A quantitative assessment method of network information security vulnerability detection risk based on the meta feature system of network security data

Weiwei Lin[1, 2*], Chaofan Yang[3], Zeqing Zhang[4,5], Xingsi Xue[3] and Reiko Haga[6]
[1] School of Big Data and Artificial Intelligence, Fujian Polytechnic Normal University, Fuqing, 350300, China
[e-mail: linww_cn@hotmail.com]
[2] Engineering Research Center for ICH Digitalization and Multi-source Information Fusion, Fujian Province University, Fuqing, 350300, China
[3] School of Computer Science and Mathematics, Fujian University of Technology, Fuzhou, 350118, China
[4] School of Information Science and Engineering, Xiamen University, Xiamen, China
[5] West Yunnan University of Applied Sciences, Dali, China
[6] CommScope Japan KK, Nagatacho, Tokyo, 100-0014, Japan
[*]Corresponding Author: Weiwei Lin

Received July 12, 2021; revised September 5, 2021; accepted October 14, 2021; published December 31, 2021

Abstract

Because the traditional network information security vulnerability risk assessment method does not set the weight, it is easy for security personnel to fail to evaluate the value of information security vulnerability risk according to the calculation value of network centrality, resulting in poor evaluation effect. Therefore, based on the network security data element feature system, this study designed a quantitative assessment method of network information security vulnerability detection risk under single transmission state. In the case of single transmission state, the multi-dimensional analysis of network information security vulnerability is carried out by using the analysis model. On this basis, the weight is set, and the intrinsic attribute value of information security vulnerability is quantified by using the qualitative method. In order to comprehensively evaluate information security vulnerability, the efficacy coefficient method is used to transform information security vulnerability associated risk, and the information security vulnerability risk value is obtained, so as to realize the quantitative evaluation of network information security vulnerability detection under single transmission state. The calculated values of network centrality of the traditional method and the proposed method are tested respectively, and the evaluation of the two methods is

This work was supported by the Natural Science Foundation of Fujian Province, China; Research on network risk assessment method based on dynamic attack behavior (Grant No. 2019J01889), the "Tiancheng Huizhi" Innovation and Education Promotion Fund, China; Construction of Network Risk Assessment Platform Based on Dynamic Attack Behavior(Grant No. 2018A02005), the Education-Scientific research Project for Middle-aged and Young of Fujian Province, China; Research on analysis system of malicious code based on API relevance (Grant No. JT180626).

http://doi.org/10.3837/tiis.2021.12.015 **ISSN : 1976-7277**

evaluated according to the calculated results. The experimental results show that the proposed method can be used to calculate the network centrality value in the complex information security vulnerability space network, and the output evaluation result has a high signal-to-noise ratio, and the evaluation effect is obviously better than the traditional method.

Keywords: One-way transmission state, Information security vulnerability, Risk quantification, Assessment, The weight

1. Introduction

With the continuous popularization of information technology, the development space of the network has been continuously expanded, and the application prospect has become more and more extensive. At the same time, the network is also facing increasingly serious security problems [1,2].

Vulnerability is an inherent attribute of network information system. Any network information system has certain vulnerability. Vulnerability is the cause and premise of network security risks. According to the feature system of network security data element, if the security and stability of the transmission environment cannot be guaranteed in the process of data transmission, the vulnerability of the network will lead to a direct impact on the integrity and authenticity of the data [3,4]. One of the methods to analyze network vulnerability is to analyze and measure the network information security vulnerability, and determine the information security vulnerability and the severity of the vulnerability [5,6]. Once data information leaks, it will lead to data leakage or data interception, monitoring and other risks. Therefore, it is very important to establish an effective network information security mechanism and evaluate the risk of network information security vulnerability.

At present, network information security vulnerability assessment technology has become the focus of relevant experts and scholars. Scholars in this field have realized the evaluation of network information security vulnerability by different means, but these methods still have different degrees of disadvantages, which need to be improved later. For example, the method of vulnerability risk assessment of Internet of things system based on game model proposed in literatures [7,8]. In this method, the game model of network attack and defense is established and the attack strategy of multiple vulnerability combination is designed. It uses the game model to analyze the income expectation of both sides and quantifies the vulnerability harm in the network with low complexity. On this basis, it evaluates the security risk of specific level of network. In references [9,10], a risk matrix-based assessment method of vulnerability related hazards of Internet of things system is proposed. This method uses CVSS V3 evaluation index, vulnerability related graph and risk matrix as research basis to assess logistics information security vulnerability. By considering the relationship between the pre / post vulnerability nodes and the characteristics of the vulnerability itself, we can prevent the high-risk vulnerability. However, the traditional network information security vulnerability evaluation method does not set the weight value in the evaluation process, which makes it

difficult for network security personnel to evaluate the risk value of information security vulnerability according to the calculated value of network centrality, resulting in the problem of poor evaluation effect. In addition, the above-mentioned methods need too much investment in the early stage, and also need to rely on a large number of historical data and expert knowledge, which is easy to cause the problem of less effective information in the output results.

