CHEMICAL ENGINEERING TRANSACTIONS
VOL. 46, 2015

A publication of
AIDIC
The Italian Association
of Chemical Engineering
Online at www.aidic.it/cet

Guest Editors: Peiyu Ren, Yancang Li, Huiping Song
Copyright © 2015, AIDIC Servizi S.r.l.,
ISBN 978-88-95608-37-2; **ISSN** 2283-9216
DOI: 10.3303/CET1546211

Application of an Improved BP Neural Network Model in Enterprise Network Security Forecasting

Xun Chen*[a, b], Lisheng Xu[a], Meng Xu[a]

[a] College of Geology and Environment Central South University, Changsha 410083, China;
[b] Changsha Aeronautical Vocational and Technical College, Changsha 410124, China
sky1125baby@163.com

In recent years, with the rise of the global network, the Internet technology as the core of large enterprise network system is developing rapidly. It is widely used in the field of electronic commerce, information service, network communication and other technical means. At the same time, the problem of network security has become increasingly prominent. Due to historical and technical reasons, the security system of enterprise network is still very weak in China. The network basic software and hardware is still use a large number of foreign products, and the core of the network security technology cannot be fully mastered. So, the security risks are obvious. Therefore, strengthening the construction of enterprise network security system and researching the safe application model has become the top priority of our country's enterprise information technology. Based on this, we propose a smoothing method to improve the initial weights and the initial threshold, and use a test method to select the hidden layer node number of neural network. So, we can minimize the fitting error of the training. In this paper, the computer network security data of an enterprise is selected, and all the indexes are scored by the experts. The result of the scoring is the input value of the improved BP neural network. Finally, we use this algorithm to predict the network security of a certain enterprise in the next three months. The score is 0.85, 0.88 and 0.91, which is close to the actual value of network security.

1. Introduction

In recent years, with the rise of the global network, the Internet technology as the core of large enterprise network system is developing rapidly. It is widely used in the field of electronic commerce, information service, network communication and other technical means. At the same time, the problem of network security has become increasingly prominent. Due to historical and technical reasons, the security system of enterprise network is still very weak in China. The network basic software and hardware is still use a large number of foreign products, and the core of the network security technology can not be fully mastered. So, the security risks are obvious. Therefore, strengthening the construction of enterprise network security system and researching the safe application model has become the top priority of our country's enterprise information technology. Network security risk prediction is an important component of network security awareness (China Internet Network Information Center 2012 and 2013). At present, the most common methods of prediction are as follows.

Grey theory method. In recent years, the application of gray theory has been extended to many scientific fields, such as environment, climate, health, medical care, population and so on. In the area of network security, there are many research results ((Deng Julong (2002), Wang Caiyin (2013), Pu Tianyin (2009), and Zheng Jieliang (2005)). The theory uses the sequences which are generated by the original sequence of the system to determine the best fitting curve, and it can effectively deal with the less data sample system. Time series method. Time series forecasting method reveals the rule of the phenomenon with time variation, and this rule is extended to the future, so as to realize the prediction of the phenomenon in the future (Yang Zhongjin (2006), Guo Mingyue (2009), Chang Taihua (2010), and Zhang Jinghui (2012)). Neural network method. Neural network is a kind of method to simulate human's cognitive process, which is a kind of nonlinear dynamic system of information distributed storage and parallel processing. Its essence is a kind of

Please cite this article as: Chen X., Xu L.S., Xu M., 2015, Application of an improved bp neural network model in enterprise network security forecasting, Chemical Engineering Transactions, 46, 1261-1266 DOI:10.3303/CET1546211 nonlinear function that represents the relationship between the input value and the output value. Forecasting methods based on neural networks have many advantages, such as good nonlinear, distributed and self-organizing learning. It has good practical value in multi variable forecasting and nonlinear forecasting. But the neural network is a black box forecasting method, which can only be used to fit the system's input and output data. Therefore, the relationship between input value and the output value is not clearly described, and the results cannot be explained reasonably (Tang Chenghua (2009), Xie Lixia, Cai (2013) Zhiping (2008) and Xu Fuyong (2005)).

Based on this, we propose a smoothing method to improve the initial weights and the initial threshold, and use a test method to select the hidden layer node number of neural network. So, we can minimize the fitting error of the training. In this paper, the computer network security data of an enterprise is selected, and all the indexes are scored by the experts. The result of the scoring is the input value of the improved BP neural network. Finally, we use this algorithm to predict the network security of a certain enterprise in the next three months.

