Analysis of Intelligent Monitoring Model of Network Security Situation Based on Grid Power Flow

Shang Gao, Shou-ming Chen, Yun-de Liang, Yan-qian Lu, and Jie-sheng Zheng(✉)

Guangdong Power Grid Corporation Information Center, Guangzhou 510062, China
gaoshang527@outlook.com, zhengjiesheng857@outlook.com

Abstract. In order to introduce the grid power flow model to intelligently monitor the network security situation, a model based on grid power flow is established. In the construction of the network security situation intelligent monitoring system, the hierarchical database is protected and managed, the attacks brought by the network security situation are changed, and the network security situation level protection system is improved and improved. On this basis, the network trend correction factor is introduced, and the network security situation is normalized according to the network security situation value. The network information flow is processed uniformly, and the intelligent monitoring model of network security situation based on power flow is built. Compared with the traditional network security situation intelligent monitoring model, the application of network security situation intelligent monitoring model can effectively solve the uncertainty and fuzziness of information provided by various network security devices.

Keywords: Power flow · Network evaluation index · Network security situation · Risk assessment

1 Introduction

The power flow of power grid is based on the determination of the network structure and the equivalent load power of distribution network. By controlling the output power of large-scale thermal power and hydropower, as well as flexible adjustment of transformer adapters and reactive power compensation equipment, under the condition of network security constraints, the goal of minimizing power generation cost, minimizing network loss and minimizing environmental pollution can be achieved. Compared with economic dispatch, the optimal power flow model is more complex, and the solution method becomes the most important problem to be studied [1]. The optimization model is decomposed into active sub-problems and reactive sub-problems by utilizing the weak coupling relationship between "active-phase angle" and "reactive-voltage" of transmission network. The overall optimization is realized by alternating iterations, which reduces the scale of the problem and improves the calculation efficiency. In addition, with the advancement of optimization mathematical theory and

S. Liu and L. Xia (Eds.): ADHIP 2020, LNICST 348, pp. 127–136, 2021.
https://doi.org/10.1007/978-3-030-67874-6_12

computer technology, a series of effective solutions such as simplified gradient method, linear programming method, quadratic programming method and Newton method have emerged, especially the application of linear and non-linear interior point method with polynomial time complexity in optimal power flow, which makes it possible to quickly solve optimal power flow problems.

Network security situation is a macro response to the network operation status. It reflects the past and current status of a network, and monitors the possible network status in the next stage. Its original information comes from network management equipment, network security equipment, network monitoring equipment [2]. Through the mathematical processing and integration of these data, we can generate numerical values and charts that can reflect the operation of the network. By analyzing the relationship between network attack and network situation, an intelligent monitoring model of network security situation is proposed. The model provides knowledge support for network security situational awareness, understanding and decision-making. At the same time, through the combination of network security situation knowledge base and power flow theory, network security situation awareness and situation understanding can solve the uncertainty and fuzziness of information provided by various network security devices. By accurately synthesizing the information obtained by various network security devices into a unified description of the environment, the correct decision-making ability of the intelligent monitoring model of network security situation can be enhanced. Aiming at the problem that the existing network security technology can not monitor the future security situation of the network, a model of intelligent situation monitoring based on power flow is proposed, which takes advantage of the characteristics of network security situation value with non-linear time series and the advantages of neural network in dealing with chaotic and non-linear data. The experimental results show that. The model can accurately obtain the monitoring results of situation values and help network managers make security decisions.

2 Design of Intelligent Monitoring Model for Network Security Situation Based on Power Flow

Through the establishment of intelligent monitoring system for network security situation, the protection and management of hierarchical database, and the improvement of power flow coupling, the improvement of power flow coupling can be achieved. The specific operation method can be carried out in the following steps.

2.1 Construction of Intelligent Monitoring System for Network Security Situation

When evaluating the network security situation, we can evaluate it qualitatively or quantitatively. For qualitative evaluation, it means only describing the existing risks qualitatively. Quantitative evaluation method expresses the evaluation factors with specific numerical values, and then all these factors are included in the algorithm to calculate the risk value. If the calculated risk value is greater, it indicates that the

network is insecure. In the qualitative evaluation of network security, in order to perceive the network security situation, independent attack recurrence, network traffic state change and network connection state evolution will be used. The qualitative risk assessment does not quantify the risk, but presents the state of network security in the form of recurrence. In the demonstration of network security situation, experts' knowledge in the field will be referred to [3]. Nowadays, many security products can easily get network evaluation index, SCYLLARUS system and Honeypot system.

