Research Progress and Future Trend Analysis of Network Security Situational Awareness

Junwei Zhang[1](✉), Huamin Feng[2], Biao Liu[2], Ge Ge[3], and Jing Liu[4]

[1] School of Cyber Engineering, Xidian University, Xian 710126, China
zhangjunwei@stu.xidian.edu.cn
[2] Beijing Electronic Science and Technology Institute, Beijing 100070, China
{fenghm,liubiao}@besti.edu.cn
[3] National Administration of State Secrets Protection, Beijing 100031, China
[4] School of Cyberspace Security, Beijing University of Posts and Telecommunications,
Beijing 100876, China
liudingjing@bupt.edu.cn

Abstract. With the continuous expansion of the network scale in recent years, network security problems have become increasingly prominent, and network security incidents have emerged one after another. Network security situation awareness is an essential part of network security defense that allows cybersecurity operators to cope with the complexity of today's networks and threat landscape. In this paper, we thoroughly review and systematize the origin and the models of network security situational awareness and the evolution of its definition, and then we give its definition. Additionally, we introduced the key technologies in this field from the three functional modules of network security situation extraction, network security situation assessment, and network security situation prediction, and analyzed their advantages and disadvantages. Last but not least, we explicitly propose four possible research directions that the researchers in network security can work on in the future.

Keywords: Network security · Situation awareness · Situation assessment · Situation prediction · Artificial intelligence

1 Introduction

Cyberspace has become the fifth national security domain outside the sea, land, air, and sky. Cyberspace security has become an important part of national security. However, with the rapid development of the scale of cyberspace, the problem of network security is becoming increasingly serious. Globally, there have been many serious cybersecurity incidents in recent years. such as the extortion outbreak in May 2017, "WannaCry", by encrypting data information in the system, make originally the data is not available, the opportunity to extort money a lot, "WannaCry" virus spread across nearly 150 countries and regions, including education, transportation, medical, energy networks, many industries are major attack by the virus. In April 2020, EDP, a Portuguese multinational

J. Xiong et al. (Eds.): MobiMedia 2021, LNICST 394, pp. 537–549, 2021.
https://doi.org/10.1007/978-3-030-89814-4_39

energy company, was attacked by ransomware. After being attacked, the attacker claimed to have obtained 10TB of EDP's sensitive data files and finally extorted a ransom of 1,580 bitcoins (equivalent to about 9.9 million euros).

For common vicious network security incidents, most network administrators are hindsight, that is, the event caused a certain impact was noticed, therefore, how to do active monitoring and active defense before the threat comes, try to avoid or reduce the occurrence of network security incidents, network security managers are very urgent needs [1]. In this paper, the origin and definition of network security situational awareness are summarized, and the technical methods of functional modules are introduced, analyzed, and compared. The research trend of network security situational awareness in the next few years and the challenges that researchers may face are proposed.

2 Definition and Development of Network Security Situational Awareness

In 1988, Endsley [2] proposed the concept of situational awareness for the first time at the International Human Factor Annual Conference, that is, "to recognize and understand environmental factors within a certain time and space, and to predict the future development trend".

Endsley's definition of situational awareness [3] has been widely accepted and applied to a variety of functional areas. He understands situational awareness as a state of knowledge and distinguishes it from the process used to achieve such a state by dividing it into three levels: situational element extraction, situational understanding, and situational prediction, as shown in Fig. 1.

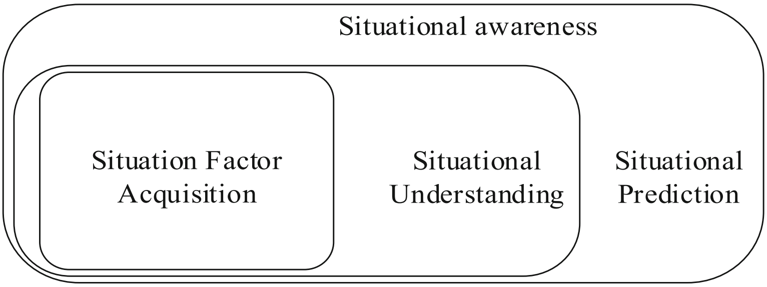

Fig. 1. Endsley situational awareness model.

First is the situation factor extraction, the main work of this level is to obtain the necessary data; the second level, situational understanding, is to analyze the data obtained from the first level. Finally, the situation prediction is made [4]. The data analysis results obtained at the second level are used to predict the situation in the short term in the future. This is also the earliest situational awareness model, which is the foundation of the network security situational awareness model.

