Survey of Network Security Situation Awareness

Changlin He\textsuperscript{1,a}, Yufen Li\textsuperscript{2,b}

\textsuperscript{1}Information Technology Service Center Hexi University, Zhangye, Gansu, China.
\textsuperscript{2}ICC of Zhangye Power Supply Company, Zhangye, Gansu, China.
\textsuperscript{a}hecl@hxu.edu.cn, \textsuperscript{b}liyufen626@163.com

Keyword: Network security situation awareness, Model, Data fusion, Survey

Abstract: With the increasing significance of network space security continues, the research and application of network security situation awareness has gained more and more attention. In this paper, it described the development as well as the concept of network security situation awareness, then analyzed the structure model of network security situation awareness, lastly, according to the structure model from the situation factors based on multi-classifier fusion extraction, network security situation assessment as well as the prediction of network security situation, it analyzed three levels of the key technology of network security situation awareness.

Introduction

The history of the development of human society keeps along with the progress of science and technology, which is expanding the history from land, sea, air to outer space. Since it comes to the twenty-first century, with the rapid development of information technology and network technology, network space has developed into a new focus of mankind after land, sea, air and sky. The network confrontation between countries has shown a growing trend, and network space warfare has evolved into a new style of warfare, which has attracted the attention of various countries. The significance of network space has become increasingly prominent\cite{1,2}.

Today, with the rapid development of network technology, we enjoy all the convenience it brought, at the same time, we must also face the various problems of network security, network attacks are becoming more common, which is also a threat to national security. It can not achieve the effective control only rely on antivirus or firewall as well as some other traditional security management modes, we must adopt a new technical means of regulation, thus the network security situation awareness system brings up. Network security situation awareness has shown prominent advantages in emergency response, network security monitoring and the prediction of network security trend. The term "situation awareness" was proposed by Endsley in 1980s, which was firstly widely used in the aviation field. Then in 1990s, Bass and other people extended it on this basis, who gave it a new connotation, for the first time, the situation awareness was introduced in the field of network security, which laid a theoretical foundation for the study of network security situation.

Today, when security incidents happened, security managers basically ask three questions: what's going on? Why did this happen? What should I do? How to answer the first two questions constitutes the core of situation awareness in network space. Whether the last
question can have a satisfactory answer mainly depends on the situation awareness of network space.

Overview of Network Security Situation Awareness

Situation Awareness

As for situation awareness, there are too many different definitions and explanations for situation awareness. In 1995, Dr. Endsley made a distinction between situation awareness and situation assessment in the literature document[3]. It is important to adopt computer automation technology in distinguishing these two during the period of situation awareness. Situation awareness is the level of "cognition", which exists mainly in the human mind, while situation assessment is a process or set of processes that can be realized by automated technology. In literature document[4], Alberts gave another description of situation awareness, which he believed." This term is described for perception of a particular point in time, the entire battle space, or the state of a part of it. In some cases, the developing traces of the happened events, as well as the prediction of the current situation, which has been the focus of attention. Situation is consisted of tasks and task constraints, the related capabilities and intention, as well as the key environmental characteristics."

Comparing the definition of situation awareness given by Endsley and Alberts, the difference is that Alberts distinguish awareness from understanding, while Endsley regards understanding as part of awareness. Moreover, Alberts seems to imply that the analysis of situation can only serve as a cognitive process.

There are many definitions of situation awareness, but the definitions given by Endsley and Alberts are widely recognized. Since 1990s, fusion model of JDL (Joined Laboratory) data was used to describe the concept of sensor fusion and multi-sensor fusion; the results of Endsley were used to define some support situation awareness applications; while Alberts on situation awareness was defined and widely adopted in network operation and warfare.

