Security Situation Awareness and Simulation Analysis of Power Information Communication System

Dong Wang [1,a], Yang Li[1,b], Gang Li[2,c], Li Yan[1,d], Min Zhao[1,e], Chao Han[1,f], Wenqing Zhao[2,g], Min Cui[2,h]

[1]State Grid Shanxi Electric Power Company, Information and Communication Branch, Taiyuan 030001, China;

[2]School of Control and Computer Engineering North China Electric Power University, Baoding 071003, China.

[a]101390080@qq.com,[b]15333666809@126.com,[c]ququ_er2003@126.com

Abstract

Internet technology has significantly increased the automation of power systems, but at the same time increased the risk of attacks on power systems. The log data generated in the operation of power information system is an important basis for the state analysis of power information system， the original log of power information system is used as the analysis data, and a model of security situation awareness of power information system is proposed. In the model, firstly, various situation prediction models are used to predict the state of the power system respectively. Then, the gray correlation algorithm is used to combine the individual predictions to complete the prediction of the security situation of the power information system. Finally, the power information system log data is analyzed and verified. Simulation results show that, combined forecasting model has more accurate prediction results than the single prediction model, at the same time, it can effectively predict the safety situation of the power information system.

Keywords

Log normalization; Situation awareness;Grey Relational Analysis; Combinational situation prediction.

1. Introduction

With the increasing informatization of the power system, and the operating efficiency has also been improved, which has brought convenience to users and increased the security risks of the power system.The emergence of Stuxnet [1] has made people realize the risks of the coupling of information systems and physical systems. At the same time, the security problems of CPPS have attracted wide attention from scholars at home and abroad.The literature [2] takes the cascading failure of the power system in Italy in 2003 as an example, and proposes two interdependent network cascading failure analysis methods. The literature [3] conducted a preliminary discussion on the form of risk propagation in power system, and established a threat transfer model using cellular automata. This model is used to analyze the influence of several key points such as the success rate of transmission and the self-healing rate of equipment in the threat transmission process of power system.

In addition, with the increasing complexity of power systems, data fusion and security situational awareness technologies have become hot research issues in the field of power system security.Therefore, the use of data analysis technology to process massive heterogeneous log data of power information systems has become a feasible solution.Distributed computing has significant advantages over traditional single computers when dealing with massive amounts of data.For example, through Hadoop [4], multiple computers can simultaneously analyze and mine data.Literature [5] proposed a method for distributed storage of log files by multiple computers, and then used the Syslog file transfer protocol to complete the collection of logs, and implemented IP

statistics algorithms for Dos and DDos attacks.However, current log analysis strategies and tools are still not well applied to power information systems [6-8].On the other hand, as an important basis for the determination and early warning of the risk level of power information systems, situational awareness is also an important part of the system security field.Literature [9] first introduced the basic concept of network security situational awareness, and then elaborated on the research status of network security situation awareness from various layers [10-13].

In view of the above situation, this paper proposes a security situational awareness model based on log data of power information system. Firstly, the power information system log data is filtered and normalized to realize pre-processing of the data. Then, evaluated the security situation of the power information system based on the human immune model [7] .Finally, based on the evaluation results, a variety of situation predictions are carried out, and various situation predictions are combined to obtain a prediction result of the final situation.

2. Security Situation Awareness Model

The model includes four steps: data preprocessing, situation assessment, multi-angle security situation prediction and combined situation prediction. The structure block diagram of the model is shown in Figure 1:

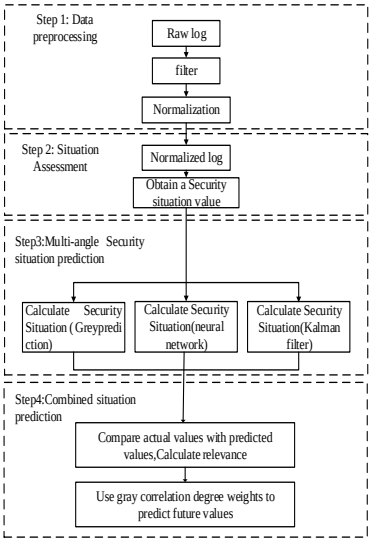

Figure 1 Model structure block diagram

2.1 Data Preprocessing

The power information system logs a lot of valuable system operation information, but there is a lot of redundancy and duplicate data in the log. Also, different vendors choose different logging formats, which results in log data not being directly available for data analysis. Therefore, in order to facilitate the extraction of important information in the log in the situation assessment, it is necessary to filter and normalize the log data.