A more classic situational awareness model is the data fusion model given by THE U.S. military JDL (Joint Directors of Laboratories), also known as the JDL model [5].

In this model, situational awareness is divided into five stages. In this model, situational awareness is divided into five stages. Followed by data preprocessing, event extraction, situation assessment, impact assessment, resource management, process control, and optimization. The main task is to monitor and evaluate the entire data fusion process in real-time, and integrate information at various levels to optimize related resources [6].

In 1999, the United States air force communications and information center Tim Bass, put forward the network space situational awareness (cyberspace situational awareness, CSA) concept [7], for the first time the concept of situational awareness is academia fusion in the field of network space safety, can effectively improve the cognition of managers to protect the network aims to shorten the time of the network security management decisions and provide the corresponding decision.

The situational awareness in the network applications mainly revolves around safety, Tim Bass in 2000 intrusion detection framework based on multisensory (see Fig. 2) [8]. The model is the prototype of network security situational awareness, reasoning framework consists of intrusion detection, intruder identity recognition, intrusion behavior, situation assessment, and threat assessment, etc.

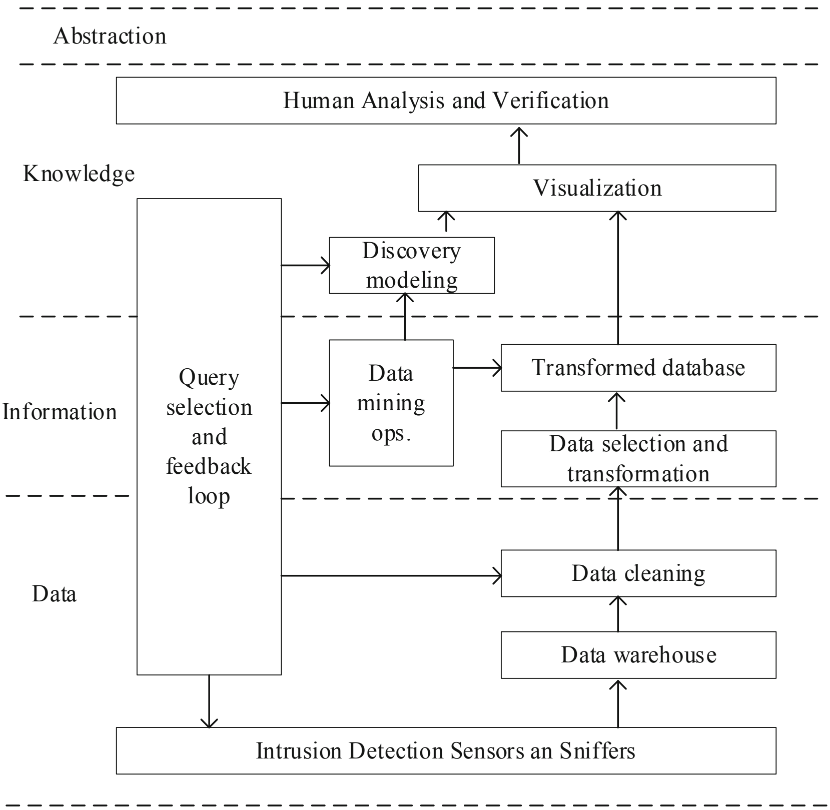
Abstraction
Human Analysis and Verification
Knowledge
Visualization
Discovery modeling
Information
Query selection and feedback loop
Data mining ops.
Transformed database
Data selection and transformation
Data
Data cleaning
Data warehouse
Intrusion Detection Sensors an Sniffers

Fig. 2. Intrusion detection data fusion model.

In 2006, Wang Hui Qiang [9] discussed the concept of cybersecurity situational awareness, thinking that it refers to "in a large-scale network environment, acquiring, understanding, displaying, and predicting future development trends of security elements that can cause changes in the network situation", this definition is a Chinese translation defined by Endsley.

In 2007, Lai Ji Bao, Wang Hui Qiang et al. [10] proposed a network security situational awareness model based on Netflow. Using Netflow technology can well realize network security situation awareness, discover potential threats and vulnerabilities promptly, and present them to decision-makers in a visual manner, to achieve the purpose of comprehensive monitoring of the entire network. At the same time, because the system is dealing with massive amounts of data and information, performance optimization issues need to be further studied.