Therefore, under the condition of one-way transmission, the quantitative evaluation method of network information security vulnerability is constructed. First of all, multi-dimensional analysis of the impact of network information security vulnerability on system confidentiality and availability. Secondly, considering that in different time periods, the number of attacks and attack methods are different, the inherent attribute dimension needs to be quantified first, so that the evaluation results will change dynamically with time, making the evaluation results dynamic and authentic.

2. Multi-dimensional analysis of network information security vulnerability

From the previous related research, it is not difficult to find that if the information security vulnerabilities appear in the network information system life cycle, then its cumulative attack amount will be distributed as a "S" curve [11]. which accords with the characteristics of the Compertz growth curve model.

Generally speaking, one-way transmission state refers to that in order to ensure the security of information transmission network, in practice, data information can only be transmitted from high security domain network to low security domain network. Therefore, this study considers using the Compertz model to fit the number of attacks in the life cycle of network information security vulnerability under one-way transmission. The analysis model is as follows:

$$V(t) = Va^b \tag{1}$$

Where, $V(t)$ represents the number of information security vulnerability attacks, t represents the time，V represents the total number of attacks suffered by the information security vulnerability in the whole life cycle at that time; b represents the growth rate of the information security vulnerability attack; a represents the amount of attack [12].

Using formula (1) to get the analysis result, because the analysis results will directly affect the calculation of attack heat, so we use the information security vulnerability to predict the attack in the later life cycle, calculation of attack heat under different conditions, the calculations are as follows:

First, subdivide the information security vulnerability lifecycle and divide it into several time periods. Suppose the information security vulnerability is represented V_i, information security vulnerability lifecycle T_i divided into n time periods，for the k period, the number of attacks is:

$$V_i(k) = V_i(k+1) - V_1(k) \tag{2}$$

On this basis, the efficiency coefficient method is used to transform the attack heat index. Considering that the amount of information security vulnerability attacks will cause the increase of the total amount of information security vulnerability attacks, need to set weights for different information security vulnerabilities. According to the different attention of the attacker to the information security vulnerability as a whole and the difference of the total number of attacks in the whole life cycle, the weight value is calculated by using the improved efficacy coefficient, and the calculation method is as follows:

$$w_i = \frac{V_i}{maxV_i(k)} \tag{3}$$

Where the w_i represents the attack heat of the information security vulnerability V_i in k time period, $max\ V_i\ (k)$ represents the maximum value of attacks in the k time period.

In multidimensional analysis, if the total amount of predicted attack of a certain information security vulnerability is too large and there is a large amount of attack in the divided time period, it is necessary to set the attack heat score of 10 in this time period, so as to ensure that the calculation results are fixed [13].

3. The property value of network information security vulnerability

On the basis of multi-dimensional analysis of network information security vulnerability, it is necessary to quantify the attribute value of network information security vulnerability. First, the qualitative method is used to classify the information security vulnerability, and the result of the division is shown in **Table 1**.

Table 1. Hazard rating for information security vulnerability

Confidentiality level	Hazard Description	Scale
C1 high	Can read any file	8.25
C2 generally high	A monitorable system	5.25
C3 medium	Valuable information confirmed	2.25
C4 low	Verify host validity	0.25

As can be seen from **Table 1**, Information security vulnerability is independent and complementary to the harmfulness of the system, although there is no conflict between them, each security attribute is not completely independent [14]. When a security attribute value of an information security vulnerability is on the high side, its value also increases. To some extent, its information attribute has destructive power. According to the characteristics of network information security vulnerability, the inherent attribute value of information security vulnerability is divided into three forms, respectively:

A: There are 3 sets of language values, which are high, medium and low.

B: There are four sets of language values, which are high, high, medium and low.

C: There are five sets of language values, which are high, high, medium, low and low.

The above three forms of language values all have a membership function, and they correspond to each other.

4. Quantitative assessment of network information security vulnerability

Based on the above multi-dimensional analysis of network information security vulnerability in one-way transmission state and the quantification of the inherent attribute value of information security vulnerability, the quantitative evaluation of network information security vulnerability is realized.

Firstly, the network flow centrality of information security vulnerability is worth the number of attack paths in one-way transmission. The calculations are as follows:

$$C_f(i) = \sum_{k \in H} \frac{m_{jk}(i)}{m_{jk}} \tag{4}$$

Where the $C_f(i)$ represents the number of attack paths in one-way transmission, H the set of information security vulnerabilities, m_{jk} represents the weight of information security vulnerability of initial attack node of attack path j, the information security vulnerability k represents the location of all possible attacks on the destination attack node [15]. $m_{jk}(i)$ represents the weight of the information security vulnerability that can be exploited in the attack path j.

