Int J Software Informatics, Volume 8, Issue 2 (2014), pp. 167–176
International Journal of Software and Informatics, ISSN 1673-7288

E-mail: ijsi@iscas.ac.cn
http://www.ijsi.org
Tel: +86-10-62661040

Predicting Network Security Situation Based on a Combination Model of Multiple Neural Networks

Yaxing Zhang and Shuyuan Jin

(Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China)

Abstract Due to rapidly increasing complex attacks, networks become more and more insecure. How to accurately predict the future security situation of networks is thus an important research issue. Forecasting security situation can improve the awareness of network states and provide decision support to threat analysis and network planning. This paper provides a combination model of neural networks to predict the security situation of computer networks. Our contribution is in two aspects. On the one hand, we select several single neural network models including Backward Propagation (BP) network, Elman network, and Radial Basis Function (RBF) network to construct the combination model. On the other hand, we use the entropy method to determine the weights of each single model in the combination model. Experimental results show that the proposed combination model can predict the security situation of networks more effectively than any single neural network.
Key words: network security situation prediction; combination model; BP neural network; Elman neural network; RBF neural network

Zhang YX, Jin SY. Predicting network security situation based on a combination model of multiple neural networks. *Int J Software Informatics*, **Vol.8, No.2 (2014): 167–176. http://www.ijsi.org/1673-7288/8/i186.htm**

1 Introduction

Tremendous attacks on Internet call for understanding both the current and future situations of network security. Accurately predicting the trend of network security situation can help network analysts to know how their network statuses vary in the next moment, which can be helpful to assess whether or not the current network is in danger. If the current network is insecure, the network administrators can take measures to prevent potential attacks, such as patching their computer systems. Accurate prediction of network security situation can help with better decision-making, and avoid huge losses due to potential attacks.

Network security situation awareness refers to the operational picture that integrates all relevant information for identifying attacks and selecting appropriate countermeasures[5]. This operational picture reveals the overall security status of the supervised network. And the information captured in the awareness process can be used to predict the security situational trend of the network[6]. There are many

Corresponding author: Yaxing Zhang, Email: zhangyaxing19@gmail.com; Shuyuan Jin, Email: jinshuyuan@ict.ac.cn
Received 2014-05-13; Revised 2014-08-24; Accepted 2014-09-12.

tools that can provide network security situation information. For example, NVisionIP provides security analysts with information of network states by displaying the network topology and traffic flows among hosts in a Class-B network[11]. VisFlow Connect-IP gives a global view of the supervised network, and can dynamically display the changes of IP connections and traffic flows[12]. The SiLK tool can record network traffic flows that provide both historical and current records for analysis[13]. However, these tools only focus on some aspects of the current or past network security situation.

As an essential part of network security situation awareness, network security situation prediction was first introduced by Bass T.[10], which predicts the future situation of network security based on the historical security situation assessment. The prediction of network security situation can promote faster and better network security situation awareness[7]. Several methods are proposed to predict intrusions in networks[14-16]. Although the existing approaches can discover single or specific complex attacks, there is still a lack of effective methods to predict the global security situation of the supervised network.

BP neural network has been widely applied in many fields, such as information processing, pattern recognition and automation, because of its better non-linear approximation capacity[17]. Tang et al. proposed a method of network security prediction based on dynamic BP neural network with covariance to resolve the limitations of depending on experts giving weights[18]. Radial Basis Function (RBF) neural networks attracted much more attention due to their better abilities of approximation of complex nonlinear mapping directly from input data to output data[17]. Meng et al. predicted the network security situation using RBF neural network with hybrid hierarchy genetic algorithm[19]. You et al. presented a method of network security situation prediction based on Elman neural network with the advantages of dynamic memory[20]. However, because the above-stated methods which use a single neural network, are inclined to jitter and fail to predict accurately when there are fluctuations in network security situations. To address the above problem, this paper provides a combination model of neural networks, which consists of BP network, Elman network and RBF network, to predict network security situation. Simulation experiments are made to compare this proposed model with the models using single neural network. Experimental results show that the proposed model is better any than single neural network. This paper is structured as follows. Section II introduces the profile of situation prediction. The neural network combination model used in this paper is described in the Section III. Section IV presents the simulation experiments to show the effectiveness of the model. Section V draws conclusions with a summary and presents future work.