In 2009, Wei Yong et al. [11] proposed a network security situational awareness model based on information fusion. Introduce the improved DS evidence theory to fuse information from multiple data sources, and then use vulnerability information and service information to calculate the network security situation through situation element fusion and node situation fusion, and perform time-series analysis to achieve a quantitative analysis of the network security situation and trend forecasting.

In 2011, Jia Yan et al. [12] proposed a security situational awareness model for large-scale networks because of the characteristics of massive, multi-mode, and multi-granularity data in large-scale networks.

In 2014, Franke U [13] regarded network situational awareness as a subset of situational awareness, that is to say, network situational awareness is a part of situational awareness, which refers to the "network" environment. But that definition is a bit too vague and doesn't specify whether it's situational awareness for security.

In 2017, Gong Jian [14] put forward the network security situational awareness is the cognitive process of the network system security status, including from the system to measure the raw data fusion processing step by step and the background of the implementation of the system state and activity of semantic extraction, identify the existence of all kinds of network activity and the intention of abnormal activity, thus obtained according to the characterization of the network security situation and the trend of network system impacts normal behavior.

In 2019, Jia Yan and others [15] proposed the definition of network security situation awareness as the detection, extraction, understanding, evaluation, and future prediction of security elements that affect the network situation in a large-scale network environment.

With the improvement of application security requirements and technical difficulties, in recent years, academic research on network security situational awareness has become more and more common and in-depth. However, at present, a unified and comprehensive definition of network security situational awareness has not yet been formed, and most of them are correct. A detailed explanation of Endsley's definition of situational awareness. In this article, network security situation awareness is defined as the extraction of the characteristic elements that affect the network security situation in a complex network environment, and the necessary fusion and classification of the extracted characteristic elements, and then the use of technical methods for evaluation and analysis, and finally a series of complex processes for predicting the network security situation in the future based on the evaluation results.

3 Key Technologies of Network Security Situational Awareness

Although there are still some problems in the division of several stages of network security situational awareness by different researchers and the understanding of the relationship between different stages, most researchers divide network security situational awareness into three functional modules of situation element extraction, situation assessment, and situation prediction. This chapter introduces the key technologies of network security situational awareness in turn according to the classification of functional modules.

3.1 Key Technologies of Network Security Situation Feature Elements Extraction

Network security posture characteristic element extraction in the underlying network security situational awareness, is the foundation of network security situational awareness and security features elements mainly include static configuration of network information and dynamic information and include the information of network topology, the former vulnerability information, and status information, etc., the latter refers to the various protective measures of log collection and analysis techniques for the threat of information, etc.

When the researchers collected information, the foreign researchers mostly from a single factor analysis, specific elements of the corresponding specific data information to assess the security situation of specific, such as Jajodia [16] and Wang [17] and others study is only gathering network vulnerability information, evaluation by collecting the information of the network vulnerability, Ning [18, 19] only gathering network alarm information, analyze the status of the alarm information to evaluate the network threat; Barford [20] et al. used the data and information about the attack collected by Honeynet to evaluate the attack situation of the network. The common point of these studies is that they all collect, analyze and study a specific network element, and only obtain single situation information, which cannot obtain comprehensive information and then analyze the overall situation, and cannot adapt to the complex and changeable network environment.

Domestic researchers, on the other hand, from multi-source data information acquisition, starting from multiple layers, multiple Angle comprehensive assessment of network security situation, such as Wang Juan [21] is put forward based on the index system of network security situational awareness, extraction of multi-source information security data, according to the requirements of hierarchy, information source and the difference between structures, the layered index model, the extracted 25 candidate index, the index information assessment of network security situation; Wang et al. [22] proposed a botnet detection technology based on information fusion to effectively integrate the complex network security information of different sensors in time and space dimensions to improve the perception ability of botnet attacks. There is a lot of research is geared to the needs of the extraction of multi-source heterogeneous information network security work [23–26], Chang Yiheng and others proposed a security situation element extraction meth-od based on probabilistic neural network, which solved the problem of low efficiency and low accuracy of situation element extraction in a complex network environment. Multisource and redundant data interference for safety information [27]. Duan Yongcheng proposed a network security situation factor extraction method based on information gain random forest, which greatly improves the accuracy of situation factor extraction [28]. These studies use different technologies to collect and collate multi-source security data.