Overview of Network Security Situation Awareness (NSSA)

The literature document[5] discussed the concept of network security situation awareness, which thought that it mean "under the large-scale network environment, focused on network security elements changes of acquisition, understanding, as well as the prediction of the future development trend." This definition basically belongs to the translation of the definition of Endsley, which lacks the content of network security situation awareness in the network security situation, and the understanding of the network security situation awareness target is incomplete. The literature document[6] is based on the analysis of the predecessors, then it gave a new definition, who thought that "network security situation awareness is the cognitive process of the security status of the network system, including the original data measured from the system step by step to the fusion extraction process as well as the realization of the background condition and activity of the semantic system, so as to identify the existence of intention all kinds of network activities and the abnormal activities. Then it can obtain the understanding on the normal behavior of the network security situation trend as well as the influence on the normal operation of network system."

Based on the function of network security situation awareness, the research contents can be summed up in three aspects: network situation awareness, network threat evaluation and network situation assessment. Situation assessment and threat assessment are one link of
situation awareness process, threat assessment is based on situation assessment. Situation assessment includes the extraction of situation elements, current situation analysis and situation prediction. Threat assessment is about the destructive ability of malicious attacks and the estimation of the whole network threat, which is based on situation assessment. The task of threat assessment is to assess the frequency of attacks and the degree of threat to the network. Situation assessment focuses on the emergence of events. While threat assessment focuses on the effects of events and situations.

**Model of NSSA Structure**

As one of the two key technologies to ensure information superiority, network security situation awareness has been extensively studied in this field by learners, who proposed a variety of analytical models. Among them, JDL model based on the concept of data fusion is a widely accepted model, the general framework of JDL model mainly includes multi-source heterogeneous data collection, data preprocess, event correlation, target recognition, situation assessment, threat assessment, response and early warning, visualization display of situation, process optimization control and management, all together seven parts[7]. Combined with the related research at home and abroad, through analyzing JDL functional model as well as the model framework of network security situation awareness proposed by Endsley, layers structure is given, namely, the structure model of security situation awareness, which can be shown in Fig.1.

![Figure 1 Network Security Situation Awareness Concept Model](image)

The first layer can mainly realize the extraction of situation index. This layer is very important for the entire network security situation awareness model. The main function of this layer is to monitor and analyze network abnormal traffic by using network flow monitoring and analysis tools. The sample data can be extracted from the alarm database, and the sample data can be processed.

The second layer can mainly realize the evaluation of network security situation, which is the key to the security situation awareness of the whole network. It can evaluate whether the
network security is attacked or not. By processing the current message network attacks that can affect the network security in network information, then according to the evaluation model of the specific situation, generating the corresponding graph of the security situation, so as to reflect the status of the network security situation system.

Third layer can realize the prediction of network security situation, according to the second layer, it can obtain the current network security situation with other network security data, so as to predict the network security situation on the next stage, which can make network security management staff can the network security situation more high-level information, providing the basis for making reasonable decision.

Key Technologies of NSSA

During the process of conducting network security situation awareness model, the network security situation assessment index can be obtained, the current prediction of current network security situation as well as the next phase of the network security situation is the key step, which can represent the continuous execution of network security situation awareness model framework. Here, the evaluation of the current network security situation is the core content of network security situation awareness. The current evaluation of network security situation is mainly to analyze and deal with a variety of network security intrusion threats, analyze the details of network intrusion behavior, so as to deal with and merge complex security incidents. Therefore, the key technologies involved in network security situation awareness include network security situation feature extraction, security situation assessment and situation prediction. In view of these key technologies, Professor Wang Huiqiang and others put forward the corresponding implementation technology in the literature document[8].

Extraction of Situation Features Based on Multi-Classifier Fusion

Because of the influence of network security situation is susceptible to attacks, viruses, bugs and human, a kind of method only using one classifier or difficult to achieve extraction of security situation factors in large-scale complex network environment, it is difficult to guarantee the detection effect. Based on this, a method of extracting security situation elements based on multi classifier fusion is proposed. This model mainly includes the classifier and the fusion of two parts, were constructed (BP neural network with genetic neural genetic algorithm, GA-BPNN) classifier, support vector machine (support vector machine, SVM) classifier and fuzzy clustering (fuzzy cluster FC) classifier. For the same event, the classification results of different classifiers may be different, therefore, further fusion reasoning using DS evidence theory, first calculates each evidence of basic probability assignment function, belief and plausibility functions; then calculate all the basic probability assignment function, the combined effect of evidence under the belief function and the likelihood function with the DS combination rule according to certain decision rules; finally, the biggest support under the combined action of hypothesis selection.

