. Framework of DDParser

The DDParser has been trained on Baidu Chinese Treebank (DuCTB), which is a large-scale manually labeled dataset of annotated binary relations between two words. There are altogether 24 part of speech (POS)tags of and 14 types of dependency relationships in the DuCBT. The frequently used POS tags are noun, verb, adjective, adverb, and preposition. Table 1 lists part of dependency relationships between those POS tags.

Figure 3 illustrates an example parsing tree that is a hierarchical organization of words linked by a directed arc from the head word to the modifier word. Each directed arc represents a syntactical dependency. For example, the subject "公共数据环境"(Common Data Environment, CDE) has an arc from the predicate "是" (is), while the "信息源" (Information Source) is also linked with the same predicate "是" (is). From these two relationships, it can be reasoned out that the concept CDE is a hyponym of the more general concept "information source".

Table 1. Frequently used dependency relationships

Dependency	Explanation
HED	Head/Core of the whole sentence
SBV	Relationship between subject and predict (Head)
VOB	Relationship between predict (Head) and object
ATT	Relationship between attributive and noun (head)
ADV	Relationship between adverbial and verb (head)
POB	Relationship between preposition and object (head)
COO	Cooccurrence between two words

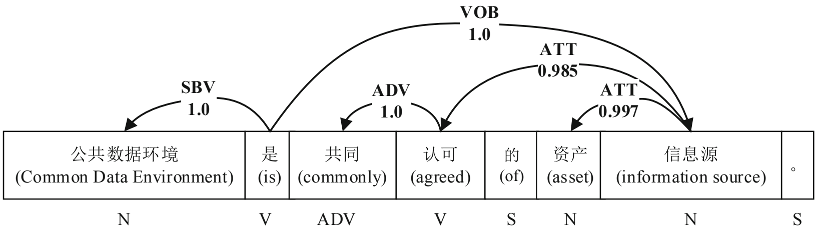


Fig. 3. Example dependency tree of a sentence

4 Inference for Semantic Relationship

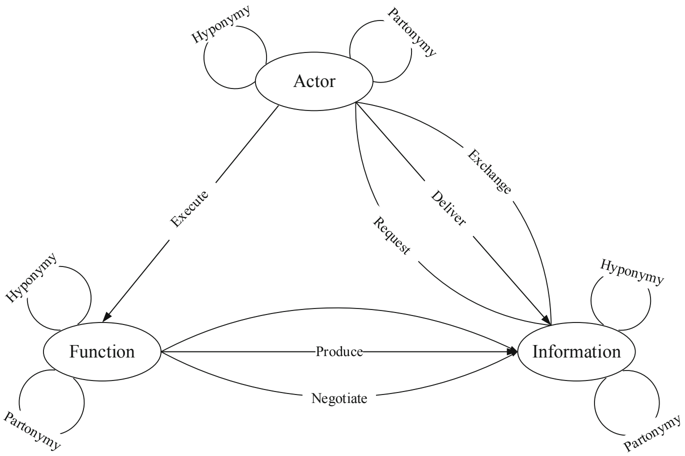


Fig. 4. Typical semantic relationships

The DDParser mainly deals with the syntactic structure of the sentence other than its semantics relationships. The syntactical relationships focus on delivering information of grammatical structure of sentences, but the development of knowledge graph concern the meaning of linkage between words or concepts. So, the semantic relationships are crucial for developing domain knowledge graphs, and then further information residing in multiples sentences can be inferred from those semantic relationships.

Firstly, three core concepts, i.e. information, actor, function are identified by manual analysis of ISO 19650 series, and simultaneously nine semantic relationships between core concepts are also defined (See Fig. 4). The alphabets A, I, F, O indicate the entity types Actor, Information, Function and Other, respectively.

A set of mapping rules from syntactical relationships to semantic relationships have been developed, and Tables 2 list the typical mapping rules. Using these mapping rules, the syntactical relationship reasoned out by the DDParser can be converted into semantic relationships.