In conclusion, the foreign researchers mostly focus on the single factor extraction and analysis of the domestic researchers tend to the extraction of multi-source elements, because the characteristic of the network security situational awareness is a fusion of a variety of network information to consider the overall situation of network security, therefore, the elements of a multi-source extraction are inevitable, but the multi-source data and information not only reduces the extraction efficiency, desultorily data also brings to the information fusion and redundant processing difficulty, at present the optimization of the extraction method has a lot of space.

3.2 Key Technologies for Network Security Situation Assessment

Network security situation assessment is the core part of network security situation perception. Based on the fusion of all kinds of security equipment data and according to the needs of network security assessment, an assessment value of the current network security situation is obtained through formal reasoning calculation with the help of some mathematical model. In short, network security situation assessment is a mapping from situation factor to situation result value [29]. The network security situation assessment methods can be divided into three categories: mathematical model-based, knowledge-based reasoning, and pattern recognition.

Situation assessment method based on the mathematical model is the most common and most common method of analytic hierarchy process, the domestic has the value of the discloser is Chen Xiu Zhen and others [30] in 2006 put forward the hierarchical network system security threat situation of the quantitative evaluation model, this model can be divided into network system from top to bottom, host, service, and attack/holes 4 levels, as shown in Fig. 3, taking the evaluation of overall “after” top-down, local first strategy, and the model is based on IDS mass alarm information and network performance indicators, and the importance of the service, the host itself and the organizational structure of the network system combining.

The model exists some deficiencies: only IDS alert information in its assessment method a safe source of information in the actual network system deployment, such as firewall, system log safety factors are indispensable, if not the information included in the calculation, it loses the network security situation assessment technology can comprehensively reflect the advantage of the network security situation. Therefore, in 2009, 2010, and 2012 respectively, Lai Ji Bao [31], Zhang Yong [32], and Meng Jin [33] all improved the above hierarchical model, making the effect of more sources of hierarchical evaluation more accurate. In 2015, Jia et al. [34] proposed a layered framework for network security situation assessment. The framework can reflect the

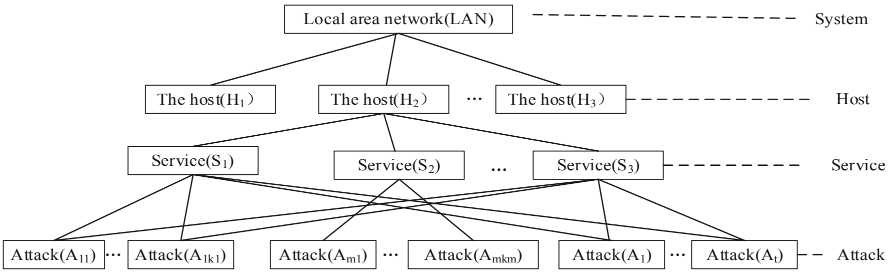

Fig. 3. Hierarchical network system security threat situation quantitative assessment model.

security status of information systems, but the disadvantage is that the framework is suitable for offline analysis, but it is not well suited for real-time analysis.

The main characteristic of the knowledge-based inference method is to rely on expert knowledge and experience in the process of constructing an evaluation model and then analyze network security situations through logical reasoning. More common are fuzzy logic reasoning, Bayesian reasoning, evidence theory, and so on.

Xie et al. [35] used a Bayesian network to model the uncertain factors in the network, calculate the probability of a successful attack, and evaluate the severity of the attack in real-time. Aguilar et al. [36] is a combination of fuzzy logic and neural network technology, base on the cognitive map presents the FCM (fuzzy cognitive map, the fuzzy cognitive map), the concept of using it to get important assets in a network dependence of damage assessment, fuzzy reasoning too difficult, however, and the figure of storage cost is big, not suitable for large, complex network environment. Boyer et al. [37] designed a situation assessment framework based on DS evidence theory to quantify network security situation. Li et al. [38] introduced a Bayesian network-based evidence network to carry out network security situation assessment, and the main idea is to carry out a similar reasoning assessment under the framework of evidence theory and with the full probability formula of Bayesian network as a reference. Yang Hao et al. [39] obtained the network vulnerability situation value by integrating vulnerability data and alarm data through DS evidence theory. The network security situation assessment method based on knowledge reasoning has a certain artificial intelligence, but the difficulty of obtaining inference rules and prior knowledge is the bottleneck of this method. Although the advantage of the evidence theory is that the required prior data is easy to obtain and can integrate different expert knowledge and data source information, it is also undesirable to have too high computational complexity when evidence conflicts.