Assessment of Network Security Situation

The pretreatment of network security event is the first step to evaluate network security situation. Network security situation assessment is a comprehensive evaluation of the overall security of the current network, which is a measurement of the security of the entire network system. After preprocessing the network security event, it should analyze and evaluate the
protection ability of the whole network about the current security threats in the current network system, at the same time, the threat of invasion degree should be shown in a visual form.

Before analyzing the association of the security event, the extensive data processing technology can be used to optimize the data characteristics during the period having security event preprocessing. But the assessment of network security situation is comprehensive to evaluate whether the status of the network is safe or not, namely, by using the historical records and log data generated by the network operation, a accurate prediction value of the current network security state information as well as the value of a period of time can be obtained at last so that network security management staff can keep on the maintenance. We should also use the methods of fuzzy inference and neural network to evaluate the network security situation, so as to get the accurate evaluation results.

The Prediction of Network Security Situation

The prediction of network security situation is a key link of active protection in large-scale network system. In the network security situation awareness model, the prediction of network security situation is the last step of the whole network security situation awareness, which can be regarded as the continuation of network security situation assessment. Only evaluating the network security situation accurately can the effective prediction of network security situation be carried out. According to the result of network security situation assessment, the current network security situation can be evaluated by a certain algorithm, so as to analyze the past and predict the future. The prediction of network security situation can play a very important role in the framework of network security situation awareness. Only by means of predicting threats can it take the effective security measures to protect network security.

Through the evaluation of the current network security situation, we can get a prediction model that can express the dynamic changes of network security, which also can predict the security situation of the future network, and visualize them as well. Thus it can help network decision makers with network decisions.

Conclusion

With the development of information society, how to ensure the security of network information has become to the big issue of national security. Therefore, it is very necessary to develop network security situation awareness. Network security situation awareness as a new technology of this year can achieve the extraction of the invasion behavior, making assessment and prediction on the future development trend of network security, which is a precision measurement of network security situation. Moreover, it can help the network decision-makers to carry out the protection of network security as well as network management, thus the research on network security technology of situation awareness has significant meaning. Network security situation awareness technology is to evaluate the overall security status of the system in a certain scale of network environment, which can predict its development trend as well.

Reference

[1] Sushil Jajodia, Peng Liu, and et. Cyber Situational Awareness Issues and Research. Springer US, 2010.
[2] Wendong Gen, Xiaoping Du, and et. Spatial Situational Awareness Introductory Theory. Beijing: National Defense Industry Press, 2015.

[3] M. Endsley. Toward a Theory of Situational Awareness in Dynamic Systems. In Human Factors Journal, Volume 37(1):32-64, March 1995.

[4] D. S. Alberts, J. J. Garstka, and et. Understanding Information Age Warfare. In DoD Command and Control Research Program Public Series, 2001.

[5] Wang HQ, Lai JB, Zhu L, Liang Y. Survey of Network Situation Awareness System. Journal of Computer Science, 2006,33(10):5–10 (in Chinese).

[6] Gong J, Zang XD, Su Q, Hu XY, Xu J. Survey of Network Security Situation Awareness. Ruan Jian Xue Bao/Journal of Software, 2017, 28(4):1010–1026 (in Chinese).

[7] A N Steinberg, C L Bowman, F E White. Revisions to the JDL data fusion model. The SPIE Aero Sense, Orlando, Florida, USA, 1999.

[8] Wang Huiqiang, Lai Jibao, Hu Mingming, Liang Ying. Research on Key Technologies for Implementing Network Security Situation Awarenes. Geomatics and Information Science of Wuhan University, Volume 33(10): 995-998, 2008.

[9] Lei Shi. The Study on the Model of Network Security Situational Awareness. Lanzhou: Lanzhou University, 2012.