Filtering phase: mainly combines and deletes duplicate data within a specified time. Delete unnecessary logs based on the contents of the log, timestamp, IP address, and priority. Then, according to the timestamp and the IP address, the log messages that are too long and unconcerned are rounded off and the redundant data is discarded.

Normalization phase: Although different vendors do not have a unified log format, the information structure recorded by the logs is relatively fixed. Even though the final storage mechanism for different types of logs is different, most of the fields are basically generic. Therefore, for the frequently occurring fields, this document chooses to keep the following fields such as timestamp, source IP address, destination IP address, source port, destination port, user information, priority, etc. during the normalization process.

As described above, the normalization process for a log record is as follows. The following is a SourceFire IPS syslog message:

Jul 16 10:54:39 SourceFire SFIMS: [1:469:1] ICMP PING NMAP

[Classification: Attempted Information Leak] [Priority: 2] (ICMP)

210.22.215.77 -> 67.126.151.137

First, use the parsing technique to scan the entire log message from start to finish, extract the part of interest out of the normalized field of time, the following is a set of common fields for normalization:

Type: Attempted to disclose information

Timestamp: July 16, 10:54:39

Priority: 2

Agreement: ICMP

Source IP address: 210.22.215.77

Target IP address: 67.126.151.137

Source port: none

Target port: none

For the acquisition of the IP address, you can use the following regular expression: \d+\.\d+\.\d+\.\d+

In this case, a valid IP address (such as 192.168.12.3) may be captured or an invalid IP address (such as 400.300.2.666) may be captured. Therefore, a regular expression matching a IP address must ensure that each number is within the correct range, in addition to detecting four numbers separated by periods. To verify the IP address, modify the regular expression to:

((?:(?:25[0-5]|2[0-4]\d|((1\d{2})|([1-9]?\d)))\.){3}(?:25[0-5]|2[0-4]\d|((1\d{2})|([1-9]?\d))))

Then, parse the target log file with the appropriate regular expression, separate the required parts of the log and re-integrate it into the target format. At the same time, keep the original log as part of the normalization event and restore the original log if necessary.

2.2 Situation Assessment

After the log data is filtered and normalized, the log data needs to be analyzed and processed to predict the state of the power information system.

2.2.1 Log Analysis

At present, there are two main methods of log analysis commonly used. One is to form a knowledge base by combining log knowledge related to abnormal behavior, and then detect the attack behavior by information matching. The other is to summarize the normal operation of the power system and the behavior of normal users to form a knowledge base, and then compare the currently obtained information with the knowledge base. The first method is based on creating rules to capture known threats, but it is difficult to detect unknown threats that are not yet known. The second method is suitable for capturing things that are not yet known. This article uses the second method for log analysis.

2.2.2 Obtaining a security situation

This paper uses the human immune network security model proposed in [7] to obtain the security situation.

Because in different logs, in addition to information such as timestamps, addresses, etc., a specific event is recorded in the log. This article extracts the number of identical events as a baseline based on the event information provided by the normalized logs collected over a period of time. In the power information system, the importance of different hosts and the effects of cyber attacks are different. In this paper, the differences between host and attack types are included in the security situation analysis. Then count the number of events that occurred during the timestamp period based on the timestamp. Among them, the IP address is used to represent a specific host.

