Security Risk Assessment for Miniature Internet of Thing Systems with 5G

Wei Chen[1,2], Lei Wang[1,2], Fangming Bi[1,2(✉)], Chaogang Tang[1,2], and Senyu Li[1,2]

[1] School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, Jiangsu, China
bfm@cumt.edu.cn

[2] Mine Digitization Engineering Research Center of the Ministry of Education, China University of Mining and Technology, Xuzhou 221116, Jiangsu, China

Abstract. In order to improve the traditional analytic hierarchy process method, information entropy and interval fuzzy number are introduced to AHP respectively on the weight of the hierarchy and the weight of the index. The effectiveness of the improved method is tested by a Simulation example which is based on risk assessment index system of miniature Internet of things system. Meanwhile, 5G as the fifth generation of mobile communication technology, will be widely used in entertainment, health care, education and autonomous driving. It will extend the capabilities of various applications on our personal devices and wearable devices will fill every corner of our lives by the application with miniature Internet of thing systems. At the same time, 5G also faces the threat of information security risk, which is our paper concerned.

Keywords: Security risk assessment · Analytic hierarchy process · Information entropy · Interval fuzzy number · 5G

1 Introduction

The Internet of things emerged as the times require which makes the new forms of network combined with various traditional and new industry applications, by using Internet platform as the backbone. Trust-based communication can greatly enhance the performance of sensor-cloud for Internet of things [1]. There is an essential difference between the Internet of things with the existing Internet and mobile communication network [2, 3]. Nowadays, the security problem has become an important problem that hinders the further development of the Internet of things [4]. How to extend the information security protection to the extension of the Internet of things system and how to protect the privacy information while sharing data in the Internet of things are the most significant problems need to be solved in the current research on the security of the Internet of things [5]. Meanwhile, 5G as the next generation of wireless technologies will bring our society into a new statement. 5G wireless networks with big-data-driven and big-data-assisted can be widely used. Another promising application scenario of fifth generation (5G) wireless communications is vehicle-to-everything (V2X).

V. C. M. Leung et al. (Eds.): 5GWN 2019, LNICST 278, pp. 174–181, 2019.
https://doi.org/10.1007/978-3-030-17513-9_12

It also can be used to meet the demand of explosive mobile data. Ultra sense network is a solution for the 5G networks. It seems that 5G has a bright future, but some risks cannot be ignored. Information security risk assessment is one of the necessary things that should be emphasized.

In this paper, we present an information security risk assessment method based on improved analytic hierarchy process. The paper is organized as follows. Firstly,the theoretical background is briefly introduced in Sect. 2. Secondly, Sect. 3 presents the information security risk assessment model based on improved AHP. Thirdly, Sect. 4 presents the illustrative example. Finally, Sect. 5 contains the conclusions.

2 Related Works

2.1 IOT Security

The Internet of things market develops rapidly, the number of terminals increases sharply, and there are big security risks. The proportion of security links in the industrial chain of the Internet of things is low. The Internet of things has gone deep into many industries and affected people's lives in an all-round way. The main contents of IOT security include: data security, network security and node security.

(1) Data security
Due to the fierce growth of IOT devices and IOT data, the large amount of data generated by IOT systems poses a serious threat to people's privacy. In response to this threat, Toch et al. [6] proposed a classification method for information security and privacy risk assessment based on data exposure level, individual user identification level, data sensitivity, user control over monitoring and data collection and analysis. In addition to risk assessment of IOT data, Radanliev and Liu et al. [7], [8] predicted the future risk of IOT network based on test and verification of real data.

(2) Network security
Advanced persistent threats (APTs), combined with many different forms of attack, are becoming a major threat to network security. Existing security protections typically focus either on one-off situations or on weaknesses that separate detection from response decisions. Li et al. [9] proposed a security perception defense mechanism based on threat intelligence support, which introduced priority perception virtual queue to make robust defense strategies based on acquired heterogeneous knowledge. Likewise, the nature of industrial networks often impedes the adoption of classic security approaches, especially popular solutions based primarily on a philosophy of detection and patching. Cheminod et al. [10] evaluated the status quo of a class of industrial distributed computing systems from the perspective of security, and analyzed the characteristics of the system, the artistic standardization of the current state and the adoption of appropriate control (countermeasures), which can help reduce the security risk below a predefined and acceptable threshold.

(3) Node security
Node security is becoming a promising example of protecting wireless communications from eavesdropping between legitimate users because the primary link from source to destination has better propagation conditions than the

eavesdropping link from source to eavesdropper. Codetta-Raiteri et al. [11] used decision network (DN) to analyze attack/defense scenarios in critical infrastructure, and they could directly use reasoning algorithm to carry out probability analysis on the risk and importance of attack. In order to reduce interrupt probability (OP), Zou et al. [12] proposed opportunity relay selection (ORS) and quantified the improvement of SRT while increasing the number of relays.