2 Situation Prediction

Generally, situation prediction can be considered as a problem of nonlinear time series prediction[21], which uses the historical network security situations to predict the next state of network security situation. Assume that there is a series of historical values of network security situations, the next moment of which will be predicted by

a prediction function using the past M values as input, as shown in Eq. (1).

$$ns_{M+1} = f(ns_1, ns_2, ns_3, \ldots, ns_M) \tag{1}$$

where $\{ns_1, ns_2, ns_3, \ldots, ns_M\}$ represent the past M values of network security situation. Thus, the prediction problem can be regarded as a functional approximation problem, and the function need to fit the hyper surface in $M + 1$ dimensions space[21].

3 Neural Network Combination Model

Artificial Neural Network (ANN), also called Neural Network (NN), is a kind of artificial intelligence approach, and was developed in 1980s. In recent years, NN has a huge breakthrough both in theory and practice[22]. It has become an emerging field of interdisciplinary frontier, which involves computer science, artificial intelligence, brain science, information science and intelligent control, etc.

3.1 BP network model for situation prediction

BP network is a feed-forward network with three or more layers. And each layer has several neurons. The network is trained with back propagation algorithm to learn the relationship of the input and output. The back propagation algorithm spreads error from back to front, and then adjusts the weights and threshold between layers to minimize the errors between the actual and predicted output[23]. Generally speaking, BP network consists of input layer, hidden layer and output layer. The hidden layer may contain more than one layer. The BP network architecture of situation prediction presented in this paper is shown as figure 1. The neurons of input layer, hidden layer and output layer in figure 1 are set to M, K, and N respectively.

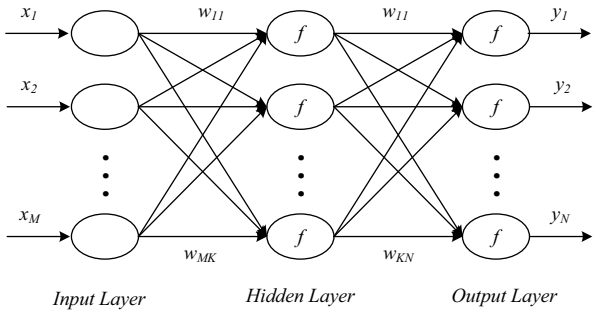

Figure 1. BP neural network architecture of situation prediction.

As Fig. 1 showing, the output of BP neural network can be shown in following equation.

$$y_j = g\left(\sum_{i=1}^{K} w_{ij}^{HO} * f\left(\sum_{m=1}^{M} w_{mk}^{IH} * x_m - \theta_k^H\right) - \theta_j^O\right) \tag{2}$$

where $k = 1, 2, \ldots, K, j = 1, 2, \ldots, N$, $(y_1, y_2, \ldots, y_N)$ expresses the output of BP network, $(x_1, x_2, \ldots, x_M)$ expresses the input of BP network. w_{ij}^{HO} presents the weight between the hidden layer and the output layer, w_{mk}^{IH} presents the weight between the

input layer and the hidden layer. θ_j^O denotes the threshold of hidden layer, θ_k^H denotes the threshold of output layer.