Let *t* be the time of a certain timestamp obtained by normalizing the log, $\alpha_j\left(0 \le \alpha_j \le 1\right)$ is the degree of harm of the *j*-type event, and $\beta_i\left(0 \le \beta_i \le 1\right)$ is the importance of the host *i*, x_i is the number of events of host *i* during normal operation of the power information system, x_{ij} is the number of *j*-type events that occur in the host *i* under the normal operating environment of the power information system, n_{ij} is the number of *j*-type time that host *i* has occurred at a certain moment. $r_i(t)$ indicates the security situation value of the host *i* at time *t*, $r_{ij}(t)$ indicates the security situation value of the *j*-type event occurring on the host *i* at time *t*. $R_j(t)$ indicates the security situation value of the *j*-type attack in the power information system at time *t*. $R(t)$ indicates the security situation value of the power information system at time *t*.The calculation methods for $r_i(t)$、$r_{ij}(t)$、$R_j(t)$ and $R(t)$ are as follows [12]:

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

$$r_{ij}(t) = 1 - \frac{1}{1 + \ln\left(\alpha_j \beta_i \left| n_{ij} - x_{ij} \right| + 1\right)} \tag{2}$$

$$R_j(t) = 1 - \frac{1}{1 + \ln\left(\alpha_j \sum_i \beta_i \left| n_{ij} - x_{ij} \right| + 1\right)} \tag{3}$$

$$R(t) = 1 - \frac{1}{1 + \ln\left(\sqrt{\sum_i \left(\beta_i \left| n_i - x_i \right|\right)^2} + 1\right)} \tag{4}$$

The security situation value is in the range [0,1], indicating the current security state of the system. The larger the security situation value indicates the greater the system security risk, and vice versa, the lower the security risk.

2.3 Multi-angle Security Situation Prediction

Before the power information network is attacked by different modes of network attacks, the security situation prediction can help the system administrator to adopt targeted defense methods and processing methods. After a series of processing and analysis on the above-mentioned power information system log data, the multi-angle security situation prediction method is used to predict the security situation of the power information system based on the obtained security situation value.

In this paper, the gray prediction model, neural network model and Kalman filter are used to predict the security situation of the power information system.Among them, the gray prediction model can complete the prediction with a small amount of data, and the model does not need special processing on the data.Therefore, in the security situation of the power information system, the use of the gray prediction model not only ensures the accuracy of the prediction, but also does not need to collect a large amount of data.In addition, the RBF neural network model and Kalman filter are also used to predict the security situation of power information systems.

2.3.1 Grey Prediction Model

The grey prediction model mainly judges the degree of association between the factors by identifying the similarities and differences of the trend trends among the target factors, and then finds the change law in the research object.

In this paper, the GM(1,1) model in the grey theory [13] is used, and the time series of security situation values is: $R(t)$={r(t_1),r(t_2),...,r(t_n)} .After accumulating, an increasing time series $\hat{R}(t)$ is obtained and a differential equation is established to estimate the development of the power information system in a near period of time, and then the prediction function F(t) is obtained.

2.3.2 Neural Network Prediction Model

In this paper, the model is trained by stochastic gradient descent method, and then the network training error is minimized.According to the chain partial differential rule, the adjustment amounts of data center, width and weight in the network are obtained as follows:

$$\mathrm{V}c_i = \eta_1 \frac{\omega_i}{\sigma^2_1} \sum_{j=1}^{N} e_1 G(x_j)(x_j - \mathrm{c}_i) \tag{5}$$

$$\mathrm{V}\sigma_i = \eta_2 \frac{\omega_i}{\sigma^3_1} \sum_{j=1}^{N} e_i G(x_j) \| x_j - \mathrm{c}_i \|^2 \tag{6}$$

$$\mathrm{V}w_i = \eta_3 \sum_{j=1}^{N} e_i G(x_j) \tag{7}$$

Where G represents a Gaussian function,*i* and *j* are subscripts of the number of hidden nodes and the number of samples. c, σ, ω represent network data center, width and weight respectively, η_1, η_2, η_3 indicate their respective learning rates (speed),*e* represents the residual between the network output value and the sample value

In the RBF network, the hidden layer neurons are composed of an activation function and a distance function. The closer to the data center, the more likely the sample is activated. On the contrary, the sample network has less influence on it.