2. Neural network model

BP algorithm not only has the input layer node, the output layer node, but also has one or more hidden layer nodes. Firstly, the input signal is propagated forward to the hidden layer node. After the function of the excitation function, the output signal of the hidden layer node is transmitted to the output layer node. Finally,we get the output results. The S type function is usually selected as the node's excitation function, which is shown below;

$$f(x)=\frac{1}{1+e^{-x/Q}} \tag{1}$$

Here, Q is the Sigmoid parameter, which is primarily responsible for the form of the excitation function. The learning process of the algorithm is composed of forward propagation and backward propagation. In the process of forward propagation, the input information is processed by the hidden layer and the information is transmitted to the output layer. Each layer of neurons only affects the state of the neurons in the next layer. If the output layer cannot get the expected output value, the algorithm is transferred to the process of the back propagation. In this process, the error signal is returned along the original path. By modifying the weights of each layer, the system error can be minimized.

Set up any network containing n nodes, the characteristics of each node are Sigmoid type. For simplicity, the network has only one output value which is y. The output value of i th node is O_i. The number of sample is N, $(k=1,2,\cdots,N)$. For a node, the input value is x_k and the output value is y_k, the output value of i th node O_{ik}, and the input of the j th node is:

$$net_{ik}=\sum_i W_{ij}O_{jk} \tag{2}$$

We define the error function as:

$$E=\frac{1}{2}\sum_{k=1}^{N}(y_k-\hat{y}_k)^2 \tag{3}$$

Where, $\hat{y}_k$ is the actual output value of the network.

Define $E_k=(y_k-\hat{y}_k)^2$, $\delta_{ik}=\frac{\partial E_k}{\partial net_{jk}}$ and $O_{jk}=f(net_{jk})$.

Therefore,

$$\frac{\partial E_k}{\partial W_{ij}}=\frac{\partial E_k}{\partial net_{jk}}\bullet\frac{\partial net_{jk}}{\partial W_{ij}}=\frac{\partial E_k}{\partial net_{jk}}O_{jk}=\delta_{jk}O_{ik} \tag{4}$$

When j is the output node, $O_{jk}=\hat{y}_k$

$$\delta_{jk} = \frac{\partial E_k}{\partial \hat{y}_k} \bullet \frac{\partial \hat{y}_k}{\partial net_{jk}} = -(y_k - \hat{y}_k) f^{'}(\partial net_{jk}) \tag{5}$$

When j is not the output node,

$$\delta_{jk} = \frac{\partial E_k}{\partial net_{jk}} = \frac{\partial E_k}{\partial O_{jk}} \bullet \frac{\partial O_{jk}}{\partial net_{jk}} = \frac{\partial E_k}{\partial O_{jk}} f^{'}(\partial net_{jk}) \tag{6}$$

$$\frac{\partial E_k}{\partial O_{jk}} = \sum_m \frac{\partial E_k}{\partial net_{mk}} \bullet \frac{\partial net_{mk}}{\partial O_{jk}} = \sum_m \frac{\partial E_k}{\partial net_{mk}} \bullet \frac{\partial}{\partial O_{jk}} \sum_i W_{mi} O_{ik} = \sum_m \frac{\partial E_k}{\partial net_{mk}} \sum_i W_{mj} = \sum_m \delta_{mk} W_{mj} \tag{7}$$

Therefore,

$$\begin{cases} \delta_{jk} = f^{'}(net_{jk}) \sum\limits_m \delta_{mk} W_{mj} \\ \dfrac{\partial E_k}{\partial W_{ij}} = \delta_{mk} O_{ik} \end{cases} \tag{8}$$

3. Improvement of BP network

The setting of the initial weight and the threshold of the memory. One of the main problems of the BP neural network model is the slow convergence speed and the length of the iteration time. Through a large number of practical applications, the initial weights and thresholds of BP neural network can be randomly selected, the convergence speed of BP neural network is greatly affected by the method. Some scholars put forward the corresponding initial weights and threshold selection method, and they have achieved some results in the field of their research. On this basis, this article proposes a new method of the initial smooth weight and threshold of memory. Methods are as follows:

$$\begin{cases} w_1^0(\bullet) = Rnd(\bullet) \\ \theta_1^0(\bullet) = Rnd(\bullet) \end{cases} \tag{9}$$

$$\begin{cases} w_2^0(\bullet) = Rnd(\bullet) \\ \theta_2^0(\bullet) = Rnd(\bullet) \end{cases} \tag{10}$$

$$\begin{cases} w_i^0(\bullet) = \dfrac{w_{i-1}^0(\bullet) + w_{i-2}^0(\bullet)}{2} \\ \theta_i^0(\bullet) = \dfrac{\theta_{i-1}^0(\bullet) + \theta_{i-2}^0(\bullet)}{2} \end{cases} \quad i = 3, 4, \cdots, N \tag{11}$$

Where, The initial weights for the i th BP network operation is w_i^0, the threshold for the i th BP network operation is θ_i^0, the termination weights for the $i-1$ th BP network operation is w_{i-1}^0, and the termination threshold for the $i-1$ th BP network operation is θ_{i-1}^0.