The pattern recognition method establishes a situation template through machine learning and divides situations through pattern matching and mapping. More advanced than knowledge reasoning, it does not rely too much on expert knowledge and experience. The main methods include the grey correlation method, rough set theory, and cluster analysis method. Many researchers [40–45] have adopted grey correlation analysis, rough set theory, and cluster analysis to carry out network security situation assessment and achieved good results. The evaluation method of pattern recognition has the advantages of high efficiency, large processing capacity, and not relying too much on expert knowledge. The disadvantage is that the stage of pattern extraction is difficult to face more complex features, thus affecting the evaluation efficiency.

3.3 Key Technologies for Network Security Situation Prediction

The ultimate purpose of an evaluation is to predict and use historical data information to provide a management basis for future network security, which is the transformation from passive to active network security management. Network security situation prediction is the highest level of the whole situation perception and plays an important role in the defense of network security [46]. At present, research on network security situation prediction methods can be roughly divided into three categories: machine learning, Markov model [47], and gray theory.

Thanks to the improvement of hardware computing speed, machine learning methods based on neural networks and deep learning have developed rapidly in recent years. In the field of network security situational awareness, the automatic perception and self-learning mechanism of machines can be established to fit the thinking ability and analysis, and judgment ability of experts, to predict complex network security events more flexibly [48]. Lin et al. proposed a network security situation prediction based on BP neural network, and Tang [49] proposed a network security situation prediction method based on dynamic covariance BP neural network. The disadvantage of the BP neural network is its slow convergence speed, ease to fall into the local optimal solution, and ease to oscillate in the learning process. In addition to BP neural network, Zhang et al. [50] established a parametric optimized wavelet neural network security situation prediction model by using an improved niche genetic algorithm to improve the prediction accuracy of the network security situation. Feng et al. [51] proposed a network security situation prediction method based on cyclic neural networks. Ren Wei et al. [52, 53] proposed a situation prediction method based on RBF neural network by taking advantage of the characteristics of network security situation values with nonlinear time series and the advantages of neural network in dealing with chaotic and nonlinear data. Compared with the neural network, support vector machine (SVM) has a faster convergence speed, Hu, et al. [54] proposed a model of network security situation prediction based on graphs and SVM, and put forward by Lu and others [55] network security situation prediction based on support vector machine (SVM), is to use different methods to determine the optimal parameters of support vector machine (SVM), improve the prediction precision and shorten the training time.

Wang et al. [56] proposed a network security situation prediction method based on a fuzzy Markov chain and established a unified information base based on multi-source log data mining technology. Wen Zhi Cheng [57] proposed a prediction method based on the hidden Markov model. Liang et al. [58] proposed an algorithm based on weighted HMM to predict the security of mobile networks.

Lai Ji Bao [59] proposed network security situation prediction based on simple weighting and gray theory and established a prediction model based on gray theory. Zhang et al. [60] also carried out network security situation prediction by moving the grey correlation model and grey prediction algorithm. Deng Yong Jie et al. [61] proposed to combine neural networks with gray theory to predict network security situation, which also obtained good results.

Each forecasting technique has its advantages and limitations. Machine learning has excellent self-learning and adaptive capabilities, which can provide high convergence speed and strong fault tolerance. However, sufficient training data is needed to obtain parameters, and it is difficult to build neurons with self-learning and adaptive capabilities. For the Markov model, although it can perform various time-series predictions, it still needs a set of training data. In addition, it is almost impossible to recognize all possible states and their transitions, especially in complex networks. Grey theory can provide a small sample of data in the short-term prediction, thus providing better prediction without any training.

4 Summary and Prospect

According to the above analysis and summary, network security situational awareness started late, and many technologies are still immature and need to be further optimized and strengthened. The following is a discussion of the development trend of network security situational awareness:

First, big data analysis and processing technology. The extraction and preprocessing of network security situation elements are the most basic part of network security situation perception. The reality is that the network environment is becoming more and more complex, and the data types and formats are growing exponentially. The massive security information cannot be directly used as the analysis object of network security situation perception. Therefore, the application of big data analysis and processing technology in the extraction of network security situation elements will be the most important research in the future.