Whether qualitative or quantitative evaluation index system, because of its different emphasis, in order to fully reflect the security situation of the network, it is necessary to consider them comprehensively. The combination of the two risk assessment methods can ensure the integrity and effectiveness of the assessment (Fig. 1).

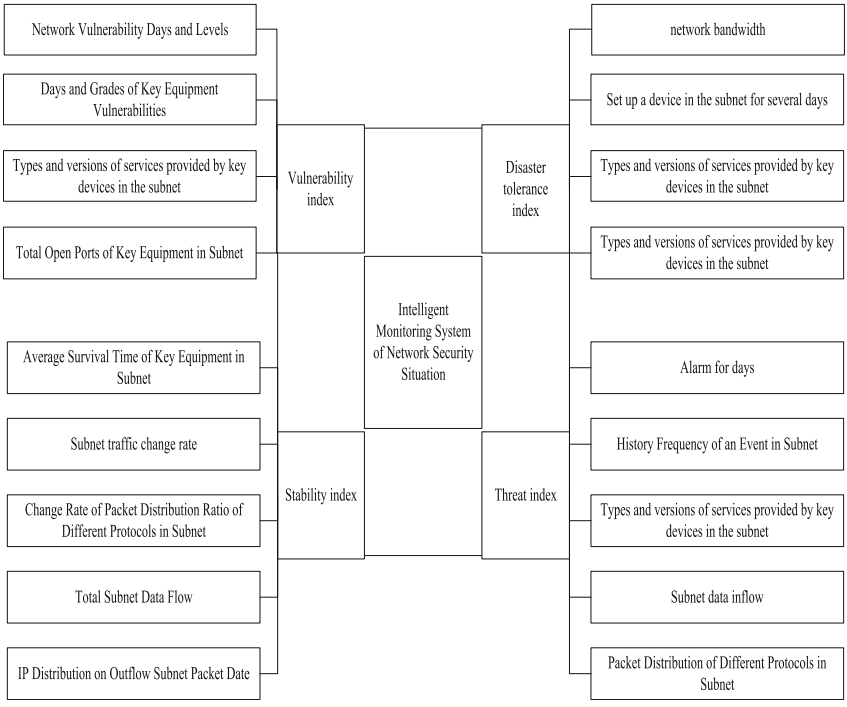

Fig. 1. Intelligent monitoring architecture of network security situation

As shown in the figure, the model uses multiple data sources and composite evaluation indicators to accurately perceive the whole network state in order to achieve the purpose of comprehensive evaluation of network security. Therefore, in order to evaluate the whole network entity (network, host, router, etc.) and all levels (network layer, operating system layer, application layer, etc.), On the premise of the following principles, an intelligent monitoring system of network security situation is established.

First, integrity and independence. In large-scale networks, the index system is used, because the index system can reflect the impact of all factors, so as to achieve a

comprehensive assessment of the network situation. And because the index system will take into account various factors, so the number of indicators will be very complex, if all indicators are not different, completely integrated, it is difficult to make a comprehensive and effective evaluation [4]. Therefore, in the evaluation of network situation, several elements should be kept relatively independent, and these relatively independent properties will be reflected by the calculation of the index set. Secondly, it is systematic and hierarchical. In the network situation index system, systematicness and hierarchy are its main characteristics. Because the network itself is a hierarchical structure, it is necessary to ensure the hierarchy when establishing the index system, so as to reflect the rationality and regularity of the index system. Thirdly, it is scientific. The selection of network situation indicators must be based on science, in order to truly reflect the true state of network situation, its scientificity is mainly reflected in the following aspects: data selection, statistical method selection and index range selection. Fourth, the persistence and goal of the indicators. All the selected indicators must satisfy the continuity of time. At the same time, the function of these indicators should be reflected at a certain time point, which can reflect the overall state of the system comprehensively Fifthly, the index system should include dynamic and static indicators. There are not only dynamic changes in the network, such as traffic, change rate, but also fixed properties, such as hosts, routing devices, etc. [5]. Although these properties are not obvious in the overall situation of the network, they are indeed an integral part of the network situation, which is the basis for the existence of the network. Therefore, in the construction of the index system, it is necessary to include dynamic and static indicators. For these indicators with different attributes, we can choose to use manual configuration to achieve.

By studying the overall structure of the network system, we can classify and sort out the index system. According to the network state, we can classify the nature of the network, so that we can evaluate the network state from the perspective of the nature. There are four main forms of network state, namely vulnerability, disaster tolerance, weili, and stability. We classify these four characteristics as the first-level indicators of network situation. On this basis, we extract 2–5 second-level indicators to meet the requirements of covering information network entities and network levels.