2.3.3 Kalman filter

The process equations and measurement equations of the Kalman filter algorithm are:

$$\mathrm{x}(k+1) = \mathrm{A}x(k) + \mathrm{B}u(k) + \mathrm{w}(k) \tag{8}$$

$$\mathrm{Z}(k+1) = \mathrm{H}x(k+1) + \mathrm{v}(k+1) \tag{9}$$

Where *A* and *B* are system parameters and *H* is the parameter of the measurement system.*W(k)* and *V(k)* represent the noise of the process and measurement.Based on known security situation values *Z(1)*, *Z(2)*, *Z(3)* and *Z(n)*.When $n \geq l$, the least squares estimate of each component of the state vector *x(i)* can be found.The steps to make a security situation prediction using a Kalman filter pair are:

Step 1: Initialize

$$\mathrm{x}_1(n) = E\{x(1)\} \tag{10}$$

$$K(1,0) = E\{[\mathrm{x}(1) - \mathrm{x}_1(1)][\mathrm{x}(1) - \mathrm{x}_1(1)]^N\} \tag{11}$$

among them, $\mathrm{x}_1(1)=E\{\mathrm{x}(1)\}$.

Step 2: Observing the vector sequence

Observation vector sequence: $\{\mathrm{J}(1),\mathrm{J}(2),\mathrm{J}(3),...,\mathrm{J}(n)\}$.

Step 3: Calculate the values of the different parameters in the model

$$G(n) = F(n+1,n)K(n,n-1)\left[C^N(n)K(n,n-1)C^N(n) + Q_1(n)\right]^{-1} \tag{12}$$

$$\alpha(n) = J(n) - C(n)\mathrm{x}_1(n) \tag{13}$$

$$\mathrm{x}_1(n+1) = F(n+1)\mathrm{x}_1(n) + G(n)\alpha(n) \tag{14}$$

$$P(n) = K(\mathrm{n}, n-1) - F^{-1}(n+1,n)G(n)C(n)K(n,n-1) \tag{15}$$

$$K(n+1,n) = F(n+1,n)P(n)F^N(n+1,n) + \mathrm{Q}_1(n) \tag{16}$$

2.4 Combined Situation Prediction

Compared with the traditional power system, the information physical power system is more complicated. The change of the network security situation is usually caused by multiple factors. A single prediction model can not correctly reflect the system's changing trend. However, through the combination of multiple prediction algorithms, the defects and deficiencies of the individual algorithms can be compensated, thus improving the overall prediction accuracy. In this paper, the different prediction results of various prediction algorithms are fused by the grey correlation degree theory, and then the prediction results closer to the real situation value are obtained.

In two different sequences of variables, the sequence of variables changes over time or other dependent variables. In grey theory, the measure of the connection between such changes is called the grey degree of association. If the change situation of the two variables has similarity to a certain extent, that is, the range of the synchronous change is high, indicating that the two variables have a high degree of correlation under the influence of the dependent variable. On the contrary, the degree of association between the two is low. This article selects the reference sequence as:

$$x_0=\{x_0(k)|k=1,2,...,n\}=(x_0(1),x_0(2),...,x_0(n)) \tag{17}$$

$$x_i=\{x_i(k)\,|\,k=1,2,...,n\}=(x_i(1),x_i(2),...,x_i(n)),i=1,2,...,m \tag{18}$$

$$\xi(k)=\frac{\min\limits_s\min\limits_t|x_0(t)-x_s(t)|+\rho\max\limits_s\max\limits_t|x_0(t)-x_s(t)|}{|x_0(k)-x_s(k)|+\rho\max\limits_s\max\limits_t|x_0(t)-x_s(t)|} \tag{19}$$

Where k is the time and equation (17) is the correlation coefficient of the sequence x_i relative to the reference number x_0 at time k. Where $\rho\in[0,1]$ is the resolution coefficient, the smaller the ρ is, the smaller the resolution is.

$$r_i=\frac{1}{n}\sum_{k=1}^{n}\xi_i(k) \tag{20}$$

r_i is the degree of association of the series x_i with respect to the reference number x_0 .Firstly, according to different model prediction values, the correlation between the predicted value and the real value of the safety information of the power information system is calculated, and the weight of each model prediction value is determined according to the correlation degree. Then, the different weight values are merged to obtain the final combined security situation prediction value.