Second, the deep integration of artificial intelligence technology and network security situational awareness. The fourth part of the article introduces in detail the key technology of network security situational awareness of each function module, it is not hard to see, artificial intelligence, machine learning, researchers have become important methods in the aspect of network security situational awareness, but there are obvious flaws, artificial intelligence technology is in the rapid development phase, a new generation of artificial intelligence technology with the depth of the situational awareness can bring new vitality for the field, to solve the problems of the situation awareness at all levels to provide new methods and inspiration.

Thirdly, the visualization research of network security situational awareness. The ultimate goal of scientific research is applied. The application of cybersecurity situational awareness cannot only have some data. It needs a more direct way to express the deeper meaning of these data. Therefore, visualization is an indispensable part. However, in the process of reading related documents, it is found that there are little researches on visualization, so the visualization of network security situational awareness is also an important direction for future research.

Fourth, new problems arising from the expansion of the application scope. With the rapid development of big data and 5G, industrial control network is deeply integrated with the Internet. The new network pattern will inevitably bring new network security problems, and the application of network security situational awareness in complex network scenes will also be the focus of future research.

To summarize, network security situational awareness of research in the phase of development, there are a lot of not forming the theory of issues that need to be perfect, there are many key technologies that need to optimize modified, a new pattern of the network brings new security issues, new application scenario requires new methods of technology, network security situational awareness will exert its advantages to provide security for network security, national security escort.

Acknowledgments. This work was supported by the "High-precision" Discipline Construction Project of Beijing Universities (No. 20210071Z0403).

References

1. Gutzwiller, R., Dykstra, J., Payne, B.: Gaps and opportunities in situational awareness for cybersecurity. Digital Threats: Res. Pract. **1**(3), 1–6 (2020)
2. Endsley, M.R.: Design and evaluation for situation awareness enhancement. Hum. Fact. Soc. Annu. Meet. **32**, 97–101 (1988)
3. Endsley, M.R.: Situation awareness global assessment technique (SAGAT). In: Proceedings of the IEEE 1988 National Aerospace and Electronics Conference, Dayton, OH, USA, pp. 789–795. IEEE (1988)
4. Husák, M., Jirsík, T., Yang, S.J.: SoK: contemporary issues and challenges to enable cyber situational awareness for network security. In: Proceedings of the 15th International Conference on Availability, Reliability and Security, Virtual Event, Ireland, pp. 2. Association for Computing Machinery (2020)
5. Giacobe, N.: Application of the JDL data fusion process model for cyber security. Proc. SPIE Int. Soc. Opt. Eng. **7710**, 5 (2010)
6. Ao, Z.G.: Cyberspace operations situational awareness. In: Cyberspace operations: mechanism and planning, pp. 691–699. Publishing House of Electronics Industry, Beijing (2018)
7. Bass, T.: A glimpse into the future of ID. Login:: the magazine of USENIX & SAGE, vol. 24, pp. 40–45 (1999)
8. Bass, T.: Intrusion detection systems and multisensor data fusion. Commun. ACM **43**(4), 99–105 (2000)
9. Wang, H.: Survey of network situation awareness system. Comp. Sci. **33**, 5–10 (2006)
10. Lai, J., Wang, H., Jin, S.: Research on network security situational awareness system based on NetFlow. Comp. Appl. Res. **24**(08), 173–175 (2007)
11. Wei, Y., Lian, Y., Feng, D.: Network security situation assessment model based on information fusion. Comp. Res. Develop. **46**(3), 353–362 (2009)
12. Jia, Y., Wang, X., Han, W., Li, A., Cheng, W.: YHSSAS: security situational awareness system for large-scale networks. Comp. Sci. **38**(002), 4–8 (2011)
13. Franke, U., Brynielsson, J.: Cyber situational awareness – a systematic review of the literature - ScienceDirect. Comp. Secur. **46**, 18–31 (2014)
14. Gong, J., Zang, X., Su, Q., Hu, X., Xu, J.: Overview of network security situational awareness. J. Softw. **28**(4), 1010–1026 (2017)
15. Jia, Y., Han, W., Yang, H.: Research status and development trend of network security situational awareness. J. Guangzhou Univ. **3**, 1–10 (2019)
16. Jajodia, S.: Topological Analysis of Network Attack Vulnerability. ACM (2006)
17. Wang, L., Singhal, A., Jajodia, S.: Toward Measuring Network Security Using Attack Graphs, vol. 49. ACM (2007)