Assuming that there is a time series of length L, $X = \{x_i | x_i \in R, i = 1, 2, \ldots, L\}$. According to the sliding-window scheme, the series can be divided into two parts including training samples and testing samples. If the number of training samples is H, which is to say there will be H sets of input as $(x_1, x_2, \ldots, x_M)$ used to train BP network, the same as the output of network. Then the error of whole training data is shown as follows. f is the transmission function in the hidden layer and g is the transmission function in the output layer. In this paper, f is the logsig function and g is the purelin function.

$$E = \frac{1}{H} \sum_{h=1}^{H} \sum_{j=1}^{N} (y_j^h - T_j^h)^2 \tag{3}$$

where $h = 1, 2, \ldots, H$, $(y_1^h, y_2^h, \ldots, y_N^h)$ and $(T_1^h, T_2^h, \ldots, T_N^h)$ denote the actual output and expected output of BP network when the input is the hth sample. E denotes the error between actual output and expected output of training samples.

The BP network uses training samples consisting of the input and corresponding output. Then the BP network will propagate the error between actual output and expected output back to the previous layer from the output layer and update the weights between the two layers until the earliest hidden layer is reached. If the error is greater than we desired, this process will be repeated.

After completing the training process, the BP network will used to test samples. The form of test samples is the same as training samples. But the input is needed only and the BP network will give the output.

3.2 Elman network for situation prediction

Elman network was first proposed by Jeffrey L. Elman in 1990[24]. It is a kind of feedback neural network with strong computing power. Generally, Elman network is composed of input layer, hidden layer, undertake layer and output layer. The neurons in the undertake layer remember the previous output of the neurons in the hidden layer by receiving the feedback signal from the hidden layer neurons. And then the output of the undertake layer neurons will be input to the hidden layer after delay and storage. This method makes Elman network become sensitive to the historical data and increases its ability to deal with dynamic information. Figure 2 displays the Elman network architecture of situation prediction proposed in this paper.

The Elman network has one more layer called the undertake layer than the BP network, so the output of Elman network will consider the output of undertaker layer.

$$x_u(t) = x(t-1) + a * x_u(t-1) \tag{4}$$

$$h(t) = f(w^{IH} x(t-1) + w^{UI} x_u(t)) \tag{5}$$

$$y(t) = g(w^{HO} h(t)) \tag{6}$$

where $x_u(t)$ represents the output of undertake layer for time t, $a(0 \leqslant a \leqslant 1)$ is the connection feedback factor of undertake layer. $h(t)$ denotes the output of hidden layer and $y(t)$ denotes the output of Elman network. w^{IH} expresses the weight matrix between the input layer and hidden layer, w^{UI} expresses the weight matrix between

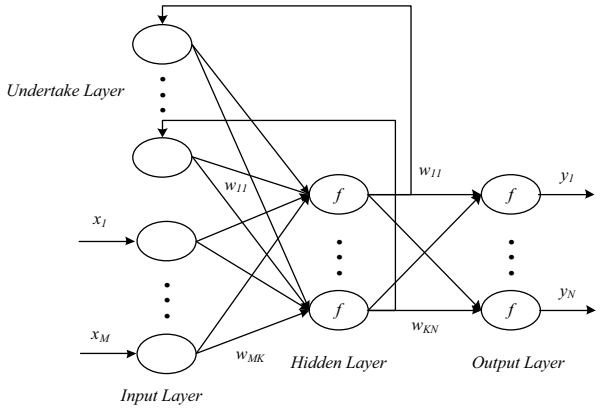

Figure 2. Elman neural network architecture of situation prediction.

the undertake layer and input layer, and w^{HO} expresses the weight matrix between the hidden layer and output layer. In this paper, we adopt sigmoid as function f and linear function as function g.

The training and test processes of Elman network is the same with that of BP network.

3.3 RBF network for situation prediction

An effective feed-forward neural network called Radial Basis Function (RBF) neural network, which has fine approximation performance and generalization ability[18]. As shown in Fig. 3, the RBF network consists three layers, namely, input layer, hidden layer and output layer. Neurons in the input layer are only responsible for transferring the input signal to the hidden layer. With the radial basis function as transfer function, the hidden layer space is constituted by mapping the input vector directly to the hidden space. While the output layer usually adopts a simple linear function.