3. Case Analysis

In order to verify the validity of the proposed model, the network log data of a power information system is used as the data set of the example for analysis and calculation. Firstly, based on the security situation values from 1st to 7th, the gray prediction model, RBF neural network model and Kalman filter are used to predict the security situation values from 8th to 14th. Then determine the weight of each model's predicted value by the true value of the security situation from 8 to 14 days. Finally, the real value of the situation from 15th to 21st is compared with the prediction values of each single prediction model and the combined model prediction value to verify the validity and accuracy of the proposed model.

3.1 Simulation Environment

In order to simulate the structure of power information system, this paper builds an experimental platform with four computer simulation environments. One server is used as the log server and the task publishing center, that is the master, and the other three are used as slaves in the Hadoop cluster. Then, the IP address, port number, dfs, and replication values are set respectively, and the log data is cached in the log server.

All four computers run in a Linux Ubuntu system environment. First use maven to compile the release version of Hadoop, and configure the core configuration files such as core-site and hdfs-site.

Then set up the run code in Eclipse. Finally, the log data is filtered and normalized separately, and the frequency of occurrence of different events is classified and counted.

3.2 Security Situation Assessment

Normalize the data obtained after filtering, and extract the number of identical events as a baseline based on the event information provided by the normalized log data collected over a period of time. The number of occurrences of various events in the time period indicated by the time stamp is sorted by time stamp, and the obtained data is analyzed by the human immune model [7], and the result is shown in figure 2.

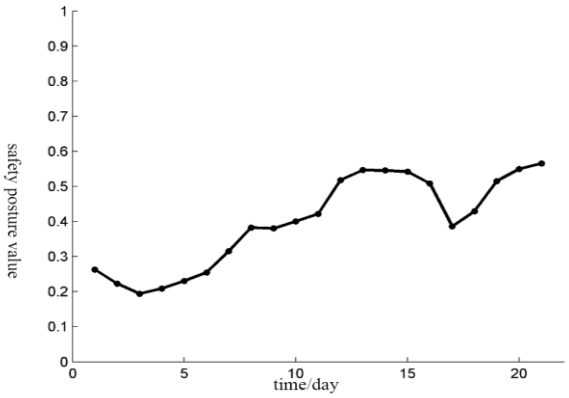

Figure 2 Network security situation assessment

Figure 2 is the result of calculating the security situation value of the normalized log data using the above method. Based on the actual values obtained from the results, the prediction accuracy of the grey prediction model, the RBF neural network model, the Kalman filter model and the combined model are compared.

3.3 Multi-angle Security Situation Prediction

3.3.1 Grey prediction

The security situation values predicted from April 8 to April 14 using the GM (1, 1) model are shown in Table 1:

Table 1 Gray forecast samples and predicted values

	Gray prediction	Sample true value
April 8	0.35	0.38
April 9	0.36	0.37
April 10	0.43	0.40
April 11	0.39	0.41
April 12	0.50	0.49
April 13	0.52	0.51
April 14	0.47	0.50

The values in Table 2 are based on the true security situation values from April 1 to April 7, and the predicted safety situation of the power information system from April 8 to April 14 is predicted.

3.3.2 Neural Network Prediction

The prediction of the security situation values from April 8 to April 14 using the RBF neural network model is shown in Table 2:

Table 2 RBF neural network prediction samples and predicted values

	Neural network prediction	Sample true value
April 8	0.36	0.38

April 9	0.36	0.37
April 10	0.41	0.40
April 11	0.43	0.41
April 12	0.50	0.49
April 13	0.52	0.51
April 14	0.49	0.50

The real security situation value from April 1 to April 7 is used as a training set to train the neural network model of this paper, and then the predicted situation of the security situation from April 8 to April 14 in Table 2 is obtained.

