International Core Journal of Engineering Volume 6 Issue 5, 2020
ISSN: 2414-1895 DOI: 10.6919/ICJE.202005_6(5).0009

# Security Situation Awareness Method for Smart Grid

Dongyang Zhang[1, a] and Qiuping He[1, b]

[1]School of Control and Computer Engineering, North China Electric Power University, Baoding, China.

[a]backyla@qq.com, [b]993032469@qq.com

## Abstract

**With the complexity of China's smart grid system, the traditional power grid operation monitoring system has been unable to meet the safe operation requirements of the power grid. In order to improve the active defense capability of the smart grid information space, it is necessary to deeply analyze the perception technology of power system network security situation, and to perceive, analyze, evaluate and predict the element States and feelings of power system in the network environment. In this paper, the security situation awareness method for smart grid includes big data analysis and combination prediction method. The analysis shows that the current technology focuses are diverse, and both methods can effectively perceive the security situation of smart grid, and the accuracy is high.**

## Keywords

**Smart grid, Information security, Situation awareness.**

## 1. Introduction

With the increasing popularity of smart grid, the information security problem in smart grid becomes increasingly prominent. How to ensure the security of information while ensuring the safe and stable operation of power grid will become the key in the design and implementation of smart grid. From the perspective of composition and distribution, smart grid is a very complex system. Compared with the traditional power transmission system, smart grid has more intelligent features such as information and automation. However, the key to realize the intelligent power grid is to integrate the power system and the information system in depth to form the information physical fusion system, and realize the self-regulation and control by automatically processing the data. Therefore, the failure of the information system itself or the network attack will not only affect the operation of the information system itself, but also affect the physical system, so that the physical system cannot operate normally.

As an important technical means to master the operation track of power grid, the application of situation awareness technology in power grid is particularly important. It can collect, understand and predict all kinds of factors related to grid operation changes in the wide area of time and space, and strive to accurately and effectively grasp the security situation of the grid, so that the security management of the grid changes from passive repair to active prevention.

On the basis of summarizing the basic idea of network security situation awareness, this paper summarizes and analyzes two current security situation awareness methods for Smart Grid: smart grid security situation awareness method based on big data analysis [1] and smart grid security situation combination prediction method based on information fusion [2].

ISSN: 2414-1895 DOI: 10.6919/ICJE.202005_6(5).0009

# 2. Network Security Situation Awareness

## 2.1 Basic concepts of network security situation awareness

The concept of network security situation awareness originated from human factors research of space flight, which is a hot research field developed in recent years [3]. It can integrate all available information, carry out comprehensive dynamic detection of the system, assess the security situation of the network, collect and analyze historical data, and predict the potential risks of the system in the future, minimize the risks and losses caused by unsafe factors, and improve the monitoring ability, emergency response ability and predict the development trend of network security They are of great significance.

Network security situation awareness technology can be divided into three stages: situation element extraction, real-time situation understanding and future situation prediction.

## 2.2 Network security situation in smart grid

### 2.2.1 Situation factor extraction

In the daily work of network security of power grid, it is necessary to collect, understand and predict various factors of network security changes of smart grid system, and strive to accurately grasp the network security situation of power grid, so that the network security management of smart grid changes from passive defense to active prevention. The staff can judge the state trend of the system security through the situation awareness prediction, and take effective security measures in time before the grid is attacked by malicious attacks.

At present, all kinds of information that can be collected in smart grid mainly include topological structure, real-time operation information, equipment status information, power grid steady-state data information, power grid dynamic data information, power grid transient fault information, power grid operation environment information, etc. The result of this paper is preparation for the understanding, evaluation and prediction of power grid security situation.

### 2.2.2 Situation factor extraction

In smart grid, the former situation recognition is based on the extraction of situation elements. Its key point is to analyze the collected data first, and then evaluate the current network situation. Traditional situation assessment methods include Bayesian network, artificial neural network, fuzzy logic method, etc., and situation assessment model is the basis of assessment methods.

### 2.2.3 Situation security prediction of smart grid

Through the research and analysis of various network situation prediction technologies, each technology has its advantages and disadvantages. Due to the particularity of smart grid system, it is not easy to be directly applied to the network of smart grid, so a new combined prediction technology is needed. After collecting, perceiving, analyzing and evaluating the situation information and elements of smart grid, this paper summarizes and infers the development law of power grid situation, and forecasts the future situation of power grid. The result of situation prediction is the main reference of smart grid regulation and control.

