Research on Network Threat and Situation Assessment Method of Electric Power Information System

Yunhui Liang*, Linghao Zhang, Sheng Wang, Jie Zhang, Juling Zhang, and Ming Wu

Electric Power Research Institute of State Grid Sichuan Electric Power Company
ChenDu, Sichuan, 610000, China,
*Corresponding author’s e-mail: Lianghh2115@sc.sgcc.com.cn

Abstract. With the rapid development of information and communication technology, the national electric power information system has been extensively developed, and the electric power information system is becoming more and more intelligent, complicated and networked. At the same time, the complexity of the power information system has also brought about the problem of network security, and various network threats have put forward higher requirements for the network security of the power information system. How to evaluate the cyber threat of power information system has become an important work of power information system network security. This article uses the network threat attribute indicators that the power information system faces, and combines the situation assessment method to conduct a situation assessment on the network security of the power information system.

1. Introduction

With the rapid development of smart grids, higher standards have been put forward for the power information system, and my country has begun to vigorously build smart grids. Compared with the traditional power system, the modern smart grid operation mode and service mode have been greatly improved. The massive data interaction and the rapidly increasing number of smart terminals have brought a new round of challenges to the security of the power information system, and in-depth exploration the situation of information security in the power system seems urgent.

At present, the development and research of smart grids are becoming more and more intelligent. The open network architecture and diversified power requirements make the power system more and more complex, which brings huge uncertainty to the construction and operation of the power system; at the same time, the system The security deficiencies in the intelligent information equipment in China increase the operation risk of the power system. Because the power grid is in the process of construction, use, and operation and maintenance, the staff did not seriously consider the network security of the information system. Therefore, under the continuous interaction of information and physical systems, information-level threats will cause more serious accidents in the power system.

Network security situational awareness is a new technology that has emerged in recent years. Simply put, it extracts, evaluates, and predicts the development trend of the future network of intrusion threat behaviors. It is a precise measurement of the network security situation and can help network decision-making. Personnel conduct network management and security protection, so it is of great significance to study network security situational awareness technology. Network security situational
awareness technology is to evaluate the overall security status of the system in a certain scale of network environment and predict its development trend.

According to the actual needs of online evaluation and analysis of power information system security situation, this paper proposes a network security situation analysis index system suitable for this demand. The focus is on discussing the quantification method of attack situation for electric power information system, defining the security situation assessment framework, and designing the online assessment algorithm of electric power information system security situation based on the actual situation and its own characteristics of each business application and network of the electric power information system. Based on the evaluation framework and online evaluation algorithm, an online evaluation and analysis system for the security situation of the power information system is constructed. This system further verifies the feasibility and effectiveness of the evaluation framework and online evaluation algorithm given in this paper.

2. Related research
The main function of situation assessment technology is to reflect the operating status of the network and the severity of the threats it faces. The network security situation assessment is mainly to collect and preprocess the original security data and events on the network, based on the established network security situation assessment index system, and on the basis of certain prior knowledge, through a series of mathematical models and the algorithm is processed, and then a quantitative or qualitative network security situation assessment result is obtained in the form of a security situation value to show the network security status. It should be noted that the size of the security situation value will also change with changes in the security situation. The amount of data involved in the whole process is relatively large and the evaluation algorithm is relatively complex, which will cause redundancy and false reporting. Therefore, data preprocessing and analysis (cleaning, integration, reduction, transformation, and event correlation analysis) are often required. Situation assessment focuses on evaluating the impact on the network after an incident occurs, and assessing the current network security situation through the analysis and modeling of the historical security situation, and sometimes even the future situation assessment. Network security managers add corresponding security measures to the network and upgrade and optimize the network through situation assessment, so as to respond to changes in the network security situation. Network security situation prediction refers to the prediction of the future development of the network based on historical information and current status. The former mainstream methods include neural networks, random forests, and decision trees and so on. In literature [9], BP neural network and RBF neural network were used to construct prediction models; in literature [11], the situation value was predicted based on Markov chain and gray theory; in literature [12], support vector machine (SVM) To build a predictive model. Because the situations is a set of non-linear, non-normally distributed values. The neural network model is difficult to determine the model structure due to the principle of minimum risk; SVM has no relevant theory to determine the parameters, so the results are biased; in the face of such non-linear data, the time series algorithm will produce large deviations.