3.3.3 Kalman Filtering Algorithm

The prediction of the security situation value from April 8 to April 14 using the Kalman filter is shown in Table 3:

Table 3 Kalman filter prediction samples and predicted values

	Kalman filter prediction	Sample true value
April 8	0.39	0.38
April 9	0.38	0.37
April 10	0.41	0.40
April 11	0.39	0.41
April 12	0.51	0.49
April 13	0.52	0.51
April 14	0.51	0.50

Table 3 is based on the true security situation value from April 1 to April 7, using the Kalman filter to predict the security situation from April 8 to April 14.

3.4 3.4 Calculation of Grey Correlation and Combination Forecast

According to the actual value of the security situation from April 1 to 7, the three models were used to predict the security situation values from April 8 to 14, respectively. The results are shown in Table 4.

Table 4 Comparison of prediction results with real values

date	Gray prediction	RBF value	Kalman value	actual value
April 8	0.3174	0.3503	0.3444	0.3825
April 9	0.3461	0.3988	0.3846	0.3802
April 10	0.3774	0.4453	0.4658	0.4002
April 11	0.4115	0.4935	0.5078	0.4220
April 12	0.4488	0.5455	0.5540	0.5181
April 13	0.4893	0.5997	0.6297	0.5465
April 14	0.5336	0.6585	0.6404	0.5454

It can be seen from Table 4 that within these 7 days, the gray prediction value and the neural network prediction value have the closest to the true security situation value in 3 days, while the Kalman filter algorithm is only closest to the real security situation value in 1 day.It is indicated that the grey prediction and neural network prediction are better in the single prediction model. In the combined model, the predicted values of the two models should account for a large proportion.

According to the calculation formula of the human immune model, the calculated security situation values are all between 0 and 1, as shown in Table 2, so there is no need to perform dimensionless processing on the calculated values. In addition, this paper takes the real situation value as the reference sequence, calculates the gray correlation degree of the three prediction algorithms, and obtains the correlation degree of each series, as shown in Table 5.

Table 5 Correlation coefficient of three algorithms

r_1	r_2	r_3
0.3048	0.8832	0.7650

After obtaining the gray correlation degree of the three prediction algorithms, the sum of the three kinds of prediction values is 1 when the ratio is constant, and then the weight of the model prediction value in the combined prediction model is obtained. Among them, the weights of the gray model, the RBF neural network model and the Kalman filter are 0.3204, 0.4847 and 0.1949, respectively. The combined security situation prediction model is as follows:

$$P = \sum_{i=1}^{3} \omega_i P_i \quad (\sum_{i=1}^{3} \omega_i = 1) \tag{21}$$

In addition, this paper uses each single prediction model to predict the security situation value of the power information system in the next 7 days, and compares it with the combined situation prediction value of the formula (21) from April 15 to 21, as shown in Table 6.

Table 6 Comparison of combined predicted and actual values

date	Actual value	Predictive value	Absolute error	Relative error
April 15	0.5418	0.5447	0.0029	3.74%
April 16	0.5084	0.4908	-0.0176	5.78%
April 17	0.3859	0.3925	0.0395	17.24%
April 18	0.4288	0.4487	0.0273	14.03%
April 19	0.5151	0.4969	-0.0452	7.51%
April 20	0.5496	0.5431	0.0275	13.77%
April 21	0.5651	0.5640	0.0190	5.46%
average error			0.0265	10.06%

In this experiment, the prediction results obtained by integrating a single prediction model, the combined prediction results and the true value of the security situation

At the same time, in order to highlight the difference between the different curves, the range of the vertical axis is reduced to 0.3 to 0.7 in Fig. 3, and the result shown in Fig. 3 is obtained:

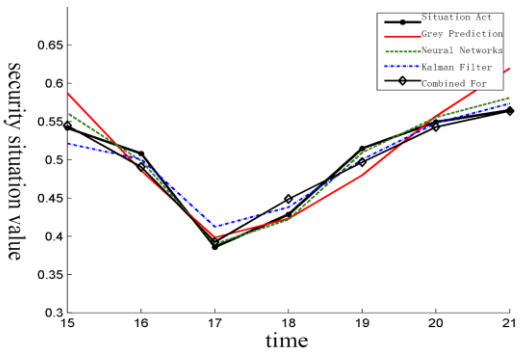

Figure 3 Comparison of combined forecast results with a single forecast

It can be seen from Fig. 3 that the results obtained by the proposed power situation system of the power information system are more consistent with the actual trend of the security situation of the power information system, and the model is more accurate and reliable than using a single prediction model. In addition, the weights obtained by the gray correlation degree can be further updated to maintain the validity of the combined prediction mode. For example, in 7 days, the new correlation degree is recalculated according to the values of the security situation time series predicted by the three prediction algorithms from April 15 to 21.Therefore, the next security factor is predicted and combined on the new correlation coefficient, so that the obtained data is more accurate and credible.