Table 2. Mapping from semantic relationships to syntactical relationships

Head	Modifier	Syntactical relationship	Semantic relationship	Example trigger word
A/I/F	A/I/F	SVB ∩ VOB	Hyponymy	是(is)/指(indicate)
A/I/F	A/I/F	SVB ∩ VOB	Partonomy	包括(contain)
F	I	VOB	Process	处理(process)
F	I	VOB	Negotiate	同意(agree)
F	I	VOB	Produce	提供(provide)
I	F	ATT	Process	处理(process)
I	F	ATT	Negotiate	同意(agree)
I	F	ATT	Produce	提供(provide)
F	A	SVB	Execute	执行(execute)
F	A	SVB	Exchange	交换(exchange)
F	A	SVB	Deliver	提供(provide)
F	A	SVB	Request	需要(need, require)
I	O	ADJ	Attribute	属性(attribute modifier)
F	O	ADV	Qualify	限制(qualify)
A	O	ADJ	Attribute	属性(attribute modifier)
F	O	ADJ	Attribute	属性(attribute modifier)

Figure 5 illustrates the conversion of the syntactical relationships in Fig. 3 into meaningful relationships that can be used for developing knowledge graph. For instance, two syntactical relationships SBV (between “公共数据环境” (CDE) and “是” (Is)) and VOB (between “信息源” (Information Source) and “是” (Is)) are mapped into one semantical relationship “Hyponymy” between the subject “公共数据环境” and the object “信息源”, following the mapping rules described in Table 2. Meanwhile,

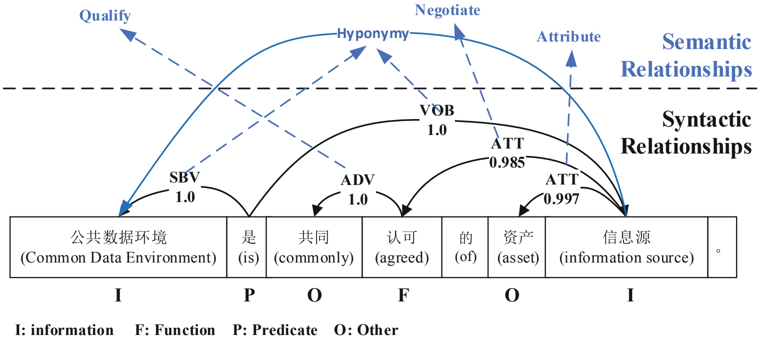


Fig. 5. Conversion from syntactical relationships into semantic relationships

the “ATT” relationship between “信息源” and “认可”(Agreed) is converted into the “Negotiate” linkage between the two entities, and the head word “信息源” is of the “Information” type, while the modifier “认可” is of the “Function” type, and furthermore a trigger word for the semantic relationship “Negotiate”. In addition, the other two syntactical relationships “ATT” and “ADV” are converted into two semantic relationships “Attribute” and “Qualify”.

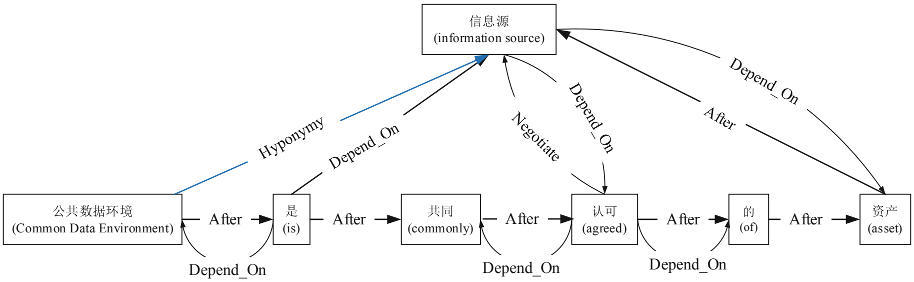


Fig. 6. Knowledge graph stored in Neo4J graph database

Since the ISO 19650 standard documents multiple sentences or paragraphs, and these sentences are interconnected with each other via shared concepts. Therefore, the graph database Neo4J is used for description of both the semantic relationships between the words and interconnection among sentences. Specifically, a node is used for denoting named entities, and a directed edge for binary relationship between two nodes. Both a node and an edge can have multiple attributes.