On the basis of formula (4), the centrality of network flow with different information security vulnerabilities is calculated as follows:

$$E = \frac{\sum_{q=1}^{+\infty} j_q C_f(i)}{V_i(k)} \tag{5}$$

Where, q represents the number of nodes in the attack path, and j_q represents the degree of node Association in the attack path. If E is greater than 0.5, there are more attack chains in the network. Considering the lack of attack depth in the calculation process, It is impossible to accurately divide the differences between the supply chains of permission levels, so in this study, we mainly divide the differences between the supply chains of permission levels from two directions [16,17]. The first direction: whether the horizontal extension of attack path j passes through multiple hosts; the second direction: whether the vertical penetration of path j passes through multiple hosts. In this process, the attack chain classification is shown in **Fig. 1**.

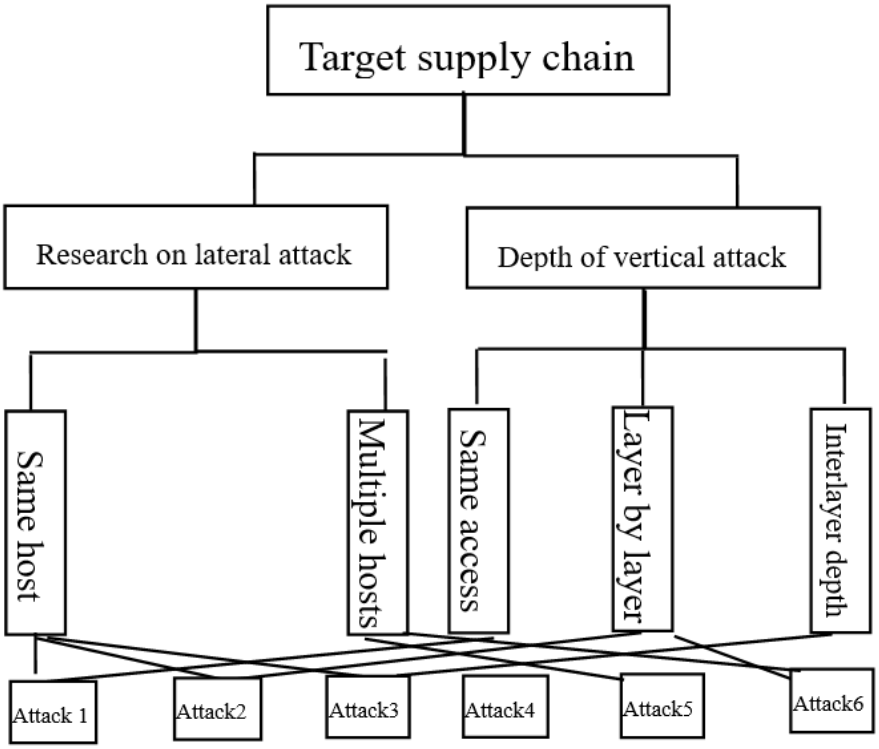

Fig. 1. Schematic diagram of attack chain classification

According to the classification results of attack chain shown in **Fig. 1**, we can see that there are six different values of weight m_{jk}. Hence, we need to use the AHP analysis method to establish the judgment model, the expression is:

$$A = C_f(i) \times \sum_{m=1}^{6} l_m \tag{6}$$

Among them, l_m represents six attack chains, $m \in [1,6]$ and the m is an integer. The matrix is based on the damage degree of attack by different attack chains.as the maximum eigenvalue of the obtained matrix A, it is shown that the obtained unit eigenvector is not credible, and the consistency test is also needed [18]. When processing, you need to reset the weight so that the minimum weight value is 1. After increasing the weight value, we evaluate the influence of the number of hosts in the network and the attack depth of the attack chain on the calculation results [19].

In order to comprehensively evaluate the information security vulnerability, it is necessary to quantify the indicators of each dimension, and the quantification process is as follows:

$$R = \frac{A \times \beta \times \lambda}{l_m \times w_i} \tag{7}$$

Among them, β represents indicator dimension and λ represents quantitative level. Finally, the efficiency coefficient method is used to evaluate the risk of information security vulnerability Association.

$$Q = R \times \left(e + C_f(i) - C_a\right) \tag{8}$$

Where the Q represents the associated risk value after the information security vulnerability V_i quantified, C_a represents the calculated value of the information security vulnerability center, it can be determined by the product of a single vulnerability CVSS score and the impact factor, e and f represents a positive constant.

