Quantitative Evaluation Model for Information Security Risk of Wireless Communication Networks Under Big Data

Bin-bin Jiang(✉)

School of Software, Nanyang Institute of Technology, Nanyang, China
gongzuo8788@163.com

Abstract. Quantitative evaluation of information security risk in wireless communication network can effectively guarantee the security of communication network. In order to solve the problem that the traditional network security evaluation method is not effective, a quantitative risk assessment model of wireless communication network information security under big data is constructed. Using the wireless composition and working principle, the risk assessment system of wireless communication is built, and the index weight is determined. On this basis, the network information function interface is deployed, and the initial probability is calculated, and the quantitative risk assessment model of wireless communication network information security under big data is constructed. The experimental results show that under the condition of increasing the frequency of network attack, the security potential value of the model is always at a higher level, which indicates that the model has better performance and is helpful to detect the security of the system. It is convenient to provide accurate safety protection measures in time to resist safety risks.

Keywords: Security risk assessment · Big data · Risk quantification · Information safety

1 Introduction

Because the communication mode and security level of different network systems are different, resulting in the unfavorable situation of network system isolation, the security level and protective measures of different elements in the same network system are not very clear, so it is difficult to ensure the accurate application of security measures to security vulnerabilities. Therefore, the construction of wireless communication network information security risk assessment model is an important basis for rational allocation of security protection resources. Through the information security risk assessment, we can clarify the information security requirements, help to formulate the optimal information security policy and select the corresponding risk control measures, so as to reduce the risk to an acceptable range. The quantitative measurement of information security risk is an objective and effective quantitative method, which has an intuitive understanding of the probability of risk occurrence and the possible loss after the risk occurs, and is more conducive to the organization of information security risk

G. Gui and L. Yun (Eds.): ADHIP 2019, LNICST 301, pp. 458–468, 2019.
https://doi.org/10.1007/978-3-030-36402-1_49

management and control. For the easy-to-issue information security incident, defensive measures can be taken early. Therefore, it is necessary to conduct research on quantitative measurement of information security risks, in order to manage and control information security risks with better cost-effectiveness [1].

Chen et al. proposed information security risk assessment based on BP neural network method. The process and method of information security risk assessment are introduced in detail. The non-linear BP neural network method is applied to the information security risk assessment model to overcome its subjectivity and artificial nature. It is an effective assessment method. The results are consistent with the theoretical analysis. The Reality of Successful Cases [2]. Li and Lian proposed network information security transmission simulation of large data mobile terminal. This paper designs a security mechanism for network reliability authentication and transmission encryption in the network transport layer to ensure the security of data transmission in the network [3]. However, the above methods have the problem of low evaluation results.

For this reason, the Quantitative Evaluation Model for Information Security Risk of Wireless Communication Networks Under Big Data method is proposed in this paper. The research results of this paper put forward new ideas for the information security risk quantification method, enriched the information security risk measurement method, and provided risk management theory and technical support. From the aspect of management, it promotes the optimal allocation of resources, rationally arranges the investment of information security funds, and carries out information security construction with better cost-effectiveness, reducing the losses caused by information security incidents; From the technical aspect, it provides a message. Security risk occurrence probability calculation model and an information security risk loss calculation idea; From the social aspect, through effective risk quantification, organizations and individuals have an intuitive understanding of information security risks, which is conducive to the protection and organization of personal information.

2 Establishment of Risk Assessment System for Wireless Communication

2.1 Determining the Weight of Assessment Indexes

According to the design principles of risk assessment index system and the security requirements of wireless communication at home and abroad, combined with the wireless composition and working principle, and comprehensively consider various factors affecting the security of wireless communication networks, this paper establishes a wireless communication security risk assessment index system. The evaluation system is mainly composed of five parts: communication transmission safety evaluation index; safety standard system evaluation index; networking safety technology evaluation index; formatted message evaluation index; each terminal safety evaluation index. The information transmitted by wireless communication has certain sensitivity and confidentiality. In order to ensure that information is not stolen by the enemy, the

information is transmitted securely in the wireless network. Before the information is transmitted, various security measures must be adopted to encrypt the message.