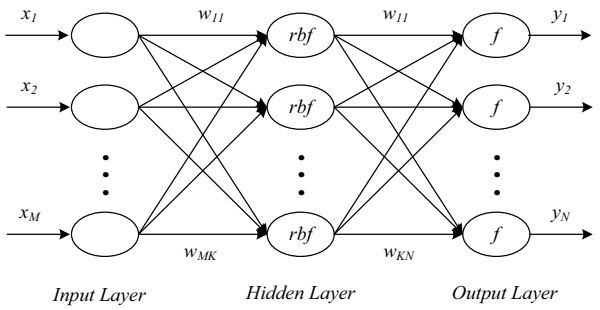

Figure 3. RBF neural network architecture of situation prediction.

The structure of RBF network is similar to that of BP network. As shown in Fig. 3, the function in the hidden layer of RBF network is radial basis function. And the training and test process is the same with BP network.

3.4 Neural network combination model for situation prediction

The combination model of neural network is composed of BP network, Elman network and RBF network as shown in Fig. 4. The past M network security situation values are taken as the input of the model. Firstly, the BP network model, the Elman network model and the RBF network model will deal with the input respectively. And then each model gives a predicted output. With the method of weighted geometric average, the combination model integrates the predicted output of three kinds of neural network described above as final output, as shown in Eq. (7).

$$SV_{com} = \beta_1 * SV_{bp} + \beta_2 * SV_{elman} + \beta_3 * SV_{rbf} \tag{7}$$

where SV_{com} represents the output of the combination model, and SV_{bp}, SV_{elman}, SV_{rbf} represent the output of BP network, Elman network and RBF network respectively, and, $\beta_i (i = 1, 2, 3)$ represent the weights of every neural network.

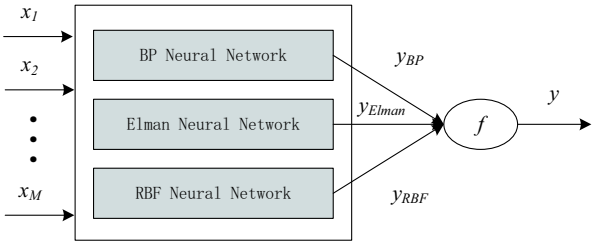

Figure 4. Neural network Combination model of situation prediction.

In this paper, a method based on entropy is used to determine $\beta_i (i = 1, 2, 3)$ described above. Firstly, this method normalizes the relative error er_{ij} of each single prediction model as shown in Eq. (8).

$$er_{ij} = \frac{e_{ij}}{\sum_{j=1}^{N} e_{ij}} (i = 1, 2, \ldots, m\,; j = 1, 2, \ldots, N) \tag{8}$$

where e_{ij} represents the prediction error of single prediction model, i represents which prediction model, such as $i = 1$ means the BP neural network prediction model, and m represents kinds of single prediction model.

Secondly, this method calculates the entropy h_i of each kinds of prediction model.

$$h_i = \sum_{j=1}^{N} er_{ij} \ln \frac{1}{er_{ij}} (i = 1, 2, \ldots, m\,; j = 1, 2, \ldots, N) \tag{9}$$

Finally, the weights of each prediction model are made in the following Equation.

$$\beta_i = \frac{1 - h_i}{m - \sum_{i=1}^{m} h_i} (i = 1, 2, \ldots, m) \tag{10}$$

4 Simulation

4.1 Sample data

The data used in this paper was collected by CNSSA[25]. "Based on the fusion of network security, CNSSA makes a quantitative assessment on the situations of network security"[26]. It outputs a value representing the current security status of the network called network security situation value. The output value is a real number varying from 0 to 10. The larger the value, the more insecure the network. The security states have four levels including log level, low level, middle level and high level. For example, when the value is between 0 and 2.5, the security status of network is in log level.