With the rapid development of artificial intelligence, the rise of machine learning provides a variety of solutions for the application of cyber security situational awareness. The decision method is to obtain the mapping relationship between the system state variables (the input of machine learning) and the security situation value (the output of machine learning) through training, such as neural network, random forest, principal component analysis[13], aiming at the security situation awareness of electric power information network, a ball vector classifier using quantum genetic algorithm to optimize training parameters is proposed to achieve precise classification of network security situation. Literature[14] proposed a neural network method that can reduce the number of input features and reduce the dimensionality of the problem. Literature[15] designed a prediction model based on RBF neural network, combined with genetic algorithm to perceive the network security situation. In order to accurately predict the network security situation, designing a sound situation awareness model is the main work at present.
3. Information System Situation Assessment System

3.1. Levels of situation assessment methods

At present, although the industry does not have a unified definition of cyber security situational awareness, research experts at home and abroad have given a relatively consistent statement based on their own years of research: scholars currently use the most widely used network situational awareness framework in the field of research applications. The models include the Endsley three-layer perception model and the Tim Bass model. The following describes the classic model of Tim Bass model. This model was first proposed by Tim Bass. As shown in Figure 3, it mainly includes five levels of modules: data refining, attack object identification, situation understanding refining, threat assessment, and resource management. The Tim Bass model is shown in the following figure:

Combining the Tim Bass model and referring to the model framework proposed by scholars in the field, based on the need for data processing in the cyberspace process, the corresponding data processing process is divided into five levels:

1. Data collection refers to obtaining various data related to cyberspace security from various devices, such as system logs, alarms, information, and network topology.

2. Data preprocessing is the preliminary processing of the acquired data. Since all kinds of data come from different devices and have different formats, the data can be cleaned, integrated, reduced, and transformed through this process, which can perform data fusion on multi-source heterogeneous data.

3. Information extraction is a further fusion understanding of the data generated after data preprocessing, by establishing an appropriate network security situational awareness indicator system, fusing data from different sources to generate underlying indicators.

4. Situation analysis is to integrate the underlying situation indicators, comprehensively process and calculate through various data processing methods, and then obtain the upper-level situation results. This is exactly the level of the network security situation assessment, which mainly includes two parts:

5. Situation presentation is to show the situation of cyberspace through appropriate visualization methods for users to make comprehensive judgments.
3.2. Algorithm selection
This chapter first analyzes the situation assessment based on the threats of the power information system network, constructs a network security situation assessment index system, and introduces the BP neural network into the network security situation assessment, and uses genetic algorithms to improve the defects in the BP neural network. Because the genetic algorithm uses a heuristic search method, rather than brute force exhaustion, at the same time, in the search process, the genetic algorithm's changing rules are not constant. Therefore, the genetic algorithm has a good search efficiency. While the BP network uses a non-linear way to convert complex problems, it does not need to analyze the non-linear relationship. Moreover, the learning speed is fast, the modeling process is simple, and the evaluation efficiency is high. Therefore, a network security situation assessment model based on genetic algorithm-BP neural network is proposed.

BP neural network is also called error back propagation neural network. As shown in Figure 2, the main structure of BP neural network is described as follows. It consists of an input layer, several hidden layers, and an output layer. The layers are connected by the weights are connected, and the nodes do not interfere with each other.

![BPNN structure diagram](image)

3.3. Algorithm implementation steps
The BP algorithm is a supervised learning algorithm, and its essence is the gradient descent method. The main idea is to repeatedly adjust the connection weight and threshold of the network through the back propagation of the error between the actual output and the expected output, so as to reduce the error between the two as much as possible. Generally, when the sum of squared errors of the output layer is less than the given. When the specified error or the error is reduced to the allowable range of the network to stop training, and save the connection weight and threshold of the network.

The specific training steps are as follows:

1. Initialization operation. Randomly give a connection weight between the input layer and the hidden layer, the hidden layer and the output layer, and the threshold of the hidden layer node and the output layer node.

2. Calculate the output of each neuron in the hidden layer and the output layer.

\[ b_j = f(s_j = \sum_{i=1}^{p} w_{ij}x_i + \theta_j), j = 1, 2, ..., p \]

\[ y_t = f(\sum_{j=1}^{m} v_{ij}b_j + r_t), t = 1, 2, ..., n \]

Where \( b_j \) is the output of the \( j \)-th node in the hidden layer, and \( y_t \) is the output of the \( t \)-th node in the output layer.