2.2 Adjusting Monitoring Sequence of Power Flow Intermediate Database

Network security situation knowledge base is an important part of network security situation assessment system. It is responsible for storing network security situation information, providing knowledge support in network security situation awareness, understanding and decision-making methods. Referring to the relationship between network attack and network security, this paper uses attacker state and network state to construct network security situation knowledge base [6].

In the knowledge base of network security situation, the relationship among network status, attacker status and network security situation is as follows. Network security situation: The security-related information in the network is expressed in the form of P (X), where P is the predicate and X is the parameter set. Attack state: Describes the system security knowledge and resources that an attacker possesses, similar to the system state, in the form of P (X). Network security situation: the whole

network and attacker's information set related to security, that is, the complete relationship between network state and attacker's state is shown in Fig. 2.

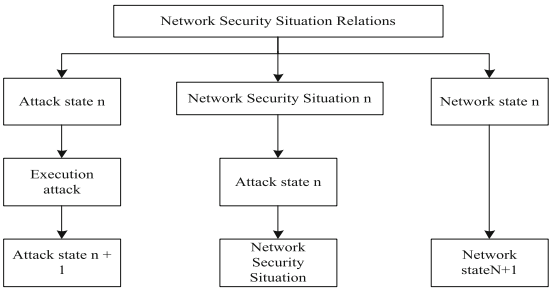

Fig. 2. Network security situation diagram

Network vulnerabilities are errors in the specific implementation and use of the network, but not all the errors in the network are vulnerabilities. Only errors that threaten network security are vulnerabilities. Many errors do not cause harm to network security under normal circumstances. Only when people intentionally use them under certain conditions can they affect network security. Although vulnerabilities may exist initially in the network, they do not appear on their own and must be found artificially. In actual use, users will find errors in the network, and attackers will intentionally use some of them and make them become a tool to threaten network security, then this error will be considered as a network vulnerability [7]. For an attacker, in order to attack a target network, it is necessary to discover the system vulnerabilities in the target system, and then consciously use the vulnerabilities to attack, that is, to find the premise of network attack.

At the same time, the network attack using network security vulnerabilities will bring dynamic state changes to the network security situation after the attack. The so-called dynamic network security state refers to the uncertainty of the attack results, such as some buffer overflow attacks, which may successfully obtain privileges, may also lead to process denial of service, and may not cause any results.

2.3 Introduction of Power Flow Correction Factor

Compared with the basic Elman neural network, the double feedback Elman network increases the feedback of the output layer nodes, which makes up for the deficiency of the basic Elman network. It takes the output layer feedback as the input of the hidden layer along with the input layer and the connection layer unit. This feature makes its information processing ability more powerful. Its mathematical model is expressed as formula (1):

$$x_c(k) = \alpha x_c(k-1) + x(k+1) \tag{1}$$

$x_c(k)$ in formula (1) represents the output of the receiving layer unit 1, αx_c represents hidden layer output. Double feedback Elman neural network still uses gradient

descent idea to obtain the learning algorithm of the network. Formula (2) is used to represent the error function in the dynamic double feedback Elman neural network, i.e. the objective function:

$$E(k) = \frac{1}{2}(y_{\partial}(k) - y(k))^T \tag{2}$$

$E(k)$ in Formula (2) denotes the output value of the output unit. y_{∂} denotes the connection weight between the value acceptance layer and the hidden layer. T denotes the connection weight between the hidden layer and the output layer [8].

In network situation monitoring, we are most concerned about the monitoring capability of the monitoring model. In order to improve the monitoring capability and accuracy of the monitoring model, we need to pay attention to the rising and falling direction of monitoring trend. If a trend correction factor is added to the model to reflect the monitoring trend, the monitoring trend can be effectively adjusted and the correct direction of monitoring can be guided, so that the monitoring accuracy can be improved [9]. Its core idea is in the process of monitoring. If the trend of monitoring value is different from the actual value or the direction of rise and fall is not consistent, the parameter of trend correction factor should be g, otherwise the parameter should be h. The trend correction factor can be expressed in formula (3):

$$f_{DP}(t) = if(y_d(t) - y_d(t-1)) \tag{3}$$

Formula (3) f_{DP} represents the trend correction factor, if represents the number of iterations, and y_d represents a relatively large value.

2.4 Normalization of Network Security Situation

The network security situation is estimated by analyzing the network security situation data, and the network model is shown in Fig. 3.