Message encryption technology is the most commonly used method to protect data security during data transmission. It is also the most basic necessary technology. It is mainly based on a specific encryption method or encryption algorithm to convert the data to be encrypted into a garbled transmission. The data needs to be restored with the key when the message needs to be read. Transmission encryption is to perform pseudo-random code encryption on the transmitted signal before the terminal device is ready to transmit the data signal, and the frequency hopping pattern selection and the start of the message are shaken. The hopping spread pattern and the pseudo-random code are selected according to different communication networks. And the size of the encryption varies.

In this study, 10 network and wireless experts from different departments were invited to represent different perspectives on wireless security. Through the above simulation wireless throughput, effective throughput, packet loss rate and node transmission delay, etc. The analysis of the importance of the indicators of the evaluation indicators, according to the principle of fuzzy analytic analysis, the results of various indicators analysis [4]. As shown in Table 1:

Table 1. Weight analysis of wireless communication security evaluation index

Evaluation index of wireless communication security	Evaluation index of communication transmission security	Evaluation index of safety standard system	Evaluation index of network security technology	Format message evaluation index	Set up the safety evaluation index of each terminal
Credit/%	89	91	82	73	88
Effective throughput bit/s	354	521	501	497	483
Packet loss rate/%	1	2	2	1	2
Node transmission delay/s	0.020	0.045	0.024	0.084	0.064
Resource utilization rate/%	87.62	94.34	89.95	97.41	94.11

Through the evaluation of each demand risk value, the various elements of data link communication security and the quantitative weight of each factor can be analyzed, and the risk events with higher risk values can be analyzed to determine relevant perfect solutions, so that the existing risks can be effectively avoiding and reducing the occurrence of this risk, but also can effectively guarantee the security of data link communication [5].

2.2 Gray Assessment of Underlying Indicators

According to the weight analysis of the wireless communication security evaluation indicators shown in Table 1, the gray categories $k = \{1, 2, 3, 4, 5\}$ are classified into five categories according to the attack intensity, which are very low, low, medium, high, and very high. The various whitening weight functions are as follows:

First grey class: $k = 1$, very low, grey $\otimes_1 \in \{0, 1, 2\}$, the whitening weight function is f_1;

$$f_1(d_{ij}) = \{d_{ij}, x \in [0, 1] \tag{1}$$

Second grey class: $k = 2$, low, grey $\otimes_2 \in \{0, 2, 4\}$. The whitening weight function is f_2;

$$f_2(d_{ij}) = \{d_{ij}/2, x \in [0, 2] \tag{2}$$

Third grey class: $k = 3$, medium, grey $\otimes_3 \in \{0, 3, 6\}$. The whitening weight function is f_3;

$$f_3(d_{ij}) = \{d_{ij}/3, x \in [0, 3] \tag{3}$$

Fourth gray class:$k = 4$, high, grey $\otimes_4 \in \{0, 4, 8\}$. The whitening weight function is f_4;

$$f_4(d_{ij}) = \{d_{ij}/4, x \in [0, 4] \tag{4}$$

Fifth grey class: $k = 5$, very high, grey $\otimes_5 \in \{0, 5, \ldots\}$. The whitening weight function is f_5;

$$f_5(d_{ij}) = \{d_{ij}/5, x \in [0, \ldots 5] \tag{5}$$

Based on various whitening weight functions, the degree of quantitative evaluation of wireless communication network information security risk under big data is analyzed [6]. The methods used in each evaluation phase are described later in this chapter. Similarly, other evaluation indicators are calculated as follows:

It can be seen from the gray risk assessment results of the evaluation indicators in Fig. 1. The cybersecurity threat assessment has certain similarities with the threat assessment in the military field. In the military field, in order to assess the threat level of an air missile, in addition to considering the missile model (either tactical ballistic missiles, precision guided missiles, or ordinary cruise missiles, different types of missiles have different lethality), but also consider missiles. Information such as temporary space, route, distance, altitude, possible targets, and our defense measures [7].