4. Simulation experiment and result analysis

4.1 Network security evaluation index system

Network and information system is a complex system engineering, which includes the external factors and the internal factors, and they are mutually restricted. Therefore, we must have a standard, unified, objective criteria to measure network security. According to the domestic and foreign network security evaluation standard, and the basic requirements of the network and information system security, we should fully consider the various factors that affecting the security of the network, such as physical security factor, operation safety factor, information security factors, system security policy and safety technical measures. Therefore, we give the network security evaluation index system. As shown in table 1:

Table 1: The network security evaluation index system

First level index	Second level index	safety index	Variable
network security	physical security	Equipment safety	X_1
		Environmental safety	X_2
		Media security	X_3
	operation safety	Risk analysis	X_4
		Access control measures	X_5
		Audit measures	X_6
		Emergency technology	X_7
	information security	Information transmission security	X_8
		Defense Technology	X_9
		Data integrity	X_{10}
		Data encryption	X_{11}
	system security policy	Application software	X_{12}
		User identity authentication	X_{13}
		Data remote backup	X_{14}
	safety technical measures	Security audit function	X_{15}
		Anti hacking measures	X_{16}

4.2 Data pre-processing of network security index

Table 1 reflects the security of computer networks from different angles. As the dimensions of the various indicators are different, so we cannot make a direct comparison. In order to make the index have comparability, and to speed up the convergence rate of the neural network, this paper has carried on the normalized processing to each index:

1) for qualitative indicators: using expert scoring method to determine its data, and we have a normalized treatment of various indicators.

2) for quantitative indicators: the following formula is used to normalize.

$$x_i = \frac{x_i - x_{i\min}}{x_{i\max} - x_{\min}} \tag{12}$$

Where, the normalized values for the i th indicator is x_i, the minimum value of the i th indicator is $x_{i\min}$, and the maximum value of the i th indicator is $x_{i\max}$.

4.3 Simulation experiment

In this paper, the computer network security data of an enterprise is selected, and all the indexes are scored by the experts. The result of the scoring is the input value of the improved BP neural network. As the neural network model of this paper is a 16-X-1 model, we carry out the training of the sample according to principle. The principle is that the number of nodes in the hidden layer is 3/4 of the number of nodes in the input layer. We try to set the number of nodes in the hidden layer to 11,12 and 13. From the results of training, it can be known that the number of hidden layer nodes is X=12, and the system fitting residual is the smallest.