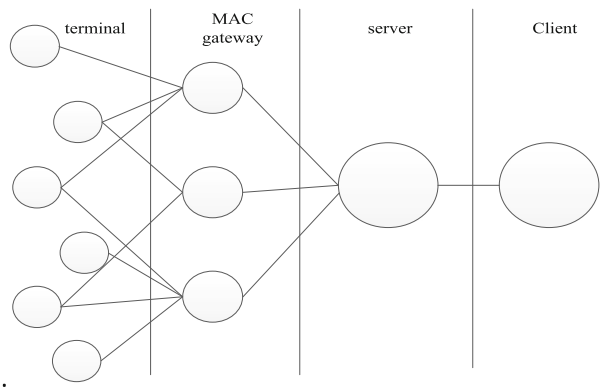

Fig. 3. Network model.

According to its linear frequency hopping spread spectrum technology, the network model is convenient to identify malicious attack information effectively, and can guarantee the network security situation.

Suppose that the data flow of m malicious attacks under the neural network is:

$$x(k) = [x_1(k), x_2(k), \cdots, x_m(k)] \tag{4}$$

In the formula, k represents the attribute value of the malicious network attack; $x_i(k)$ represents the feature vector of the malicious data of the communication network.

According to the process of network attack and the non-linear sequencing of alarms generated by security devices, the network security situation value x obtained by weighting all kinds of alarms can be abstracted as a function of time series t. Namely: $x = f(t)$, This situation value has the characteristics of nonlinearity [10]. Therefore, the network security situation value can be treated as a time series, so assuming the time series $x = \{x_i | x_i \in R, i = 1, 2, ...L\}$ with network security situation value, we now hope to monitor the following M situation values through the situation value of the first N time of the sequence [11].

In order to eliminate the possibility of large errors due to the use of data in the process without processing, this paper normalizes the situation values [12, 13]. The specific normalization formula is shown in (5):

$$x_i = \frac{x_i^t - x_{\min}}{x_{\max} - x_{\min}} x(k) \tag{5}$$

In formula (5), x_i is the calculated situation value, x_i^t is the normalized situation value, and $x_{\min}$ and $x_{\max}$ represent the maximum and minimum values in the network security situation value, respectively.

3 Model Effectiveness Verification

The experimental data select 120-day network status data of a university campus network to monitor the network security situation of the campus network. The evaluation indexes are carried out by using the index system established. There are four first-level indicators and 22 second-level indicators of risk, vulnerability, availability and reliability in the index system. We use Math to calculate these indicators according to the above calculation situation value method. Mathematica software is used to calculate the situation value, and 120 situation values are obtained.

According to the cyber security incident indicator system we developed in Sect. 3, we use the commonly used method of evaluating the grading scale of the Likert quantity. According to the semantic principle, we develop a five-level evaluation level standard: The levels correspond to an element of good, good, general, poor, and poor in the fuzzy set. For the convenience of calculation, we quantize the _5 kinds of fuzzy evaluations respectively, and assign their corresponding values to 5, 4, 3, 2, 1. The corresponding situational value table for the evaluation grading standards is shown in Table 1.

Table 1. Evaluation grading criteria corresponding situation value

Evaluation situation value	Comment	Grading
$x_i > 4.5$	Good	E1
$3.5 < x_i < 4.5$	Good	E2
$2.5 < x_i \leq 3.5$	Good	E3
$1.5 < x_i \leq 2.5$	Good	E4
$x_i \leq 2.5$	Good	E5

3.1 Preliminary Experiment Preparation

Using the basic Elman model and the dual feedback Elman neural network model with trend correction factor, in the experiment, the network security situation is monitored by these two models.

The basic Elman neural network and the dual feedback Elman neural network with trend correction factor are all based on a three-layer network structure, that is, there are _5 input layer nodes, 10 hidden layer nodes and 1 output layer node. The layer unit node, the former has one receiving layer unit node, and the latter has two receiving layer unit nodes. Because the input layer has _5 input nodes, the input is the continuous 5th network security situation value, and one output node of the output layer outputs the monitored value of the number of attacks on the 6th day.

3.2 Network Security Intelligent Monitoring Node Coverage Comparison

The network security trend monitoring model and the traditional network security situation intelligent monitoring model are used to monitor the network security situation. Monitor the cybersecurity situation values from day 91 to day 110 in the data set. That is, d86 (the situation value on the 86th day to the 90th day) was used to monitor d91 (the situation value on the 91st day), and d92 was monitored using d87–d91. And so on, monitor d110. The monitoring results and actual results are shown in Fig. 4:

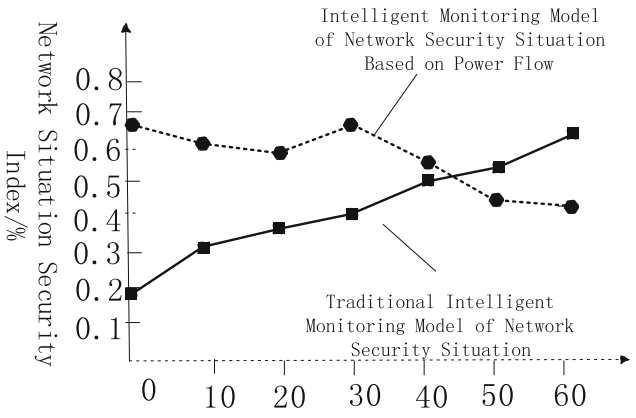

Fig. 4. Contrast experimental results

It can be seen from Fig. 4 that in the two models, the network traffic situation intelligent monitoring model of the power flow of the grid has three monitoring times, and the monitoring effect evaluation functions LS E and AAE are smaller than the basic Elman neural network. In Fig. 3, by comparing the results of the two models of the SYNFIood attack monitoring evaluation function, we can find that the AAE obtained by the SYNFIood attack of the network security situation intelligent monitoring model of the power grid is 0. 007462, and the AAE value of the basic Elman neural network monitoring is 0. 005552, the former increased by 34.2070 than the latter; this shows that the network security trend based intelligent monitoring model based on grid power is more capable of monitoring.

Compared with the traditional network security situation intelligent monitoring model, the network traffic situation intelligent monitoring model of the power grid not only increases the feedback of an output layer, but also increases the trend correction factor to control and adjust the monitoring trend of the rising and falling trend. Therefore, the model has Stronger information processing capability enhances monitoring performance, and its monitoring capability is significantly stronger than the traditional network security situation intelligent monitoring model.

In summary, the two monitoring models are feasible in the field of network security attack monitoring. However, through the monitoring and comparison of the two, the monitoring capability of the network security situation intelligent monitoring model based on the power grid trend is stronger, and the monitoring results obtained are quite satisfactory.

4 Conclusion

Network security management is not only a technical issue, but also a management issue. Therefore, how to find a solution from the security incidents that have occurred is the most concerned issue for researchers. Since the concept of network security situational awareness has been proposed, network administrators have begun to consider the security threat status of the overall network from multiple angles and macro perspectives, and to achieve the purpose of assisting decision-making based on the comprehensive evaluation index system of the network.

Acknowledgments. This research is funded by Jiangsu Tong Brand Professional Construction Project (Z215015002).

References

1. Ningbo, Peng, J., Changpeng, et al.: Analysis and research of power network monitoring signals based on equipment intelligent logic model modeling. Electron. Technol. Softw. Eng. (21), 216–217 (2017)
2. Xu, W., Dai, L.: Research on unified information model of monitoring integration platform based on smart grid. New Technol. Prod. China **23**(5), 41 (2017)

3. Jun, X., Lei, Z., et al.: Distribution system security region model based on power flow calculation. J. Electr. Eng. China, **37**(17), 334–336 (2017)
4. Anonymous. Construction method of large data application model for smart grid monitoring operation. Power Syst. Autom. **42**(20), 121–128 (2018)
5. Niu, W., Bao, P., Tang, H., et al.: Smart grid security vulnerability mining model based on data mining. Power Technol. **42**(4), 134–155 (2018)
6. European Network and Information Security Agency: Baseline guidelines for internet of things security in key infrastructure areas. Inf. Secur. Commun. Secr. **54**(1), 80–95 (2018)
7. Shuai, L., Weiling, B., Nianyin, Z., et al.: A fast fractal based compression for MRI images. IEEE Access **7**, 62412–62420 (2019)
8. Li, W., Wang, S., Li, X., et al.: Information security prevention and control system for power grid enterprises based on artificial intelligence. Power Inf. Commun. Technol. **17**(2), 105–109 (2017)
9. Chen, C., Tu, Z., Gu, L.: State grid corporation network and information security situation awareness practice . Power Inf. Commun. Technol. **45**(6), 3–8 (2017)
10. Jiang, C., Jiang, J.: Practice and innovation of network security internal audit in power grid enterprises. China Internal Audit **229**(7), 68–70 (2018)
11. Wang, H.: Application of information security situation analysis method and system in power informatization. Digit. Technol. Appl. **43**(2), 215–217 (2017)
12. Liu, S., Glowatz, M., Zappatore, M., Gao, H., Gao, B., Bucciero, A.: E-Learning, e-education, and online training, pp. 1–374. Springer, USA
13. Zheng, P., Shuai, L., Arun, S., Khan, M.: Visual attention feature (VAF): a novel strategy for visual tracking based on cloud platform in intelligent surveillance systems. J. Parallel Distrib. Comput. **120**, 182–194 (2018)