Apply formula (8) to evaluate information security vulnerabilities. During the calculation, the range of values after the index is quantified should be 0~10. When calculating spatial correlation risk, the e value is 0.1, f value is 9.9 [20].

To sum up, the design of quantitative assessment method for network information security vulnerability under single transmission state is achieved.

5. Test and result analysis

To verify the validity and availability of the quantitative assessment method of information security vulnerability risk based on the meta-feature system of network security data designed in this study, a comparative test experiment was designed to verify it.

Place four computers and a smart printer in the experimental network structure, one of which provides Web services and Mail services, and three of which are the work hosts. Attackers can access internal network information through the Internet. The information security vulnerability settings for the above equipments are shown in **Table 2**.

Table 2. Information security vulnerabilities of equipments in networks

Host	Information security vulnerability	Attack mode	Access enhancement
server	ServU5.0	Overflow attack	ROOT
server	Dvbbs7.0sp2	Inject attack	User
firewall	Linux7.0	Overflow attack	ROOT
Host1	SQLleak	Direct utilization	ROOT
Host2	telnet	Direct utilization	User
Host3	RPCleak	Network monitoring	User
Printer	Printing services	Race condition	User

According to the characteristics of information security vulnerability, the attack chain between information security vulnerabilities is established by using information security vulnerability attack rules. **Fig. 2** is the network attack roadmap depicted in conjunction with the cyberspace structure, where the virtual node represents the attack result, that is, the network information security vulnerability. Inside, $i \in [1,7]$, and i is integer.

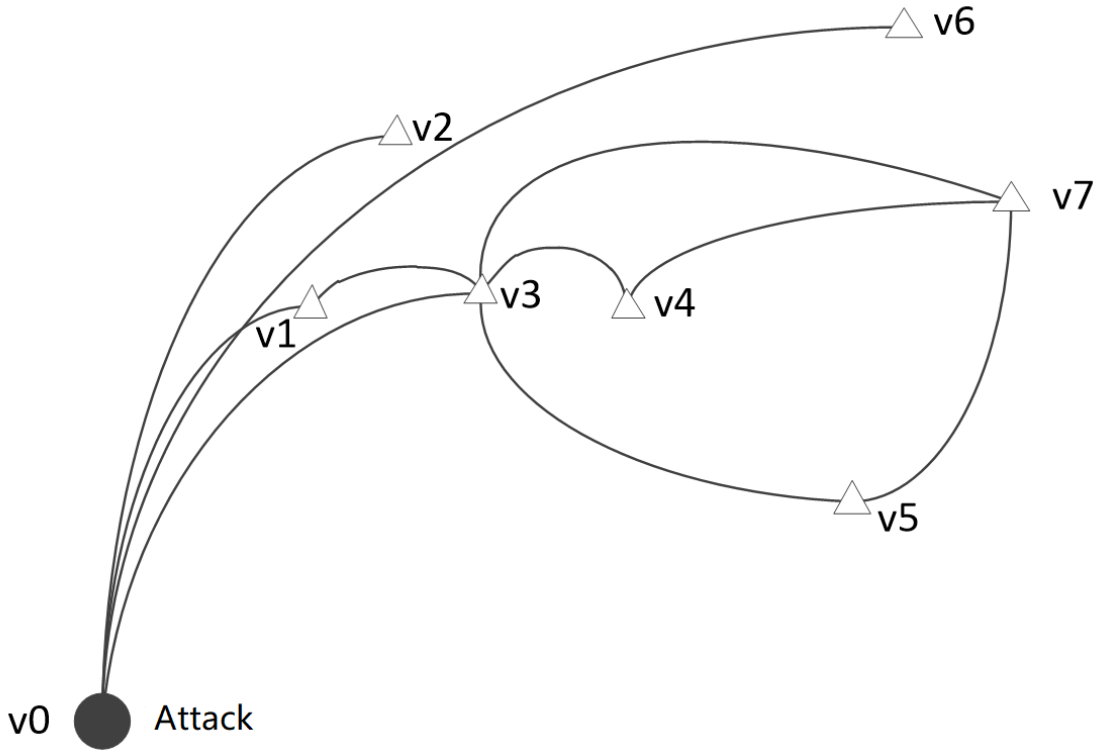

Fig. 2. Distribution of network information security vulnerabilities

In order to expound the harmfulness of association attack, it is confirmed in the experiment that the security of other hosts in the network will be threatened after the network information structure leaks. In order to make the experiment illustrative, according to the network attack route and information security vulnerability distribution shown in **Fig. 2**, respectively test the proposed information security vulnerability risk quantitative assessment method based on the network security data meta feature system and the network centrality calculation value of the game model based risk assessment method of the Internet of things system leakage in the literature [7], and infer the weighted value and the weighted value Evaluate the significance of the effect. Apply Formula (3) to get the corresponding weight value, and the experimental results are shown in **Table 3** and **Fig. 3**.