3. Calculate the output layer and the hidden layer to correct errors through the loss function.

4. Calculate the new connection weight and threshold.

\[ v_{ij}(n+1) = v_{ij}(n) + \alpha d_t^k b_j \]

\[ w_{ij}(n+1) = w_{ij}(n) + \beta e_t^k a_t^k \]

\[ r_i(n+1) = r_i(n) + \alpha d_t^k \]
Among them, $\alpha$ and $\beta$ are learning coefficients.

(5) Repeat training. Select the next set of training samples and repeat the steps until all samples have been trained or the error has been reduced to a pre-set range, and the training ends.

4. Experimental results

In order to analyze the performance of the power information system network security situation assessment model based on genetic algorithm BP neural network proposed in this paper, the simulation platform is, Intel Core i7 CPU, memory 16G, Windows 10 operating system, to realize the power information system network security situation assessment algorithm, Obtain 100,000 network threat information from the power information system, and select the neural network and the BP neural network based on the genetic algorithm for comparison experiments. The algorithm iterates 100 times. Figure 3 is a graph of the mean square error loss of the algorithm for 100 iterations.

![](image1.png)

It can be seen intuitively in Figure 3 that compared with the traditional neural network; the results of the improved BP neural network to evaluate the network security situation have a faster algorithm convergence rate and a lower error rate.

Next, select 10 pieces of data to test the algorithm, as shown in Figure 4 below.

![](image2.png)

Figure 4. Comparison of actual and expected threat values
It can be seen from the figure that the result of using the genetic-based BP neural network to evaluate the network security situation is almost the same as the actual situation value of the network. The accuracy of the evaluation results is very high, which proves the effectiveness and accuracy of the genetic-based BP neural network algorithm for evaluating the network situation.

5. Conclusions
It can be seen from the increasing number of network attacks that today's power information network environment has become more and more complex, and the security situation is worrying. According to the actual situation of the power information network system, this paper constructs an evaluation system that can more comprehensively reflect the network security situation, and proposes a BP neural network model based on genetic algorithm. The modified model realizes fast and accurate situation prediction.

Acknowledgments
This work was supported by the State Grid SiChuan Electric Power Company of China (Project Name: Research and platform development of full flow Advanced Sustainable threat intelligent analysis technology based on deep learning).

References
[1] Wang Haoran. Research on the application of information security situation analysis methods and systems in power informationization [J]. Digital Technology and Application, 2017(02): 215-217.
[2] Hao Junjie, Wang Dan, Yang Donghai. Research on online assessment framework and algorithm of network security situation of power information system[J]. Power System Protection and Control, 2013, 41(09): 116-120.
[3] Zhao Tong. Research on key technologies of cyber threat situation assessment based on multi-source logs [D]. Tianjin University of Technology, 2018.
[4] Huang Min. Research on cyber threat assessment technology based on organizational recognition [D]. National University of Defense Technology, 2015.
[5] Chen Decheng. Research on Power Information Network Security Situation Awareness under Intrusion Attacks [D]. Nanjing University of Posts and Telecommunications, 2019.
[6] Shi Lei. Research on the Network Security Situational Awareness Model [D]. Lanzhou University, 2012.
[7] Chang Qian. Research and application of key technologies for intelligent analysis of network security situation [D]. University of Electronic Science and Technology of China, 2020.
[8] Ma Dong. Research on key technologies of network threat detection and situation prediction[D]. National University of Defense Technology, 2013.
[9] Xiao P.,Xian M, Wang H. Network security situation prediction method based on MEA-BP[C]. 3rd IEEE International Conference on Computational Intelligence and Communication Technology, CICT 2017:1-5.
[10] Lai Zhiquan. Network security situation prediction model based on hybrid optimized RBF neural network [D]. Lanzhou University, 2017.
[11] Zhan Xiong, Guo Hao, Zhang Yun, et al. Network security situation prediction method based on hidden Markov model[J]. Telecommunications Science, 2015, 31(S1): 79-84.
[12] Wang Jian, Li Ke, Zhao Guosheng. Security situation prediction optimization model for perceived quality assurance[J]. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2018,46(01):22-25.
[13] Xu Ruzhi, Wang Yufei. Research on Security Situation Awareness of Electric Power Information Network [J]. Power System Technology, 2013, 37(01): 53-57.
[14] Yan Yu, Liu Tianqi. Dynamic security analysis neural network input feature optimization based on decision table-rough set theory[J]. Automation of Electric Power Systems, 2004(15): 25-29.

[15] Xie Lixia, Wang Yachao, Yu Jinbo. Network security situation awareness based on neural network[J]. Journal of Tsinghua University (Natural Science Edition), 2013, 53(12): 1750-1760.