The data was collected by CNSSA during May 13th, 2011 to May 18th, 2011 with an interval of 5 minutes. During May 17th, 2011 to May 18th, 2011, the following attacks were simulated.

(1) Probe Attack. An attacker resident on the host 10.0.49.1 used Nmap[26] to perform probe attack to subnet 10.0.200.1-50, from 10:38 AM to 10:41 AM, May 13th, 2011.

(2) Simultaneous complex attacks including portscan, smurf and teardrop attacks, from 15:13 AM, on the date of 2011-5-17 to 9:17 AM, on the date of 2011-5-18. Three attacks were launched simultaneously. Specifically, one attacker resident on the host 10.0.49.1 launched a port scan to the subnet 10.0.0.0/16 from 15:13 AM on the date of 2011-5-17 to 9:17 AM on the date of 2011-5-18; one attacker resident on the host 10.0.49.1launched smurf attack to hosts with IPs from 10.0.0.0 to 10.255.255.255 from 15:13 AM to 9:38 PM on the date of 2011-5-17; and one attacker resident on the host 10.0.49.1 launched teardrop attack to host 10.0.49.2 from 15:13 AM on the date of 2011-5-17 to 9:17 AM on the date of 2011-5-18.

4.2 Performance index

In order to evaluate the performance of the proposed model, we used the Mean-Square Error (MSE) in the comparison. MSE is the mean of the square sum between the actual output and the predicted output. The definition of MSE is denoted as follows:

$$MSE = \frac{\sum_{i=1}^{N} (y_i - P_i)^2}{N} \tag{11}$$

where $i = 1, 2, \ldots, N$, y_i and P_i denotes the actual and the predicted outputs separately.

4.3 Parameter

In this paper, 300 sets of data in description of section 4.1 were used to train the neural network model. In the experiment, M was set to be 3 because the future situation to be predicted is greatly influenced by the situation closer to it in time accordance with the practice. After training, we get the weighs of three kinds of prediction model.

$$SV_{com} = 0.3135 * SV_{bp} + 0.5019 * SV_{elman} + 0.1846 * SV_{rbf} \tag{12}$$

4.4 Results

We use matlab to implement our experiments. In this paper, 300 sets of data in description of section 4.1 were used to train the neural network model. 27, 22, and 37 sets of data were used to test the effect of the neural network combination model described in Section III respectively. Then a comparison between the results of prediction with this method and each single neural network model was described in detail.

NN combination model proposed in this paper integrates BP network, Elman network with RBF network. Its prediction results are shown in figure 5. In figure 5, the horizontal axis shows the number of the test data, and the vertical axis represents the network security situation value. This picture shows the testing curve of four prediction methods including the combination model and each single neural network model. Figure 6 shows the mean square error of four prediction methods. In this figure, the combination model gets minimum mean square error in the four methods. Figure 5 and figure 6 illustrate that the method of combination model performs better in predicting network security situation.

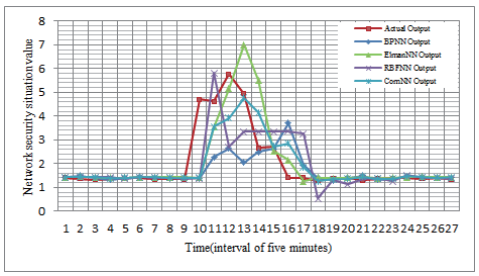

Figure 5. Testing curve of four prediction methods

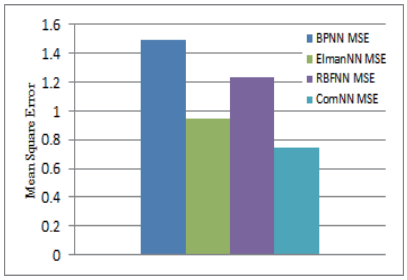

Figure 6. MSE curve of four prediction methods

We do another two experiments showing the same idea. In Fig. 7 and Fig. 8, the test data were 22 sets. In Fig. 10 and Fig. 11, the test data used in the experiment were 37 sets. Figure 7 and Fig. 9 show the testing curve of the four methods. Figure 8 and Fig. 10 show the mean square error of the four methods. We can see that the combination model gets minimum mean square error from Fig. 8 and Fig. 10, shown as Fig. 6.