Table 3. Calculated values of information security vulnerability spatial network centricity of different methods

path	weight	Number of attack chains containing requested information security vulnerabilities							
	m_{jk}	v0	v1	v2	v3	v4	v5	v6	v7
v0-v1	1	0	0	0	0	0	0	0	0
v0-v2	1	0	1	0	0	0	0	0	0
v0-v3	1	0	2	0	0	0	0	0	0
v0-v4	2	0	3	0	0	0	0	0	1
v0-v5	3.73	0	1	0	2	2	0	0	1
v0-v6	8.94	0	5	0	2	2	0	1	0
v0-v7	8.94	0	0	0	6	3	4	0	0
result	Literature [7] Methods	0	2.22	0	1.85	0	0	0.36	0
	Methodology proposed	0	19.5	0	16.5	2.58	4.56	3.23	3.59
Quantification of results		0.10	10	0.10	8.25	1.59	2.58	1.71	1.73

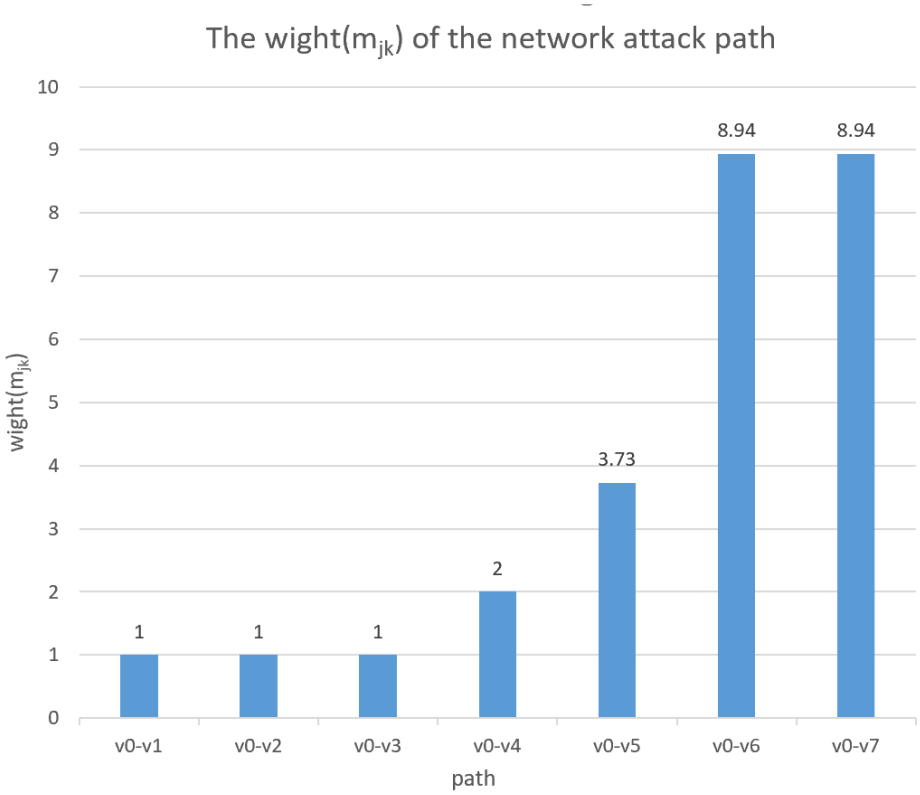

Fig. 3. The wight(m_{jk}) of the network attack path

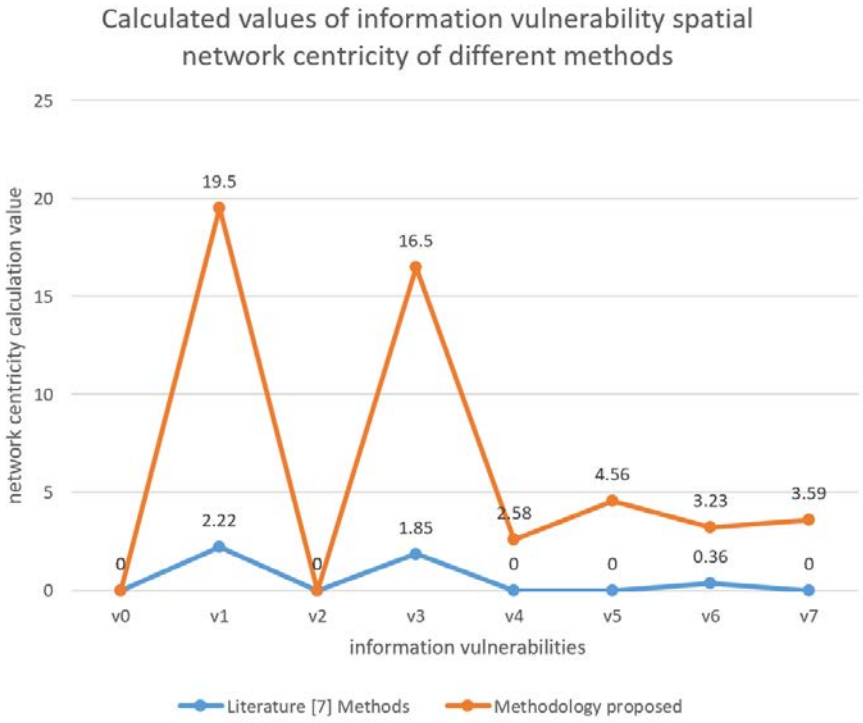

Fig. 4. Calculated values of information security vulnerability spatial network centricity of different methods

Analysis **Table 3** shows that network centricity calculation value of information security vulnerability v1 is the largest, and it is the key node of information security vulnerability network. This is related to the fact that information security vulnerability v1 is at the top of the attack chain. The experimental results show that the greater the centrality value, the greater the impact on the entire information security vulnerability network. Using the proposed method, information security vulnerability v3 has a centrality value of 16.5, which is second only to v1 in importance. Therefore, in the subsequent development of defense strategies, security personnel need to focus on protection. The position of v1, v3 and v7 is the focus of the chain of attack protection. The results shown in **Table 3** and **Fig. 4** also reflect the effectiveness of the proposed method. Because it is difficult to