4. Conclusion

Although Internet technology is integrated with traditional power systems, the efficiency of power system operation is improved. However, due to the openness of the Internet and the fact that the current network security protocols are not yet fully mature, potential network security risks are also threatening the operational security of power information systems. This paper takes the power system operation log data as the angle, analyzes the available information from the log data and predicts the future security situation of the CPPS system to achieve the effect of accurate warning.

This article uses the Hadoop distributed computing framework to achieve efficient calculation of big data. At the same time, the problem that the log format is not uniform is proposed. Through a series of rules normalization, the log content becomes data suitable for processing.

Based on the security situation time series value of power information system, a security situation awareness model of power information system is proposed.

The gray correlation degree method is used to combine the prediction results of each single prediction model, and different single prediction results are combined to obtain the combined prediction result of the security situation of the power information system.

Acknowledgements

This work is supported by State Grid Shanxi Electric Power Company Information and Communication Branch Science & Technology Project(Application Research of Power Communication Mobile Operation and Maintenance System Based on Big Data Analysis),double first-class graduate construction project of North China Electric Power University.

References

[1] Ilias Mavridis, Helen Karatza. Performance evaluation of cloud-based log file analysis with Apache Hadoop and Apache Spark[J]. The Journal of Systems and Software 125 (2017) : 133–151.

[2] Buldyrev S V, Parshani R, Paul G, et al. Catastrophic cascade of failures in interdependent networks[J]. Nature, 2010, 464(7291):1025

[3] Ye Xiaming, Wen Fuzhen, Shang Jincheng, He Yang. Information physics security risk propagation mechanism in power system[J].Power grid technology,2015(11):3072-3079.

[4] Ilias Mavridis, Helen Karatza. Performance evaluation of cloud-based log file analysis with Apache Hadoop and Apache Spark[J]. The Journal of Systems and Software 125 (2017) :133–151.

[5] Ren Kai, Deng Wu, Yu Wei. Research on Network Log Analysis System Based on Big Data Technology[J]. Modern Electronic Technology, 2016(1): 39-44.

[6] Wang He, Liu Wei. Network Log Analysis Based on Data Mining[J]. Journal of Suzhou University, 2011(4): 43-47.

[7]LI Gang,TANG Zhengxin,LI Jifeng,MA Xiaobo,YIN Jun.Safety situational awareness and combined forecasting of smart grid[J].Electric Power Information and Communication Technology,2016,14(11):1-7.

[8] Huang Xubo, Liu Xiaojie, Li Tao, et al. An immune-based network security risk assessment method[J]. Journal of Computer Applications, 2005, 22(4): 213-215.
[9] Li Shuo, Dai Xin, Zhou Yixia. Research progress of network security situational awareness[J]. Journal of Computer Applications, 2010(9): 3227-3232.
[10] Deng Julong. Grey System Theory [M]. Wuhan: Huazhong University of Science and Technology Press, 1990.
[11] Rifkin J . The third industrial revolution: how lateral power is transforming energy, the economy, and the world[M]. New York：Palgrave Mac Millan，2011：28-34.
[12] Zhao Junhua, Wen Fuzhen, Xue Yusheng, et al. The architecture of power CPS and its implementation technology and challenges [J]. Automation of Power Systems, 2010, 34(16): 1-7.
[13] Tang Wei, Wang Qi, Ni Ming, et al. Analysis of Network Attacks in Power Information Physics Fusion System[J]. Automation of Electric Power Systems, 2016, 40(6): 148-151.