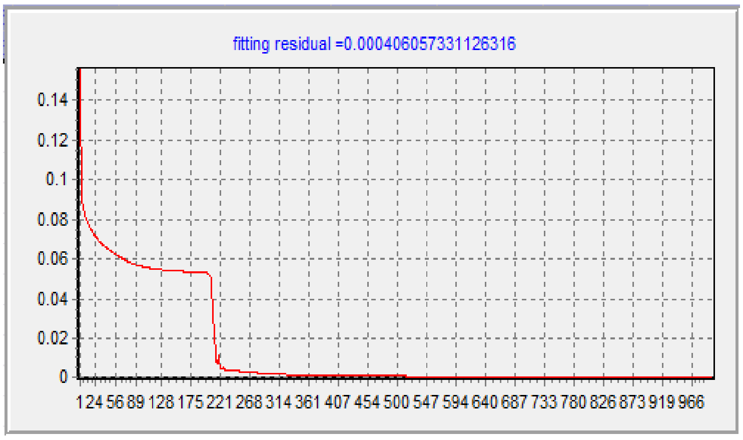

Figure 1: The number of hidden layer nodes is 11 in neural network training

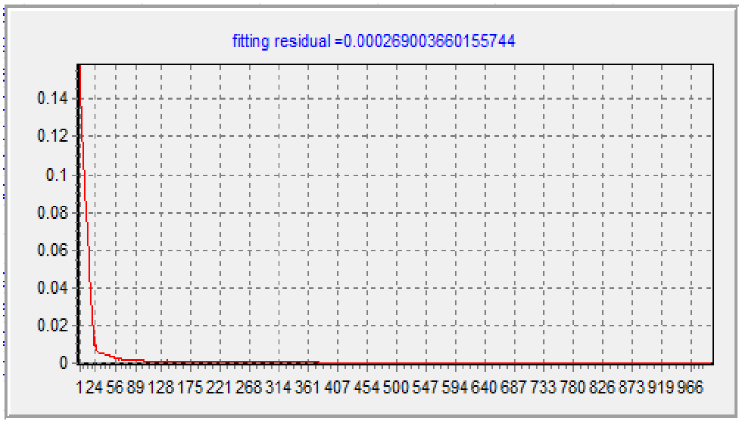

Figure 2: The number of hidden layer nodes is 12 in neural network training

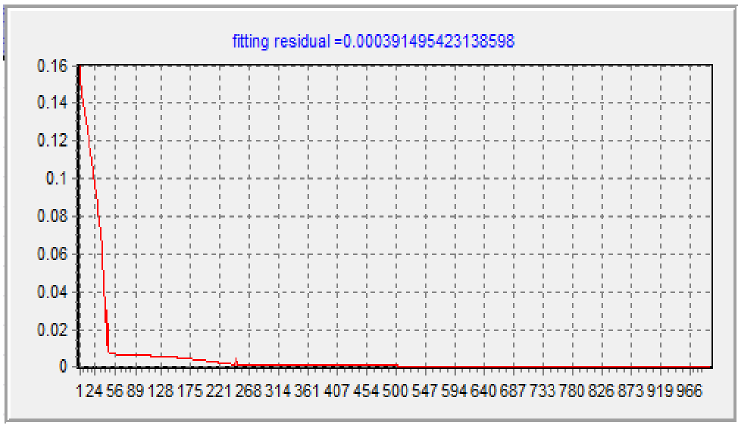

Figure 3: The number of hidden layer nodes is 13 in neural network training

It can be seen from the test results of figure 1-3, the node number and the initial value in this paper can effectively shorten the convergence period, accelerate the training speed, and make the fitting precision of the residual error reach the highest. Finally, we use this algorithm to predict the network security of a certain enterprise in the next three months, the score is 0.85, 0.88 and 0.91, which is close to the actual value of network security.

5. Conclusions

In this article, we propose a smoothing method to improve the initial weights and the initial threshold, and use a test method to select the hidden layer node number of neural network. So, we can minimize the fitting error of the training. In addition, the computer network security data of an enterprise is selected, and all the indexes are scored by the experts. The result of the scoring is the input value of the improved BP neural network.

References

Cai Z.P., Liu F., 2008, Security risk probability forecasting model based on neural network [J].Computer science, 35 (12): 28-33.

Chang T.H., Xu R.Z., Lv G.J., 2010, Study on the method of network security situation prediction based on time series [J]. Practice and cognition of mathematics, 40 (12): 124-133.

China Internet Network Information Center. 2013. Statistical report on Internet development in China. 2013.

China Internet Network Information Center. 2012. Statistical report on Internet development in China. 2012.

Deng J.L., 2002, Gray Theory [M]. Wuhan: Huazhong University of Science & Technology Press Co., Ltd.

Guo M.Y., Xiao Z.H., 2009, Time series analysis and SAS application [M]. Wuhan: Wuhan University press.

Institute C S. 2010/2011 CSI Computer Crime and Security Survey, http://gocsi.com/survey.

National Internet Emergency Center. 2011 China Internet Network Security Report. http://www.cert.org.cn/publish/main/46/2012/20120523085533341215471/20120523085533341215471_.html.

Pu T.Y., 2009, Probe on the Network Security Situational Awareness Model Based on the Gray Theory [D]. Changsha: Hunan University.

Tang C.H., Yu S.Z., 2009, Method of Network Security Situation Prediction Based on Likelihood BP [J]. Computer Science, 36(11): 97-101.

Wang C.Y., 2013, Assessment of Network Security Situation Based on Grey Relational Analysis and Support Vector Machine [J]. Application Research of Computer, 30(6): 1859-1862.

Xie L.X., Wang Y.C., Yu J.B., 2013, Network Security Situation Awareness Based on Neural Network [J]. Journal of Tsinghua University: Science and Technology, 53(12): 1750-1760.

Xu F.Y., Shen J., Li J.Y., 2015, based on Delphi and ANN network security comprehensive evaluation method research [J]. Microcomputer development, 15 (10): 11-15.

Yang Z.J., 2006, Analysis and prediction of time series [J]. China Science and technology information, (14): 267-268.

Zhang J.H., Wang G., Wu N., 2012, Application of network security situation prediction method [J]. Computer simulation, 29 (2): 98-101.

Zheng J.L., 2005, Research on network information security assessment model based on Grey Theory [D]. Nanjing University of Information Science and Technology, 2005 (5): 39-44.