2.2 Security Target System of the Internet of Things

'EPCGlobal' Internet of things architecture is currently one of the most representative architecture of the Internet of things [13]. The architecture divides the Internet of things into three levels: the perception layer, the network layer and the application layer.

(1) Perceptual layer
The perception layer of Internet of things is the foundation of data acquisition by Internet of things. It mainly uses video recognition, wireless terminals, sensors and other data acquisition devices to realize real-time perception and collect basic data. At the same time, the trust-based sensors also have an executive control system to perform simple control operations [1].

(2) Network layer
The network layer of the Internet of things is usually based on the existing mobile communication network or the Internet. It mainly realizes the function of information transmission and aggregation, and transmits, integrates and spreads large scale information through the network [14]. At the same time, the network layer also contains certain functions of managing and processing the acquired perceptual data. Using Cloud computing as a platform for data storage and analysis of the Internet of things is the key to connect the Internet layer and application layer. The researchers developed a complex formal mathematical decision model to support the selection of cloud computing services in multi-source scenarios [1, 15].

(3) Application layer
The application layer of the Internet of things acquires perceptual information from the supporting platform such as the Internet of things data center, and provides various services for users by using the acquired information. At present, there are more and more applications of Internet of things including public management, intelligent transportation, smart home [16], medical and health, public safety and other fields, but the whole system is not sound enough. The common Internet of things applications includes monitoring applications, payment applications, query applications, and so on. Android has emerged as the widest-used operating system for smartphones and mobile devices. Security of this platform mainly relies on applications (apps) installed by the device owner since permissions [17].

2.3 Analytic Hierarchy Process

Risk assessment may be a necessary process in Internet of things network security, and one deliverable can be used to deal with threats, thus promoting the formulation of security strategy [18]. Analytic hierarchy process (AHP) is often used as a qualitative and quantitative analysis method in the process of risk assessment [19]. The first task of

using analytic hierarchy process to evaluate a system is to build a hierarchical model. Then some qualitative and unquantifiable factors are quantified on the basis of the hierarchical model, and some quantitative data are obtained through processing and analysis to help decision-makers to make decisions [8].

Traditional AHP method for information security risk assessment can be generally divided into four steps:

Step 1. Hierarchical structure model of the system
This step aims to analyze the relevant elements of the system. Then stratify the system according to a certain standard. We usually divide the system into three layers: the target layer, the criterion layer and the scheme layer.
Step 2. Structure judgment matrix
Judgment matrix is formed to calculate the weight of criteria. To compare in a more efficient way, nine point scales have been proposed as is shown in Table 1.

Table 1. The numerical scale in AHP used in the paired-comparison.

Significance	Description
1	Two elements are equally important
3	One element is weakly important than another
5	One element is important than another
7	One element is strongly important than another
9	One element is absolutely important than another
2, 4, 6, 8	These are intermediate values of decision

Step 3. Calculating the relative weight of the single layer
Calculating the characteristic vector of the judgment matrix and then normalize the characteristic vector to get the weight of the single layer.
Step 4. Calculating the final combination weights of each layer element.

3 Information Security Risk Assessment Model

In the evaluation process of AHP, the accuracy of the hierarchy weight depends on the construction of the judgment matrix. When the traditional analytic hierarchy process (AHP) is used to integrate the different evaluation results of the same scheme, a simple method of calculating the average value is often used, and the information behind the difference is ignored. Therefore, the concept of entropy and entropy method is introduced. With entropy method, weight is adjusted according to the difference of evaluation.

After optimization, the process of AHP risk assessment model can be express six steps as Fig. 1.

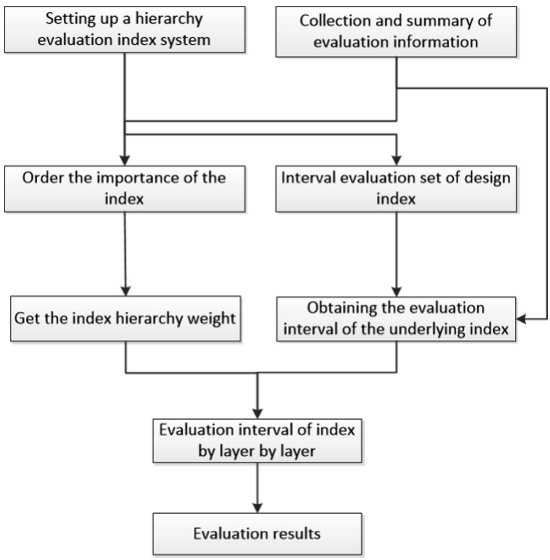

Fig. 1. Structure chart of improved AHP risk assessment model

Firstly, establish the hierarchy index system. According to the actual risk status of the system, the risk factors of the system are identified by risk identification, and the corresponding evaluation index is constructed. According to the common characteristics of the indicators, it is rationally designed into a hierarchical index system structure.