For example. Figure 6 shows that the sequence of the words in the same sentence is represented by an array of “AFTER” relationships from the preceding word to the succeeding one, while the semantic relationship is depicted by the “Depend_On” relationship from the modifier word to the head word. The type of the syntactic relationship is represented as the attribute of the “Depend_On” edge. In comparison with the SQL relational database, the enriched description for edge in Neo4J can greatly reduce the

JOIN operation required by SQL database, leading to faster query. Moreover, the inferred semantic relationships are also stored in the same Neo4J database.

5 Case of Knowledge Inference

The graph structure of Neo4J database can be further used for knowledge reasoning. In particular, when referring ISO 19650 standards for decision making, it is important to infer the reference or dependency among the standard sentences. The attribute-enriched path between entities is very useful for automatic identification of the afore-mentioned dependencies.

Figure 7 illustrates a typical case of reasoning with the knowledge graph. The sentence of the Sect. 3.3.15 of ISO 19650 Part 1 indicates that the Chinese word "共同" (commonly), modifying the word "认可" (agreed), is the trigger word of the core concept "角色" (Actor) which is defined in the Sect. 3.2.1 of ISO 19650 Part 1. Meanwhile, in the second sentence in Fig. 7 there are 3 hyponymy relationships between "人员"(Person), " 组织"(Organization), and "单元"(Unit) and "角色"(Actor). This implies that these people, organizations, and organizational unit involved in the process of project construction should achieve an agreement of the composition of the CDE, a source of information shared among the project participants. In this way, the standard Sect. 3.3.15 can refer to 3.2.1 via the following Cypher query:

```
MATCH(a:公共数据环境)
WHERE (a)-[*]-(b:共同)
MATCH(c:角色)
WHERE (b)-[:Trigger_Word]- > (c)
MATCH(d)
WHERE(c)-[:Hyponymy]-[d]
RETURN d
```