## 2.3 Status quo of security situational awareness technology for domestic and foreign power grids

With the maturity of wide area measurement system (WAMS), ICT and advanced measurement infrastructure (AMI), situation awareness technology plays an irreplaceable role in ensuring the security of power grid and develops rapidly.

At present, a lot of research work has been done on network security detection and prevention of transmission system at home and abroad. The SIFT project of NCASSR [4] [5] developed security situation awareness software such as NVisionIP and VisFlowConnect-IP. Braun and jessant [6] and Lu [7] of Lincoln lab used support vector machine as the synthesis basis to fuse various types of information, so as to realize situation awareness. In China, Wang Xuan Hong [8] put forward two

ISSN: 2414-1895 DOI: 10.6919/ICJE.202005_6(5).0009

kinds of security situation prediction and evaluation algorithms based on D-S evidence theory and support vector machine respectively; Jiang Chengzhi and others [9] put forward a new security situation awareness model of power system information network based on intelligent agent; Zhang Yong [10] put forward a risk estimation model of smart grid operation based on fuzzy theory. However, most of the above research work is only for theoretical research, and the research object cannot well cover the characteristics of information physical system (CPS), and the research on situation awareness cannot be effectively combined with smart grid.

Therefore, the development of a new means to identify, predict and respond to network attacks has become a key research direction in the field of power system network security at present and in the future.

## 3. Smart grid security situation awareness method

### 3.1 Security situation awareness of smart grid based on big data analysis

The network components (e.g. switches, routers) and security components (IDS, access control system, etc.) of the wide area power system in the smart grid can generate security related big data, which are very valuable resources for security situation awareness. Based on the long-term monitoring of smart grid, the security situation awareness can be realized by analyzing the generated big data related to security.

The security situation awareness mechanism of smart grid based on big data analysis combines fuzzy clustering, game theory and reinforcement learning to realize the security situation analysis of smart grid.

Firstly, the security data related to the main electrical equipment, substation bus, network equipment, substation controller, control center and engineer station in the smart grid are collected by agent technology; secondly, the collected data are gathered to the security situation awareness center, and the association method based on fuzzy clustering is used to conduct preliminary association analysis of the collected data; finally, game theory and Strengthen learning to conduct security situation awareness.

The basic design principle is shown in Figure 1:

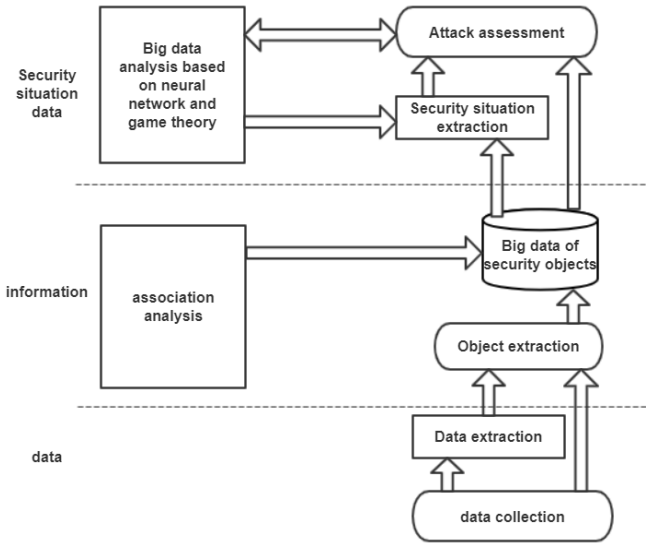


Figure 1. Design principles based on big data analysis

#### 3.1.1 Situation factor extraction

In the smart grid security situation awareness mechanism based on big data analysis, security situation data is collected by agent technology.

The agent collecting data collects the relevant data according to the instructions of the security situation awareness center, collects the data to the management layer after filtering and preprocessing,

ISSN: 2414-1895 DOI: 10.6919/ICJE.202005_6(5).0009

and presents the status data of the devices on the client to the management layer through the collection agent.

Three situational factors, network traffic, access control operation and device status, are used to realize basic security situation data collection. For network traffic, network traffic collection is based on simple network management protocol (SNMP) and the underlying network interface to capture the network traffic of the operating system. For device status, SNMP technology is used to collect data of security situation. The security data sources of equipment status include: equipment management system, data collection agent and network management station (NMS). For access control operation data, data broker method is used to collect data from network security devices. In addition, the feature extraction of security situation is based on information gain ratio (IGR), which is used as a measure to determine the correlation of each feature.