Secondly, obtaining the importance order of each layer. Through the assessment of the system security experts or senior managers, the importance of the indicators in the risk assessment index system is classified according to the 1–9 scale method independently. The corresponding judgment matrix is constructed according to the ranking results.

Thirdly, calculating the weight of the index. For different experts or executives, the weight matrix is calculated by AHP and the consistency test is carried out. After passing the test, it is merged into index weight matrix. Then entropy weight is used to solve the entropy weight of the index weight matrix, and the weight of index level is adjusted by entropy weight.

Fourthly, constructing interval evaluation set of index evaluation value. According to the actual situation of the risk assessment, a reasonable interval evaluation set is designed. The evaluation set should be as concise and reasonable as possible so that the investigator can understand the meaning of the evaluation clearly, and the manager can also determine the risk condition according to the result of the evaluation.

Fifthly, getting the evaluation value interval of the lowest index. According to the results of the risk assessment, the evaluation value interval of each lowest evaluation index is solved. In order to ensure the rationality of the evaluation results, the method of removing the extremes at the both ends can be taken to get the interval vector of the lowest index evaluation value.

Sixthly, combining the index hierarchy weight and index evaluation value interval, the evaluation value interval corresponding to the last layer of index is solved from bottom to top, and the comprehensive evaluation result of the whole evaluation system is finally obtained.

4 Simulation Experiment

In order to verify the correctness of the improved AHP risk assessment model, this chapter takes a miniature Internet of things system as an example to study the risk assessment model proposed above.

The risk assessment questionnaire is built on the basis of the four level evaluation index in the risk assessment system. 30 survey results were randomly selected as the basis for evaluating the importance of indicators. The distribution of evaluation results is shown in the following Table 2.

Table 2. Evaluation results of index importance

Forth level index	Very high	High	Medium	Low	Very low
Physical environment of outdoor equipment (X_{111})	2	7	17	4	0
Physical environment of internal equipment (X_{112})	0	4	9	14	3
Maintenance degree of hardware operation management (X_{113})	1	3	7	11	8
Degree of completeness of information security software (X_{121})	0	2	11	14	3
System security log (X_{122})	4	11	11	3	1
System access control (X_{123})	3	14	7	4	2
System update maintenance (X_{124})	1	7	14	6	2
Degree of completeness of database management (X_{131})	0	3	5	17	5
Data access control (X_{132})	6	10	7	6	1
Data secrecy (X_{133})	4	9	8	6	3
Influence of internal factors (X_{141})	0	2	4	11	13
Influence of external factors (X_{142})	1	0	5	10	14
Communication encryption (X_{211})	2	2	9	11	6
Communication access control and authentication (X_{212})	4	3	16	5	2
Attack protection (X_{213})	1	4	12	7	6
Security of communication platform (X_{214})	0	1	15	10	4
Information flow control (X_{221})	2	4	17	4	3
Environmental awareness and protection (X_{222})	0	3	12	14	1
Security level division (X_{223})	3	2	9	9	7
Technical level of staff (X_{311})	1	1	11	14	3
Staff safety awareness level (X_{312})	4	4	7	9	6
Staff supervision and management system (X_{313})	2	5	14	8	1
User operation specification (X_{321})	6	4	12	5	3
User safety awareness and attitude (X_{322})	4	7	8	10	1

With this evaluation method, when setting the risk response strategy, we can evaluate the specific details by combining the interval of index evaluation value and the hierarchy weight. For example, it can be seen from the evaluation value of the fourth level index that the system has loopholes in the authority management, which needs to be further improved, as well as the second level index from the level weight. The risk of data communication in the system has the highest weight, and the risk should be increased in the process of risk management and control. The risk control and management measures of information security are reasonably set up through comprehensive index weight and risk value interval.

5 Conclusion

Risk assessment is the cornerstone of information system security. After intensive study of relevant standards and methods in this field, comprehensive understanding of relevant theories and investigation and evaluation of the implementation process this paper deeply studies the risk assessment method based on hierarchical analysis and neural network, and establishes an index body of information security risk assessment based on the miniature Internet of things system. Furthermore, we put forward the improved AHP risk assessment model. Meanwhile, we emphasized the importance of information security risk assessment as a solution for the 5G networks. The effectiveness of the simulation test is tested. However, there are still some subjective factors in the evaluation process, and the information entropy cannot deal with the situation that only a few experts give the correct evaluation results. These problems remain to be solved further.