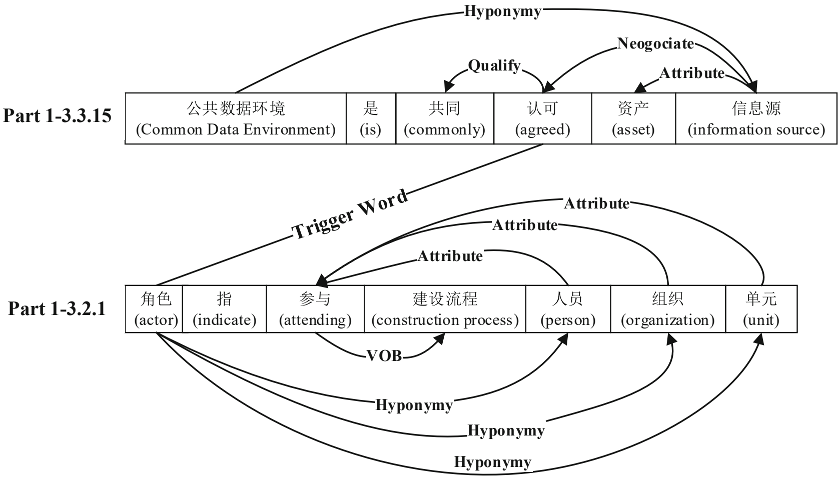


Fig. 7. Case of inferring dependency between standard sentences

6 Conclusions

Engineering infrastructure development requires appropriate sharing of information among all participants. Although the IFC standard plays a key role in unifying format of shared BIM data, this information sharing needs an information management framework mutually agreed by the project participants. The ISO 19650 standard series provide the concepts, principles, procedures and rules for building such a collaboration framework in order to establish a reliable information source. Since the 5 parts of ISO 19650 series constitute a complex system, the AEC community expect a knowledge graph to capture the key concepts and relationships in those standards in order to facilitate the application of the collaborative management framework. Unfortunately, manual development of ISO 19650 knowledge graph is costly and time consuming. Therefore, the NLP-based information extraction method has been specifically developed to facilitate the construction of the ISO 19650 knowledge graph. In particular, the difficulty arising from the lack of corpus can be greatly overcome by inferring domain semantic relationships from the syntactic relationships with the mapping rules. Finally, the experiment verified the feasibility and usefulness of the developed information extraction method.

Acknowledgments. This research was supported by the sponsorship from the Economic Research Institute of State Grid Zhejiang Electrical Power Company (Grant No. SGZJJY00SJJS2100042).

References

1. National Institute of Building Science, Frequently asked questions about the national BIM standard-united states. https://www.nationalbimstandard.org/faqs#faq1, Accessed 02 Sept 2021
2. BuildingSmart, Industry Foundation Classes (IFC) - An Introduction. https://www.buildingsmart.org/standards/bsi-standards/industry-foundation-classes/, Accessed 02 Sept 2021
3. ISO, ISO 16757–1:2015 Data structures for electronic product catalogues for building services - Part 1: Concepts, architecture and model, 1st edn (2015)
4. ISO, ISO 19650 Part 1: 2018 Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) - Information management using building information modelling—Part 1: Concepts and principles, 1st edn (2018)
5. ISO, ISO 19650 Part 2: 2018 Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) - Information management using building information modelling—Part 2: Delivery phase of the assets, 1st edn (2018)
6. ISO, ISO 19650 Part 3:2020 Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) - Information management using building information modelling—Part 3: Operational phase of the assets, 1st edn (2020)
7. ISO, ISO 19650 Part 5: 2020 Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM)—Information management using building information modelling—Part 5: Security-minded approach to information management, 1st edn (2020)

8. Jiang, Y., Jin, B., Zhang, B.: Research progress of natural language processing based on deep learning. Comput. Eng. Appl. **57**(22), 1–14 (2021)
9. Baidu, Dependency parsing. https://cloud.baidu.com/doc/NLP/s/nk6z52eu6, Last accessed on 2021/10/10
10. Zhang, S., Wang, L., Sun, K., Xiao, X.: A practical Chinese dependency parser based on a large-scale dataset. https://arxiv.org/abs/2009.00901, Accessed 10 Oct 2021
11. Song, H., Zhao, G., Sun, R.: Developments of knowledge reasoning based on deep reinforcement learning. Comput. Eng. Appl. (2021). https://kns.cnki.net/kcms/detail/11.2127.tp.20211022.1446.008.html, Accessed 08 Nov 2021
12. Rahman, M.M., Takas, A., Demartini, G.: Representation learning for entity type ranking. In: Proceedings of the 35th Annual ACM Symposium on Applied Computing, pp. 2049–2056. ACM, New York (2020). https://doi.org/10.1145/3341105.3374029
13. Reinanda E., Meij E., Pantony J., et al.: Related entity finding on highly-heterogeneous knowledge graphs. In: Proceedings of 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. Barcelona: IEEE, 330–334. [doi: https://doi.org/10.1109/ASONAM.2018.8508650] (2018)
14. Huang, J., Ding, S., Wang, H., et al.: Learning to recommend related entities with serendipity for web search users. ACM Trans. Asian Low-Res. Lang. Inf. Process. **17**(3), 25 (2018). https://doi.org/10.1145/3185663
15. Dozat, T., Manning, C.D.: Deep biaffine attention for neural dependency parsing. arXiv preprint arXiv:1611.01734 (2016)

Author Index

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 173–174, 2022.
https://doi.org/10.1007/978-981-19-3486-5