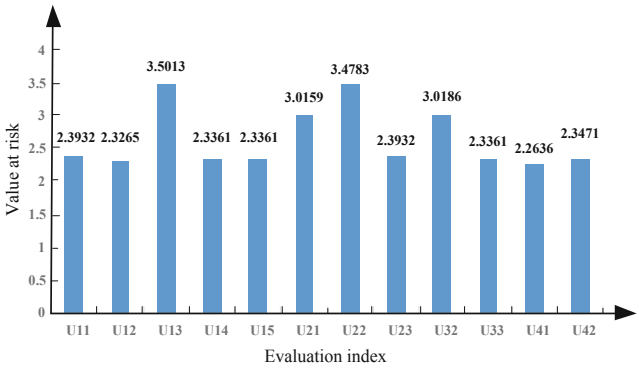

Fig. 1. Grey risk assessment results for assessment Indices

Similarly, in the cyberattack threat assessment process, the type of attack is first analyzed to determine its severity from the nature of the attack. In addition, factors such as the probability of success of the attack, the criticality of the attack against the asset, and the frequency of the attack should be considered to comprehensively assess the threat of the attack. The same type of attack may have different threat levels in different environments, which is related to factors such as network configuration and security policy [8]. This paper summarizes the factors affecting the threat of cyberattacks into six categories: attack destructiveness, environmental factors, probability of success, statistical factors, associated factors and attack effects.

3 Quantitative Risk Assessment of Information Security in Wireless Communication Network

3.1 Deployment of Network Information Functional Interface

The system function interface can be divided into two types: external interface and internal interface. The external interface is responsible for data interaction with the user through the front-end interface, including the user login interface, the management control interface, and the data entry interface. The management control interface further includes: first, a user management interface and an indicator management interface: implemented by a database communication interface; second, plug-in management interfaces: using class [9]. System, Reflection, Assembly, assembly loads an external DLL plug-in [10]. Users can input pre-assessment data through the data entry interface, and the administrator can extend the system through the control center. The internal interface is responsible for automatically processing the data according to the SEM model evaluation process, which is the data interaction interface of the internal modules of the program, as shown in Table 2;

Table 2. Deployment of network information function interface

Serial number	Interface name	Realization	Describe
1	Attack tree generation interface	Public *AttTree GenerateTree (VInfo *&vhead)	Taking the vulnerability information of wireless communication equipment as parameter, attack tree is generated and the root node pointer is returned
2	Theoretical security loss calculation interface	Public float Cal-I'ocLost *&treenode)	Taking the state node as a parameter, the theoretical security loss of the node is calculated and returned
3	Grey clustering interface	Public float Cal GreyCluster (String sql)	Calculate and return an array containing three grey clustering coefficients

Table 2 shows the deployment of the network information function interface, including the indicator system, user information, and plug-in information. It exists in the database before the system runs. It can only be modified by the control center, otherwise it remains unchanged; the dynamic table can be divided. For the pre-data table and the post-data table, the pre-data table includes network topology information, device vulnerability information, and network status specific values. The post-data table includes theoretical node loss, node clustering coefficient, actual node loss, and evaluation result. In the dynamic table, some data tables are manually entered by the user, and only occur before the evaluation calculation starts. Once it is determined that it cannot be changed; the data of the other part of the table is automatically changed according to the operation of the system evaluation work, and is not controlled by human factors.

3.2 Calculate Initial Probability

Monte Carlo simulation is used to calculate the maximum loss of information security risk. Here, geometric Brownian motion is chosen as a stochastic model to reflect the value change of information assets. First, the advantage of geometric Brownian motion to simulate the value of information assets is that the value of general Brownian motion may be negative, while the value of geometric Brownian motion can never be negative, satisfying the characteristic that the value of information assets is never negative; The geometric Brownian motion is consistent with the fluctuation of the information asset market; the geometric Brownian motion process and the real information asset value affected by the information security risk all show the same curved trajectory. Therefore, it can be expressed as:

$$\Delta S_{t+1} = S_t\left(\mu\Delta t + \rho\Im\sqrt{\Delta t}\right) \tag{6}$$

In formula (6), Δt is the value of information assets at the moment of $t+1$; S_t is the value of information assets at the moment of t; μ is the average rate of return on information assets; ρ is the volatility of the rate of return on information assets. In this paper, $\Im$ is the ultimate source of information asset value risk, namely the occurrence of information security events. The occurrence of information security events directly leads to the change of the value of information assets, so the number of times of information security events also causes changes in the value of information assets. In the third chapter of this paper, it has been shown that the frequency of information security events follows Poisson distribution, so it can be assumed that random variables can be assumed. Obey Poisson distribution.