#### 3.1.2 Correlation analysis of security situation factors

In the smart grid security situation awareness mechanism based on big data analysis, fuzzy clustering based on graph theory is used to realize data association analysis, and fuzzy equivalence relationship is used to cluster and associate the big data of situation factors.

#### 3.1.3 Security situation awareness prediction

Using game theory and machine learning to realize the security situation awareness of smart grid. In the smart grid security game, legitimate users and attackers are a pair of players. The most important problem for players is to adjust their behaviors according to the behaviors of other players in the interactive environment. The equilibrium in game theory is a long-term process in which irrational players find the best result over time.

In order to implement security situation awareness in smart grid, hierarchical neural network is introduced into game theory. According to the requirements of security situation factors, input and output parameters are based on the above factors to collect and extract rules. In addition, many factor values are collected as training samples of neural network. In order to build a security situation awareness model, the real security factor data is input into the neural network. Next, the output of the neural network is compared with the output of the modeling object, and the error is used to adjust the parameters of the learning model. Finally, a neural network is established to show the corresponding relationship between the actual input and output.

### 3.2 Security situation combination prediction of smart grid based on information fusion

Due to the particularity of power system and the randomness and uncertainty of network security situation, the results of power grid security situation are often affected by many factors, and a single prediction model is difficult to get more accurate security situation prediction value. Therefore, different algorithms can be fused to improve the accuracy of prediction.

Based on the information fusion, the combined forecasting method of security situation of smart grid is proposed. Through artificial immune model, the security situation value of power grid is obtained based on the information collected in smart grid, and the combined forecasting method is realized by combining grey correlation degree, grey prediction, neural network model and Kalman filter.

In the stage of situation understanding, the real-time risk detection method of network security, which is similar to the principle of artificial immune, is used to establish the clone selection, learning mechanism and life cycle model of antibody, and a risk prediction model of network security based on antibody concentration is proposed. In the stage of situation prediction, the grey correlation analysis is used to combine grey prediction, neural network and Kalman filter is used to get the combined prediction method based on information fusion.

#### 3.2.1 Acquisition of safety situation value

Collect data, use artificial immune model to calculate the network security situation value of power grid.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202005_6(5).0009

The main function of the human immune system is to distinguish the self-harmlessness and non-self-harmfulness in the human body and to remove foreign bodies. The antibody concentration in human body is affected by the invasion of foreign microorganisms, and the severity of patients' illness can be evaluated by the concentration of different antibodies.

On the basis of human immune network security model, the mapping relationship between human immune system and artificial immune model is established. The corresponding relationship between human immune system and artificial immune model is shown in Table 1.

Table 1. Correspondence between human immune system and artificial immune model

| Human immune system | Artificial immune model |
|---|---|
| antigen | The binary string is obtained by extracting the characteristics of the message (IP datagram, TCP message, etc.) |
| B cells, T cells and antibodies | Antibody in binary string |
| Binding of antibody and antigen | r continuous bit matching algorithm |
| Autologous tolerance | Negative selection algorithm |
| Cell clone | Antibody replication |
| Increase in antibody concentration | Increased security risk of the system |
| human body | Hosts in the network |

As shown in Table 1, the host in the network is equivalent to the human body. Each host with security policy in the network can independently generate and train antibodies in the environment of network security threat, and memory cells generate memory antibodies. Once the corresponding antigens that have been invaded are found, they will copy themselves and generate corresponding antibodies.

When the host running in smart grid is faced with potential danger, the importance of different hosts and the harm degree of different types of attacks are considered respectively. Suppose that $\alpha_j(0\leq\alpha j\leq 1)$ is the harm degree of J-type attack behavior, $\beta i(0\leq\beta i\leq 1)$ is the importance of host i , xi is the number of antibodies detected by host i in the normal operation environment of smart grid, Ni is the number of antibodies detected by host I at any time, and $n_i$ is the number of antibodies detected by host i to deal with J-type attack. Let $r_i(t)$ represent the security situation value of host i at time t, $r_{ij}(t)$ represent the security situation value of host i under type j attack threat at time t, $R_j(t)$ represent the security situation value of the whole system under type j attack threat at time t, and R (t) represent the security situation value of the whole system at time t. The calculation methods of $r_i(t)$、$r_{ij}(t)$、$R_j(t)$、R(t)are shown in Figure 2:

$$r_i(t) = 1 - \frac{1}{1 + \ln(\beta_i|n_i - x_i| + 1)}$$

$$r_{ij}(t) = 1 - \frac{1}{1 + \ln(\alpha_j\beta_i|n_{ij} - x_i| + 1)}$$

$$R_j(t) = 1 - \frac{1}{1 + \ln(\alpha_j \sum_i \beta_i |n_{ij} - x_i| + 1)}$$

$$R(t) = 1 - \frac{1}{1 + \ln(\sqrt{\sum_i (\beta_i|n_i - x_i|)^2} + 1)}$$

Figure 2. calculation methods of $r_i(t)$、$r_{ij}(t)$、$R_j(t)$、R(t)

ISSN: 2414-1895 DOI: 10.6919/ICJE.202005_6(5).0009

Obviously, all values are in the [0,1] range, which helps to visualize the current safe operation state of the system. The higher the value is, the more likely the power system is to be attacked; the closer the value is to 0, the lower the risk is.

### 3.2.2 Prediction of safety situation value

Obtain samples, respectively, use gray prediction algorithm, RBF neural network algorithm, Kalman filter algorithm to calculate the security situation value in the next period of time.

The results of power grid security situation are often affected by many factors. A single prediction model is difficult to get more accurate security situation prediction value. Therefore, different algorithms can be fused to improve the accuracy of prediction. GM (1,1) model of grey system theory can carry out grey prediction, which is simple and easy to realize. Its prediction results can correctly reflect the development trend of the sequence, but it is difficult to reflect the periodicity and randomness. RBF neural network prediction model can get more accurate results, but it takes a certain time to train the samples, and it may fall into local solution Sex. Kalman filtering algorithm is a kind of optimal autoregressive data processing algorithm, which can predict the next value through a set of sequences under the premise of noise, with high efficiency.

The above-mentioned different algorithms have their own advantages and disadvantages. Combining multiple models and using data fusion can reduce the impact of the characteristics of a single algorithm on the situation prediction results of smart grid network, to a certain extent, it can make up for the limitations of a single algorithm, which is more comprehensive and reliable than a single prediction algorithm.

### 3.2.3 Analysis based on grey relation degree

Comparing the obtained value with the real value of security situation, the grey correlation degree between each value and the real value is calculated, and then the combined weight of three models is obtained. Finally, the more reasonable prediction value of security situation of power grid network is obtained by combining the three models.

Figure 3 shows the overall situation awareness algorithm flow of the smart grid security situation combination prediction method based on information fusion:

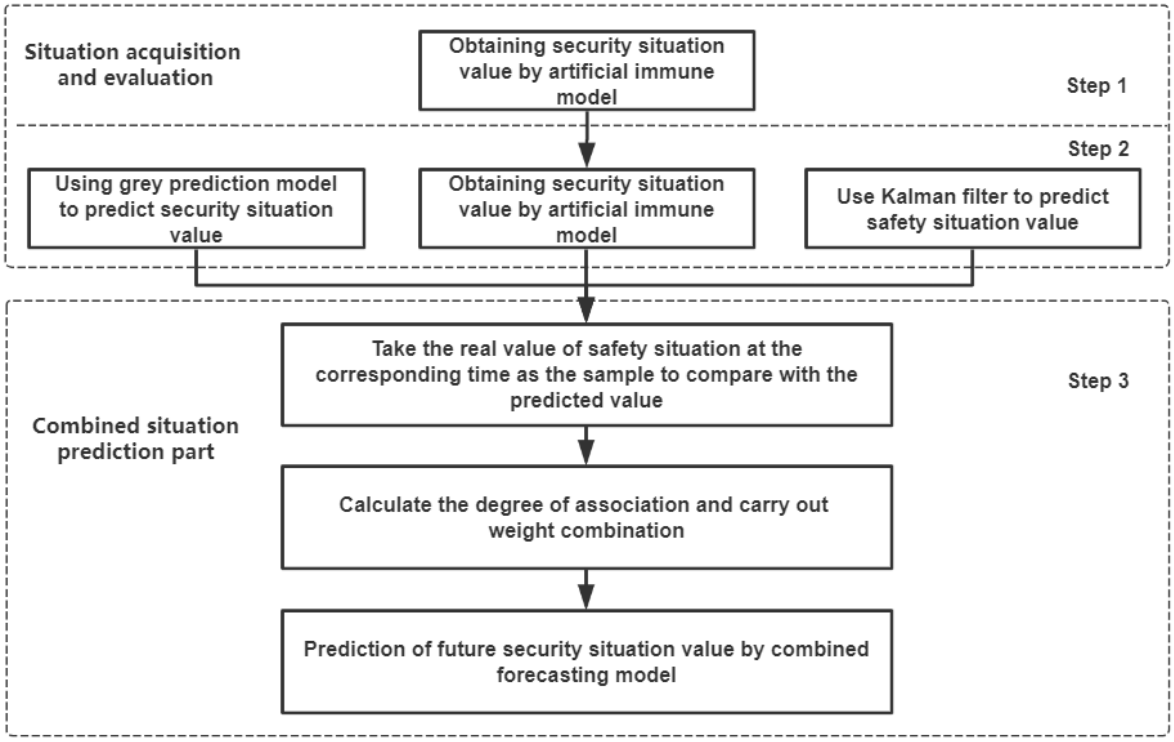


Figure 3. Overall situation awareness algorithm flow

ISSN: 2414-1895 DOI: 10.6919/ICJE.202005_6(5).0009

## 4. Conclusion

With the development of smart grid system, the combination of smart grid and public network is more and more extensive. The problem of network security faced by smart grid is more and more complex, and the attack methods for smart grid are more and more diversified. The future smart grid must integrate advanced information security technology, not only need to resist all kinds of new attacks, but also have the ability to predict unknown threats and attacks, to ensure the normal operation of smart grid.

The smart grid situation awareness technology based on big data analysis combines fuzzy clustering, game theory and reinforcement learning to realize the security situation analysis of smart grid.

Based on information fusion, combined forecasting method of smart grid situation awareness is proposed. Through artificial immune model, the security situation value of power grid is obtained based on the information collected in smart grid. Combined with grey correlation degree, combined with grey forecasting, neural network model and Kalman filter, the combined forecasting method is realized.

Two kinds of situation awareness algorithms have certain accuracy to predict the network security situation of smart grid, and can effectively reflect the change trend and development of power grid security situation. The smart grid security situation awareness mechanism based on big data analysis can get the quantitative smart grid security risk value, and has a low error rate. The forecasting accuracy of the combined forecasting method based on information fusion is higher than that of the single forecasting model.

## Acknowledgments

This paper was financially supported by “the Fundamental Research Funds for the Central Universities (2016MS122)”.

## References

[1] Wu J , Ota K , Dong M , et al. Big Data Analysis-Based Security Situational Awareness for Smart Grid[J]. IEEE Transactions on Big Data, 2016.

[2] Gang L I , Zheng-Xin T , Ji-Feng L I , et al. Security Situation Awareness and Combination Forecasting in Smart Grid[J]. Electric Power Information and Communication Technology, 2016.

[3] Peng Y , Zhi-Cheng M A , Dan J , et al. Evaluation model of network situation and its awareness prediction oriented to intelligent power grid[J]. Journal of Lanzhou University of Technology, 2015.

[4] Lakkaraju K , Yurcik W , Bearavolu R , et al. NVisionIP: An interactive network flow visualization tool for security[C]// Proceedings of the IEEE International Conference on Systems, Man & Cybernetics: The Hague, Netherlands, 10-13 October 2004. IEEE, 2004.

[5] Yin X , Yurcik W , Slagell A . The design of VisFlowConnect-IP: a link analysis system for IP security situational awareness[C]// IEEE International Workshop on Information Assurance. IEEE, 2005.

[6] Jerome J. Braun,Sunil P. Jeswani. Information fusion of a large number of sources with support vector machine techniques[P]. SPIE Defense + Commercial Sensing,2003.

[7] Lu J , Yang X , Zhang G . Support vector machine-based multi-source multi-attribute information integration for situation assessment[J]. Expert Systems with Applications, 2008, 34(2):1333-1340.

[8] WANG Xuan-hong, XIAO Yun. Network Security Situational Awareness Model Based on Information Fusion [J]. Science Technology And Engineering,2010,10(28):6899-6902. DOI:10.3969/j.issn.1671-1815.2010.28.010.

[9] Cheng-Zhi J . Research on Electric Information Network Security Situation Awareness Model Based on Intelligent Agent[J]. Computer Science, 2012.

[10] Yong Z . Smart Grid Operation Risk Assessment System Based on Fuzzy Theory[J]. Power & Energy, 2015.