calculate the network centricity at v2, v4, and v5 locations when calculating the network centricity value with reference [7], and the results of the proposed method are consistent with the actual situation, it can be proved that the proposed quantitative assessment method of information security vulnerability risk based on the meta-feature system of network security data is implemented in complex information security vulnerability spatial network. This is because the proposed method takes into account the impact of attack chain depth on network centrality after setting weights, and quantifies the intrinsic attribute values of information security vulnerabilities through qualitative methods. Even in more complex environments, the evaluation results of the built methods are most significant.

To further verify the validity of the proposed quantitative assessment method for information security vulnerability risk based on the meta-feature system of network security data, this method is compared with the game model-based vulnerability risk assessment method of the Internet of Things system in literature [7] and the risk matrix-based vulnerability

Association hazard assessment method of the Internet of Things system in literature [9], and the network communication output from different methods is tested. The signal-to-noise ratio of the quantitative assessment results for information security vulnerabilities is shown in **Table 4** and **Fig. 5**.

Table 4. Comparison of SNR of the output of different evaluation methods（unit: dB）

Number of iterations	This thesis Methodology	Literature [7] Methodology	Literature [9] Methodology
100	55.75	37.58	24.67
200	63.63	42.93	28.46
300	69.56	39.75	29.56
400	72.68	50.90	32.34
500	75.98	55.42	48.75