18. Pan, N.: Techniques and tools for analyzing intrusion alerts. ACM Trans. Inf. Syst. Secur. **7**(2), 274–318 (2004)
19. Pan, N., Xu, D.: Alert correlation through triggering events and common resources. In: Proceedings of the Computer Security Applications Conference, 2004, 20th Annual, pp. 360–369. IEEE Computer Society (2004)
20. Barford, P., Yan, C., Goyal, A., Li, Z., Paxson, V., Yegneswaran, V.: Employing honeynets for network situational awareness. Adv. Inf. Secur. **46**(1), 71–102 (2010)
21. Wang, J., Zhang, F., Fu, C., Chen, L.: Research on index system in network situational awareness. Comput. Appl. **27**(008), 1907–1909, 1912 (2007)
22. Hailong, W., Gong, Z.: Heterogeneous multi-sensor information fusion model for botnet detection. In: Proceedings of the 2010 International Conference on Intelligent Computation Technology and Automation, pp. 428–431 (2010)
23. Liu, X., Wang, H., Cao, B.: Network security situation awareness model based on multi-source fusion. J. PLA Univ. Sci. Technol. (2012)
24. Wu, H., Hu, A., Song, Y., Bu, N., Jia, X.: A new intrusion detection feature extraction method based on complex network theory. In: Proceedings of the 2012 Fourth International Conference on Multimedia Information Networking and Security, pp. 852–856 (2012)
25. Tsang, C., Kwong, S.: Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction. In: Proceedings of the 2005 IEEE International Conference on Industrial Technology, pp. 51–56 (2005)
26. Lai, J., Wang, H., Zheng, F., Feng, G.: Network security situation element extraction method based on DSIMC and EWDS. Comput. Sci. **37**(011), 64–69 (2010)
27. Chang, Y., Ma, Z., Li, X., Gong, D.: Security situation element extraction based on probabilistic neural network. Cybersp. Secur. **11**(128(10)), 60–65 (2020)
28. Duan, Y., Li, X., Yang, X., Yang, L.: Network Security Situation Factor Extraction Based on Random Forest of Information Gain (2019)
29. Zhang, J.: Research on some key technologies of network security situation assessment. Doctor's degree, National University of Defense Technology (2013)
30. Chen, X., Zheng, Q., Guan, X., Lin, C.: Hierarchical network security threat situation quantitative assessment method. J. Softw. **17**(004), 885–897 (2006)
31. Lai, J.: Research on several key technologies of network security situational awareness based on heterogeneous sensors. Doctor's degree, Harbin Engineering University (2009)
32. Zhang, Y.: Research and system implementation of network security situational awareness model. Doctor's degree, University of Science and Technology of China (2010)
33. Meng, J.: Research on key technologies of network security situation assessment and forecast. Doctor's degree, Nanjing University of Science and Technology (2012)
34. Jia, Y., Wu, H., Jiang, D.: A hierarchical framework of security situation assessment for information system. In: Proceedings of the 2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, pp. 23–28 (2015)
35. Peng, X., Li, J.H., Ou, X., Peng, L., Levy, R.: Using Bayesian networks for cyber security analysis. In: Proceedings of the 2010 IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2010, Chicago, USA. IEEE (2010)
36. Szwed, P., Skrzynski, P.: A new lightweight method for security risk assessment based on fuzzy cognitive maps. Int. J. Appl. Math. Comp. Sci. **24**(1), 213–225 (2014)
37. Boyer, S., Dain, O., Cunningham, R.: Stellar: a fusion system for scenario construction and security risk assessment. In: Proceedings of the Third IEEE International Workshop on Information Assurance (IWIA 2005), pp. 105–116 (2005)
38. Li, X., Deng, X., Jiang, W.: A novel method of network security situation assessment based on evidential network. In: Chen, X., Yan, H., Yan, Q., Zhang, X. (eds.) ML4CS 2020. LNCS, vol. 12486, pp. 530–539. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-62223-7_46