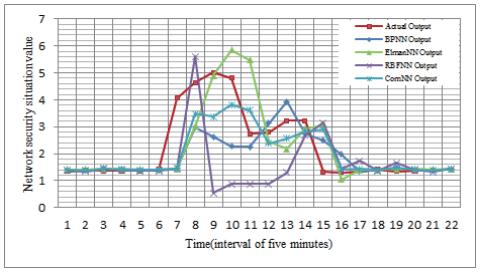

Figure 7. Testing curve of four prediction methods

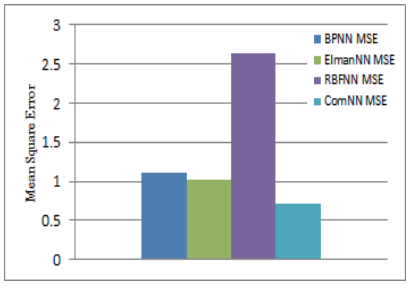

Figure 8. MSE curve of four prediction methods

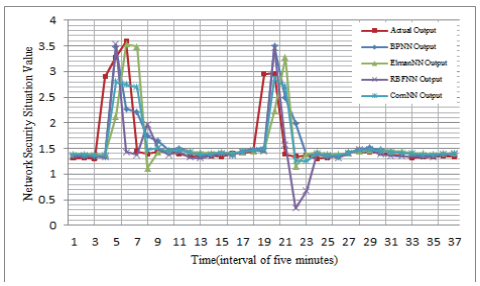

Figure 9. Testing curve of four prediction methods

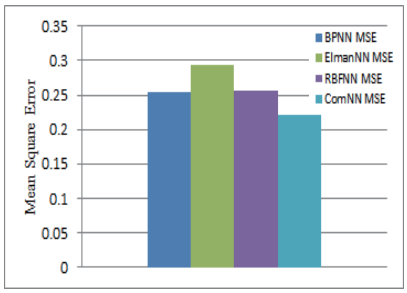

Figure 10. MSE curve of four prediction methods

5 Conclusions and Future Work

The technology for predicting the situation of network security can reflect the global security situation of the network and predict the trend of the situation. This method not only provides network managers a better understanding of the network security situation, but also helps them to make decisions quickly and to protect networks in the network environment effectively. In this paper, we presented a method based on the combination of multiple commonly used neural networks, including BP neural network, Elman neural network and RBF neural network, which integrates the advantages of individual neural networks. Experimental results showed that the proposed model can more accurately predict the situation of network security than the ones with only single neural network. However, there are still many research issues regarding network security situation prediction that remain unsolved. Therefore, in the future we will improve the effect of the combination model, including the weights determining of the three kinds of neural networks in the combination model.

References

[1] Kristjanpoller W, Fadic A, Minutolo MC. Volatility forecast using hybrid neural network models. Expert Systems with Applications, 2014, 41(5): 2437–2442.

[2] Xuan Z. Survey of Network Security Situation Awareness and Key Technologies. Frontier and Future Development of Information Technology in Medicine and Education. Springer Netherlands, 2014: 3281–3286.

[3] Zhang Y, Jin S, Cui X, et al. Network security situation prediction based on BP and RBF neural network. Trustworthy Computing and Services. Springer Berlin Heidelberg, 2013: 659–665.

[4] Wei X, Jiang X. Comprehensive analysis of network security situational awareness methods and models. 2013 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation (IMSNA). IEEE. 2013. 176–179.