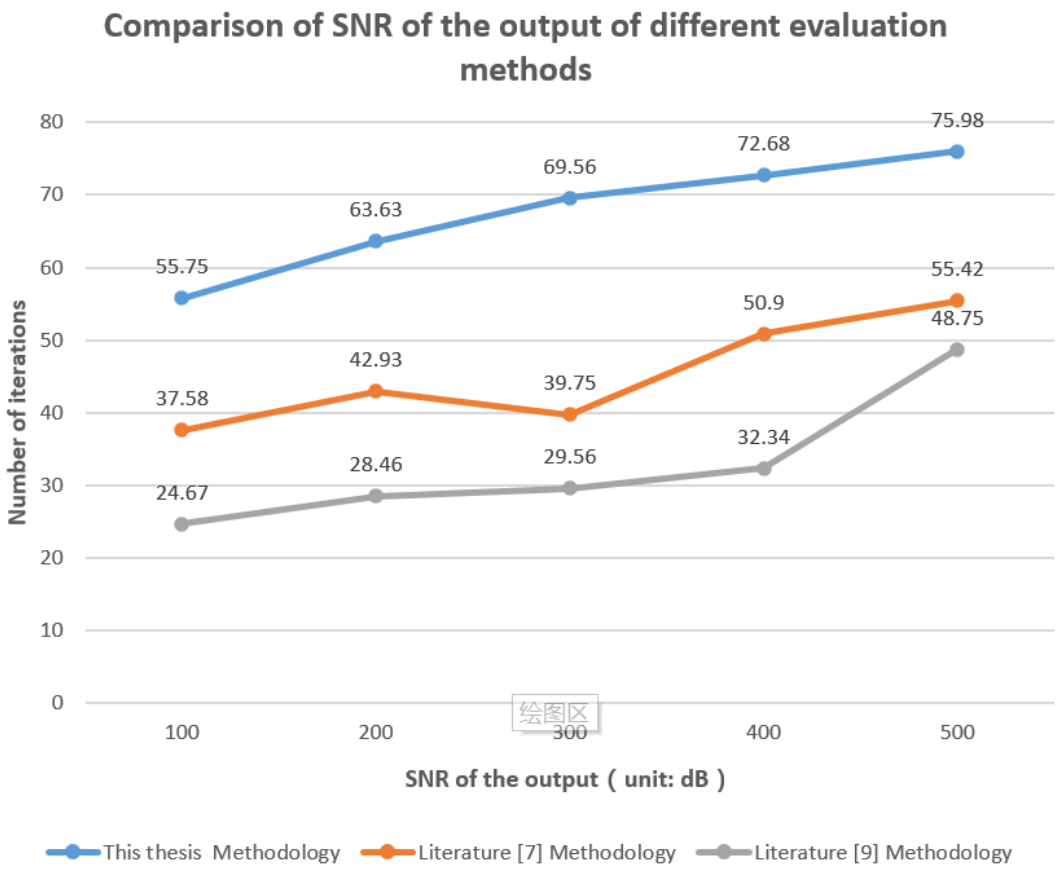

Fig. 5. Comparison of SNR of the output of different evaluation methods

As the number of iterations increases, the signal-to-noise ratio of the output evaluation results from different network information security vulnerability assessment methods also changes. However, the peak signal-to-noise ratio of the proposed quantitative assessment

method for information security vulnerability risk based on the network security data meta-feature system remains the highest, which proves that the evaluation method has the most effective information in the output results. This is because the data meta-feature system can visually describe the data attributes. On the basis of quantifying the intrinsic attribute values of information security vulnerabilities, the proposed method uses the efficiency factor method to transform the associated risks of information security vulnerabilities, which effectively improves the signal-to-noise ratio of the output results.

In summary, the quantitative assessment method of information security vulnerability risk based on the network security data meta-feature system designed in this study has higher application advantages, and the output signal-to-noise ratio of the evaluation results is high, which proves that the method has a good application effect.

6. Concluding remarks

In order to overcome the shortcomings of traditional quantitative assessment methods for network information security vulnerability risk, this paper designs a quantitative assessment method for information security vulnerability risk under one-way transmission based on the network security data meta-feature system. This method uses multidimensional analysis to analyze the problems of network information security vulnerabilities, and uses qualitative methods to quantify the intrinsic attribute values, so as to achieve the design of a quantitative evaluation method for network information security vulnerabilities under one-way transmission. In the performance comparison phase, the network centricity calculation values and the output signal-to-noise ratio of different network information security vulnerability assessment methods are tested. The experimental results show that the network centricity calculated by the proposed method is more accurate than the traditional method, and the output result has a high signal-to-noise ratio and a large share of effective information, which proves the effectiveness of the method.

Reference

[1] W. G. Wu, J. L. Yang, and J. Geng, “Risk Assessment of Central Hospital Information System Vulnerabilities Based on WOA-KELM,” *Information Technology*, vol. 43(4), pp. 96-100, 2019. Article (CrossRef Link)

[2] W. Han, Z. Tian, Z. Huang, L. Zhong and Y. Jia, “System Architecture and Key technologies of network security situation awareness system yhsas,” *Computers, Materials & Continua*, vol. 59, no. 1, pp. 167–180, 2019. Article (CrossRef Link)

[3] K. N. Lei, Y. Q. Zhang, C. S. Wu and H. Ma, “A System for Scoring the Exploitability of Vulnerability Based Types,” *Journal of Computer Research and Development*, vol. 54, no. 10, pp. 2296-2309, 2017. Article (CrossRef Link)

[4] C. Lv, J. Zhang, Z. Sun and G. Qian, “Information Flow Security Models for Cloud Computing,” *Computers, Materials & Continua*, vol. 65, no. 3, pp. 2687–2705, 2020. Article (CrossRef Link)

[5] F. Zhao, “Research on Network Security Trend Perception In One-Way Transmission Process of Information,” *Computer Simulation*, vol. 6, pp. 456-460, 2018. Article (CrossRef Link)

[6] G. Yang, M. Yang, S. Salam and J. Zeng, “Research on Protecting Information Security Based on the Method of Hierarchical Classification in the Era of Big Data,” *Journal of Cyber Security*, vol. 1, no. 1, pp, 19–28, 2019. Article (CrossRef Link)

[7] Z. Y. Wei, M. D. Wu, N. Ma, M. Lei and W. Bi, “Vulnerability Risk Assessment of IoT System Based on Game Model,” *Journal of Information Security Research*, vol. 4, pp. 48-55, 2018.