We set the holding period to one year, that is $\Delta t = 1$. We divide it into an average of 52 equal periods of time to simulate the value trend of information assets, S_t is the value of information assets at initial Tim, ΔS_{t+1} for the value of information assets at the moment of $t+1$, ΔS_{t+1} the amount of change in the value of information assets over a period of time. Then the average and standard deviation of the rate of return on information assets for each period of time is $\frac{\mu}{52}$ and $\frac{\rho}{52}$. The value of the information assets at the moment of $t+1$ is:

$$\Delta S_{t+1} = S_{t+i-1}\left(\frac{\rho}{52}\Delta t + \frac{\Im}{52}\right) \tag{7}$$

According to the probability calculation model of information security events established by formula (7), the mean value of occurrence frequency of information security events of different kinds of information security events is calculated respectively. Thus completed big data wireless communication network information security risk quantitative evaluation model design.

4 Experiment

In order to verify the validity of the quantitative risk assessment model for wireless communication network information security under big data, in the actual test, the model designed in this paper is set as the experimental group and the traditional evaluation model as the control group. The concrete steps are as follows.

4.1 Experimental Steps

The first step is to select 18 kinds of training samples with different characteristics, including 15 types of normal operation data and 3 types of attacked data, and calculate the expected values of each standard attribute of each training sample, namely, the group of feature information vectors of this kind of samples.

The second step is to input a certain amount of attack information randomly into the wireless sensor network and process the node running data once every 100 s to form the node operation information vector with standard attributes.

The third step is to pair the node's information vector with the elements in the feature vector group, and to express the set-pair relationship by the expression of the number of connections. The sensitivity of four Eigenvectors in the vector is calculated by analytic hierarchy process (AHP) according to the result of expert score. The calculation judgment matrix is;

Wormhole Judgment moment of attack:

$$A_3 = \begin{bmatrix} 1, \frac{1}{2}, 1, \frac{1}{5} \\ 2, 1, 2, \frac{1}{2} \\ 1, \frac{1}{2}, 1, \frac{1}{5} \\ 5, 2, 5, 1 \end{bmatrix} \tag{8}$$

The situation factor layer to the target layer weight is k = [0.2406, 0.2144, 0.1255, 0.4194]. The conformance test passed. According to formula (8), the degree of connection between the data and each element in the feature vector group is obtained, and the association degree array is formed.

4.2 Experimental Results

The security value of network information is obtained by counting the percentage of running states of all nodes in wireless communication network. The nodes matching one of the 15 types of normal operation data are considered as normal running nodes, and the nodes matching with one of the three types of abnormal operation data are considered as abnormal running nodes, and the nodes without classification or lack of data are classified as uncertain states. In this experiment, 11 groups of tests were carried out, and the attack intensity of the nodes in different test groups was different. In order to verify the effectiveness of this method, this experiment will choose the busy time of network use, that is, the time range is 6:00–24:00. Because most users are in the rest stage between 0:00–5:59, the frequency of network operation is low during this period, so it is not used as the detection period of this experiment. Where the formula for calculating the information security value and the percentage of nodes attacked in the network is:

$$N_i = \frac{kf_n}{\Delta S_{t+1}} \tag{9}$$

Through the previous analysis, when all the nodes are the information security values of wireless sensor networks, the information security values of sensor networks show a downward trend. Therefore, if this method is tested, if the same situation occurs, it indicates that the proposed method is effective and accurate. The relationship between the information security value of a wireless sensor network and the percentage of the node being attacked in the network is shown in Figs. 2 and 3:

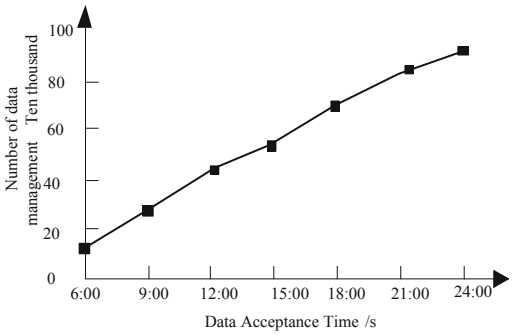

Fig. 2. Traditional forecasting model

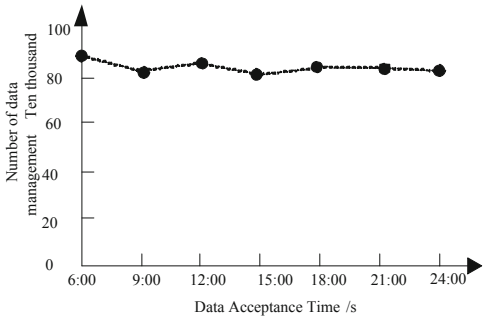

Fig. 3. Quantitative risk Assessment model of wireless communication network information security under large data

Through the analysis of experimental results, when the network tends to be absolutely safe, the wireless sensor network information security value is 35385 (prone to infinity). As the network attack frequency increases gradually, the sensor network information security value begins to decrease, when all nodes in the network are The wireless sensor network information security value is 2.61610 when attacked. As shown in Fig. 2, the abscissa is the frequency of the network attack (attack strength), and the ordinate is the security posture value calculated according to formula (7). According to the figure, the information security of the wireless sensor network decreases with the increase of attack intensity.

The margin of network information security is the amount by which the percentage of attacked nodes in the network increases by one percentage point, and the network information security value decreases. In order to verify the effectiveness of the model, the marginal rate of network information security of the model and the traditional model are compared, and the comparison results are shown in Table 3.

Table 3. Network information security marginal rate

Attack strength	Network information security edge rate /%		
	Running results of this model	Results of traditional model operation	Actual operation results
Very low	98.22	86.24	98.67
Low	85.56	76.03	85.23
Medium	76.83	52.88	76.15
High	63.45	32.86	63.40
Very high	52.05	20.53	51.98

It can be seen from Table 3 that with the increase of network attack intensity, the marginal value of information security of the two models gradually decreases, indicating that the two models are more sensitive to the changes of low-intensity attacks. The result of this model is higher than that of the traditional model, which is consistent with the actual operation. It shows that this model can correctly evaluate the security and risk of wireless communication network information.

5 Concluding Remarks

This paper analyzes the quantitative evaluation model of information security risk in wireless communication network under big data, and provides a model for calculating the probability of information security risk occurrence and a way of calculating information security risk loss. It is beneficial to protect the information security of organizations and individuals.

References

1. Liu, H.: Security evaluation and simulation of privacy information transmission based on big data analysis. Comput. Simul. **35**(2), 342–345 (2018)
2. Chen, X., Chen, H., Wang, C., et al.: Information security risk assessment based on BP neural network. Inf. Commun. **184**(4), 170–171 (2018)
3. Li, L., Lian, Y.: Network information security transmission simulation of large data mobile terminal. Comput. Simul. **35**(6), 194–198 (2018)
4. Chai, J., Wang, S., Liang, H., et al.: Quantitative method of information security risk assessment elements based on analytic hierarchy process. J. Chongqing Univ. **40**(4), 44–53 (2017)
5. Wang, H., Fan, K., Mo, W.: Information security risk assessment based on improved DS evidence theory and BN. Telev. Technol. **41**(6), 24–30 (2017)
6. Guan, T.: Design and implementation of information security risk assessment system for electric power industry. Netw. Secur. Technol. Appl. **11**, 122–124 (2017)
7. Tang, W., Wang, J., Yang, R., et al.: Quantitative risk assessment of large power grid operation based on support vector machine. J. Hefei Univ. Technol. (Nat. Sci. Ed.) **40**(4), 486–491 (2017)

8. Fu, C., Wang, X., Zhang, W., et al.: A component security attribute model driven information security risk assessment approach for train control center. Tiedao Xuebao/J. China Railw. Soc. **39**(8), 77–84 (2017)
9. Chai, T., Weng, J., Xiong, D.Q.: Development of a quantitative risk assessment model for ship collisions in fairways. Saf. Sci. **91**, 71–83 (2017)
10. Jing, X., Hu, H., Yang, H., et al.: A quantitative risk assessment model involving frequency and threat degree under line-of-business services for infrastructure of emerging sensor networks. Sensors **17**(3), 642 (2017)