39. Yang, H., Xie, X., Li, Z., Zhang, L.: Simulation of network security situation estimation model under multiple intrusion environment. Comp. Simulat. **033**(006), 270–273 (2016)
40. Zhao, G., Wang, H., Wang, J.: Research on survivability situation assessment of network based on grey relational analysis. Small Microcomp. Syst. **10**, 1861–1864 (2006)
41. Wang, C.: Assessment of network security situation based on grey relational analysis and support vector machine. Appl. Res. Comp. (2013)
42. Zhuo, Y., He, M., Gong, Z.: Rough set analysis model for network situation assessment. Comp. Eng. Sci. **34**(3), 1–5 (2012)
43. Li, X., Li, X., Zhao, Z.: Combining deep learning with rough set analysis: a model of cyberspace situational awareness. In: Proceedings of the 2016 6th International Conference on Electronics Information and Emergency Communication (ICEIEC), pp. 182–185 (2016)
44. Xiao, C., Qiao, Y., He, H., Li, J.: Multi-level fuzzy situation assessment based on optimal clustering criteria. Comp. Appl. Res. **30**(4), 1011–1014 (2013)
45. Wen, Z., Chen, Z., Tang, J.: Network security situation assessment method based on cluster analysis. J. Shanghai Jiaotong Univ. (Chin. Ed.) **50**(9), 1407–1414 (2016)
46. Leau, Y.-B., Manickam, S.: Network security situation prediction: a review and discussion. In: Intan, R., Chi, C.-H., Palit, H.N., Santoso, L.W. (eds.) ICSIIT 2015. CCIS, vol. 516, pp. 424–435. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46742-8_39
47. Ioannou, G., Louvieris, P., Clewley, N.: A Markov multi-phase transferable belief model for cyber situational awareness. IEEE Access **7**, 39305–39320 (2019)
48. Lin, Z., Chen, G., Guo, W., Liu, Y.: PSO-BPNN-based prediction of network security situation. In: Proceedings of the 2008 3rd International Conference on Innovative Computing Information and Control, p. 37 (2008)
49. Tang, C., Yi, X., Qiang, B., Xin, W., Zhang, R.: Security situation prediction based on dynamic BP neural with covariance. Procedia Eng. **15**, 3313–3317 (2011)
50. Zhang, H., Huang, Q., Li, F., Zhu, J.: A network security situation prediction model based on wavelet neural network with optimized parameters. Digital Commun. Netw. 139–144 (2016)
51. Feng, W., Fan, Y., Wu, Y.: A new method for the prediction of network security situations based on recurrent neural network with gated recurrent unit. Int. J. Intell. Comput. Cybernet. **13**(1), 25–39 (2018)
52. Ren, W., Jiang, W., Jiang, X., Sun, Y.: Network security situation prediction method based on RBF neural network. Comp. Eng. Appl. **42**(31), 136–138, 144 (2006)
53. Jiang, Y., Li, C., Yu, L., Bao, B.: On network security situation prediction based on RBF neural network. In: Proceedings of the 36th China Control Conference (2017)
54. Hu, J., Ma, D., Liu, C., Shi, Z., Yan, H., Hu, C.: Network security situation prediction based on MR-SVM. IEEE Access **7**, 130937–130945 (2019)
55. Lu, H., Zhang, G., Shen, Y.: Cyber security situation prediction model based on GWO-SVM. In: Barolli, L., Xhafa, F., Hussain, O.K. (eds.) IMIS 2019. AISC, vol. 994, pp. 162–171. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-22263-5_16
56. Wang, Y., Li, W., Liu, Y.: A forecast method for network security situation based on fuzzy Markov chain. In: Huang, Y.-M., Chao, H.-C., Deng, D.-J., Park, J.J.H. (eds.) Advanced Technologies, Embedded and Multimedia for Human-centric Computing. LNEE, vol. 260, pp. 953–962. Springer, Dordrecht (2014). https://doi.org/10.1007/978-94-007-7262-5_108
57. Wen, Z., Chen, Z.: Network security situation prediction method based on hidden Markov model. J. Cent. South Univ. **46**(10), 137–143 (2015)
58. Liang, W., Long, J., Chen, Z.: A security situation prediction algorithm based on HMM in mobile network. Wirel. Commun. Mob. Comput. **2018**, 5380481 (2018)
59. Lai, J., Wang, H., Liang, W., Zhu, L.: Study of network security situation awareness model based on simple additive weight and grey theory. In: Proceedings of the 2006 International Conference on Computational Intelligence and Security, pp. 1545–1548 (2006)

60. Zhang, F., Wang, J., Qin, Z.: Using gray model for the evaluation index and forecast of network security situation. In: Proceedings of the 2009 International Conference on Communications, Circuits and Systems, pp. 309–313 (2009)
61. Deng, Y., Wen, Z., Jiang, X.: Network security situation prediction method based on grey. Theory **2**, 69–73 (2015)