[5] Kemmerer RA, Büchkes R, Fessi A, König H, Herrmann P, Wolthusen SD, Jahnke M, Debar H, Holz R, Zseby T, Haage D. Outcome working group – situational awareness. Network Attack Detection and Defense, 2008, 08102.

[6] Wei Y, Lian YF. A network security situational awareness model based on log audit and performance correction, Chinese Journal of Computers, 2009, 32: 763–772.

[7] Xu B. Network Security Situation Prediction[Degree Thesis]. Dalian, China: Dalian University of Technology, 2008, 1: 6–8.

[8] Ren W, Jiang XH, Sun TFg. The prediction method of network security situation based on RBF neural network. Computer Engineering and Applications, 2006, 31: 136–144.

[9] Xia WW, Wang HF. Prediction model of network security situational based on regression

analysis. 2010 IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS). 2010.

[10] Bass T. Intrusion detection systems &multisensor data fusion: Creating cyberspace situational awareness. Communications of the ACM, 2000, 43(4): 99210.

[11] Lakkaraju K, Yurcik W, Lee AJ. NVisionIP: netflow visualizations of system state for security situational assessment. Proc. of the 2004 ACM workshop on Visualization and Data Mining for Computer Security. 2004.

[12] Yin XX, Yurcik W, Slagell A. The design of VisFlowConnect-IP: A link analysis system for IP security situational assessment. Proc of the 3rd IEEE International Workshop on Information Assurance (IWIA'05). 2005.

[13] Shimeall T, Faber S, DeShon M, Kompanek A. Analysts' handbook: Using SiLK for network traffic analysis. Silk Documentation, 2009.

[14] Wang LY, Liu AY,Jajodia S. Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts. Computer Communications, 2006, 29(15): 2917–2933.

[15] Xu HB, Dai YX, Ping HF, et al. A detection and forecast algorithm for multi-step attackBased on intrusion Intention. Journal of Software, 2005, 16(12): 2132–2138.

[16] Zhang GL, Sun JZ. A novel network intrusion attempts prediction model based on fuzzy neural network. The 6th International Conference in Artificial Intelligence and Lecture Notes in Bioinformatics. LNCS-1. 2006. 3991. 419–426.

[17] Wang H, Lai J, Liu X, et al. A quantitative forecast method of network security situation based on BP neural network with genetic algorithm. Second International Multi-Symposiums on Computer and Computational Sciences(IMSCCS 2007). IEEE. 2007. 374–380.

[18] Tang CH, Xie Y, Qiang BH, Wang X, Zhang RX. Security situation prediction based on dynamic BP neural with covariance. Advanced in Control Engineering and Information Science, 2011.

[19] Meng J, Ma C, He JL, Zhang H. Network security situation prediction model based on HHGA-RBF neural network. Computer Science, 2011, 38: 70.

[20] You MY, Ling J, Hao YJ. Prediction method for network security situation based on elman neural network. Computer Science, 2012, 39(6).

[21] Jibao L, Huiqiang W, Xiaowu L, et al. A quantitative prediction method of network security situation based on wavelet neural network. The First International Symposium on Data, Privacy, and E-Commerce(ISDPE 2007). IEEE. 2007. 197–202.

[22] Haykin S. Neural Networks, a Comprehensive Foundation, Second Edition. Prentice Hall, 1998: 161∼175, 183∼221, 400∼438.

[23] Sadeghi BHM. A BP-neural network predictor model for plastic injection molding process. Journal of Materials Processing Technology, 2000, 103(3): 411–416.

[24] Elman JL. Finding structure in time. Cognitive Science, 1990, 14(2): 179–211.

[25] Xi R, Jin S, Yun X, et al. CNSSA: A comprehensive network security situation awareness system. 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE. 2011. 482–487.

[26] Salkind NJ. Encyclopedia of research design. Independence, 2002, 10(47).