[8] W. Fang, F. Zhang, Y. Ding and J. Sheng, "A New Sequential Image Prediction Method Based on LSTM andDCGAN," *Computers, Materials & Continua*, vol. 64, no. 1, pp. 217–231, 2020. Article (CrossRef Link)
[9] X. X. Ren, J. Chen, C. Y. Li, Y. X. Yang, "Hazard Assessment of IoT Vulnerabilities Correlation Based on Risk Matrix," *Netinfo Security*, vol. 11, pp. 86-93, 2018. Article (CrossRef Link)
[10] W. Fang, L. Pang and W. N. Yi, "Survey on the Application of Deep Reinforcement Learning in Image Processing," *Journal on Artificial Intelligence*, vol. 2, no. 1, pp. 39-58, 2020. Article (CrossRef Link)
[11] Y. H. Liu, X. L. Gao, M. C. Zhu and P. H. Su, "Research on Classification Method of Network Security Data Based on Data Feature Learning," *Netinfo Security*, vol. 19(10), pp. 50-56, 2019. Article (CrossRef Link)
[12] B. Y. Zhang and M. Wang, "Research on Quantization Method of Network Attack and Defense Based on CVSS Vulnerability Score," *Journal of Ordnance Equipment Engineering*, vol. 4, pp. 147-150, 2018.
[13] Y. Y. Feng, "Network Information Encryption Vulnerability Detection System Based on Artificial Fish Swarm Algorithm," *Information & Communications*, vol. 12, pp. 53-57, 2019.
[14] G. J. Fan and L. L. Yang, "Coverage Holes Discovery Algorithm without Location Information in Wireless Sensor Networks," *Application Research of Computers*, vol. 6, pp. 1826-1829, 2018.
[15] G. C. Qian, Q. Ding and S. J. Zhang, "Research on Information Security Vulnerability Awareness and Early Warning Technology," *Techniques of Automation and Applications*, vol. 2, pp. 51-55, 2018.
[16] S. L. Ma, "Simulation Research on Real Time Detection of Network Information Encryption Vulnerability," *Computer Simulation*, vol. 3, pp. 328-331, 2018.
[17] Y. Xiao, "research on network data security check based on a novel feature transformation algorithm," *Bulletin of Science and Technology*, vol. 35(5), pp. 127-131, 2019. Article (CrossRef Link)
[18] M. Fang, "Instantiated Computer Network Threat Risk Assessment Model for UML Model," *Communications Technology*, vol. 5, pp. 1234-1241, 2019.
[19] J. Li, P. F. Cao and Yang Jun, "Research on NoC static vulnerability detection system based on big data technology," *Modern Electronics Technique*, vol. 42(21), pp. 77-81, 2019. Article (CrossRef Link)
[20] F. Wang, L. Hong, X. Gu, "Risk Assessment Algorithm of Software Vulnerability Based on Sigmoid Function," *Journal of Information Security Research*, vol. 11, pp. 993-996, 2018.

Weiwei Lin received the B. S. degree in Automation from Southeast University, China in 2001, the M. S. degree in Software Engineering from University of Electronic Science and Technology of China, China in 2011. He is an associate professor in School of Big Data and Artificial Intelligence, Fujian Polytechnic Normal University, China. His research interests include network security, artificial intelligence and cloud computing.

Chaofan Yang received the bachelor's degree from the Fujian University of Technology, China, in 2019. Now, he is a graduate student in college of information and science engineering, Fujian University of Technology. His research domain include Intelligent Computation, Nature Language Processing and Ontology Matching Technique.

Zeqing Zhang received a bachelor's degree and a master's degree in engineering from Huaqiao University and Chengdu University of Electronic Science and Technology in 2001 and 2010. He is an associate professor in West Yunnan University of Applied Sciences, China. His research interests include computer vision, deep learning, document recognition, and artificial intelligence.

Xingsi Xue received the B. S. degree in Software Engineering from Fuzhou University, China in 2004, the M. S. degree in Computer Application Technology from Renmin University of China, China in 2009, and the Ph.D. degree in Computer Application Technology from Xidian University, China in 2014. He is an associate professor at Center for Information Development and Management, Fujian University of Technology, and the director of Intelligent Information Processing Research Center, Fujian University of Technique. His research interests include intelligent computation, data mining and large-scale ontology matching technology. He is the member of IEEE and ACM.

Reiko Haga received the B. S. degree in foreign language (English) From Fujian Teacher's University, Fujian, China, in 1982. She has been working for CommScope Japan as manager of customer service team for more than twenty years. Her research interests include computer vision, deep learning, document recognition, and network security.