Acknowledgement. The research is supported by National Natural Science Foundation of China (Grant No. 51874300), the National Natural Science Foundation of China and Shanxi Provincial People's Government Jointly Funded Project of China for Coal Base and Low Carbon (Grant No. U1510115), National Natural Science Foundation of China (Grant Nos. 51874299, 51104157), the Qing Lan Project, the China Postdoctoral Science Foundation (Grant No. 2013T60574), the Ph.D. Programs Foundation of Ministry of Education of China (Grant No. 20110095120008) and the China Postdoctoral Science Foundation (Grant No. 20100481181).

References

1. Feng, J.Y., Liu, Z., Wu, C., Ji, Y.S.: Mobile edge computing for internet of vehicles: offloading framework and job scheduling. IEEE Veh. Technol. Mag. **14**(1), 28–36 (2019)
2. Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D.: Sensing as a service model for smart cities supported by Internet of Things. Trans. Emerg. Telecommun. Technol. **25**(1), 81–93 (2014)
3. Wang, X., Liu, Z., Gao, Y., Zheng, X., Chen, X., Wu, C.: Near-optimal data structure for approximate range emptiness problem in information-centric Internet of Things. IEEE Access **7**, 21857–21869 (2019)
4. Marett, K., Vedadi, A., Durcikova, A.: A quantitative textual analysis of three types of threat communication and subsequent maladaptive responses. Comput. Secur. **80**, 25–35 (2019)

5. Mohsin, M., Sardar, M.U., Hasan, O., Anwar, Z.: IoTRiskAnalyzer: a probabilistic model checking based framework for formal risk analytics of the Internet of Things. IEEE Access **5**, 5494–5505 (2017)
6. Toch, E., et al.: The privacy implications of cyber security systems: a technological survey. ACM Comput. Surv. **51**(2), 36:1–27 (2018)
7. Radanliev, P., et al.: Future developments in cyber risk assessment for the internet of things. Comput. Ind. **102**, 14–22 (2018)
8. Wu, C., Liu, Z., Zhang, D., Yoshinaga, T., Ji, Y.S.: Spatial intelligence toward trustworthy vehicular IoT. IEEE Commun. Mag. **56**(10), 22–27 (2018)
9. Li, Y.Q., Dai, W.K., Bai, J., Gan, X.Y., Wang, J.C., Wang, X.B.: An intelligence-driven security-aware defense mechanism for advanced persistent threats. IEEE Trans. Inf. Forensics Secur. **14**(3), 646–661 (2019)
10. Cheminod, M., Durante, L., Valenzano, A.: Review of security issues in industrial networks. IEEE Trans. Industr. Inf. **9**(1), 277–293 (2013)
11. Codetta-Raiteri, D., Portinale, L.: Decision networks for security risk assessment of critical infrastructures. ACM Trans. Internet Technol. **18**(3), 29:1–22 (2018)
12. Zou, Y.L., Wang, X.B., Shen, W.M., Hanzo, L.: Security versus reliability analysis of opportunistic relaying. IEEE Trans. Veh. Technol. **63**(6), 2653–2661 (2014)
13. Bandyopadhyay, D., Sen, J.: Internet of Things: applications and challenges in technology and standardization. Wirel. Pers. Commun. **58**(1), 49–69 (2011)
14. Xu, D.Y., Ren, P.Y., Ritcey, J.A.: Independence-checking coding for OFDM channel training authentication: protocol design, security, stability, and tradeoff analysis. IEEE Trans. Inf. Forensics Secur. **14**(2), 387–402 (2019)
15. Martens, B., Teuteberg, F.: Decision-making in cloud computing environments: a cost and risk based approach. Inf. Syst. Front. **14**(4), 871–893 (2012)
16. Jacobsson, A., Boldt, M., Carlsson, B.: A risk analysis of a smart home automation system. Future Gener. Comput. Syst. Int. J. Escience **56**, 719–733 (2016)
17. Deypir, M., Horri, A.: Instance based security risk value estimation for Android applications. J. Inf. Secur. Appl. **40**, 20–30 (2018)
18. Gritzalis, D., Iseppi, G., Mylonas, A., Stavrou, V.: Exiting the risk assessment maze: a meta-survey. ACM Comput. Surv. **51**(1), 11:1–30 (2018)
19. Xu, N., Zhao, D.M.: the research of information security risk assessment method based on AHP. In: Wu, Y.W. (ed.) Sports Materials, Modelling and Simulation, vol. 187, pp. 575–580. Trans Tech Publications Ltd., Stafa-Zurich (2011)