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

ISBN 978-88-95608-37-2; **ISSN** 2283-9216
DOI: 10.3303/CET1546205

Application of Grey Neural Network Forecasting Model Based on Background Value Improvement in Enterprise Network Security Evaluation

Limin Zhao*, Peng Yue

College of Management, Xinxiang Medical University, Xinxiang, Henan, 453002, China.
zhaoxxmu@163.com

Network security is related to the proper protection of the network system hardware, software, and the data in the system. They are not subjected to accidental or malicious destruction, alteration and disclosure to make the system run continuously and reliably. Then, the network service is not interrupted. As we all know, BP neural network is used more fully in the network security. It has a strong nonlinear approximation ability, the algorithm is simple and easy to implement, but it is easy to fall into local extreme value, which is difficult to ensure that the algorithm converges to the global minimum point, and the global search ability is not strong. Based on this, this paper makes an improvement on the background value of grey model, and uses the output value of the gray model to establish the neural network forecasting model. In addition, this paper presents a decision method of the importance degree of the enterprise network security evaluation index which is based on BP neural network. The main feature of this method is that the evaluation index is extracted directly from the network connection weights. Finally, this article proves that the grey neural forecasting model based on background value improvement can be used to evaluate the development trend of enterprise network security more accurately.

1. Introduction

Network security is related to the proper protection of the network system hardware, software, the data in the system. They are not subjected to accidental or malicious destruction, alteration and disclosure. So as to make the system run continuously and reliably. Then, the network service is not interrupted. Because the network has the characteristics of connectivity, users enjoy the convenience of the network. At the same time, their information resources will be exposed. Due to the network information related to the national government, military, cultural and educational fields, so much of the information stored in the network is classified. If this information is violated, it will bring immeasurable loss to the country's political and economic. Therefore, our research on network security is especially important (Zhang Jun, Luo Baoqing (2010), Zhao, Qiu Xiaofeng (2010), and Zhang Yunyong, Chen Qingjin (2010)).

Domestic and foreign scholars pay much attention to the study of computer network security. The agent theory is a frontier theory of computer science and artificial intelligence. Using Agent technology, many scholars had proposed many models or some basic application system in the network security. The scholars had carried out a lot of research, such as virus detection (Jieh-Sheng Lee, Jieh Hsiang (1997)), intrusion detection (Balasubramaniyan, J.S.et al (1998), Crosbie M, Spaford E H (1995), and Jai S B., Jose O., Isacof D, et al (1998)), log audit (Ling-yu Chou, Timon Du (2007)), and security management and monitoring (Michalas, A., Kotsilieris, T., Kalogeropoulos, S., et al (2001), Satoh, I (2002)). They were based on the basic features of Agent to build their own network security system. More importantly, artificial neural network model can effectively overcome the defect of the traditional statistical model. By adjusting the weights of the connections between neurons, they can capture the nonlinear rules between the computer network security and the attributes, so as to realize the accurate evaluation of the computer network security (Gong Hui, Feng Xin (2010), Wang Gang, Zhang Zhiyu (2006), and Kaufmann K W (2010)). Ren Wei (2006) proposed a method based on RBF neural network to carry out the situation prediction. He used the neural network to deal with the

Please cite this article as: Zhao L.M., Yue P., 2015, Application of grey neural network forecasting model based on background value improvement in enterprise network security evaluation, Chemical Engineering Transactions, 46, 1225-1230 DOI:10.3303/CET1546205

chaos and nonlinear data, so as to solve the problem of network security situation prediction. In order to improve the precision of computer network security evaluation, Wu Renjie (2011) proposed a particle swarm optimization neural network model for the evaluation of computer network security.
To sum up, this paper makes an improvement on the background value of grey model, and uses the output value of the gray model to establish the neural network forecasting model. Moreover, this paper presents a decision method of the importance degree of the enterprise network security evaluation index which is based on BP neural network. The main feature of this method is that the evaluation index is extracted directly from the network connection weights. Finally, this article proves that the grey neural forecasting model based on background value improvement can be used to evaluate the development trend of enterprise network security more accurately.

2. Related concepts

2.1 Gray model

GM (1, 1) model is the most commonly used in gray modeling. First of all, it makes an accumulation of the original data sequence X_i^0. After the accumulation, the data has a certain exponential growth trend. Then, we get the sequence X_i^1. The specific method is shown as follows:

$$x^{(1)}(k)=\sum_{i=1}^{k}x^{(0)}(i) \tag{1}$$

Let the background value series be

$$z^{(1)}(k)=\frac{1}{2}[x^{(1)}(k-1)+x^{(1)}(k)],\ k=2,3,\cdots,n \tag{2}$$

The grey differential equation is constructed with $x^{(1)}$ by formula (1).

$$\frac{dx^{(1)}}{dt}+ax^{(1)}=u \tag{3}$$

Which a is called development coefficient. u is called grey action variable.
The discrete form of formula (3) is

$$x^{(0)}(k)+az^{(1)}(k)=u \tag{4}$$

Put parameters into grey differential equation (4), the solution is

$$x^{(1)}(t)=[x^{(1)}(1)-\frac{\hat{u}}{\hat{a}}]e^{-\hat{a}t}+\frac{\hat{u}}{\hat{a}} \tag{5}$$

In the end, we get the recursive formula of the gray prediction model.

$$\hat{x}^{(0)}(k+1)=\hat{x}^{(1)}(k+1)-\hat{x}^{(1)}(k)=(1-e^{\hat{a}})(x^{(0)}(1)-\frac{\hat{u}}{\hat{a}})e^{-\hat{a}k},\ k=1,2,\cdots \tag{6}$$

2.2 Neural network model

BP neural network is a mature model of artificial neural network technology. It is a multilayer feed forward neural network, which is composed of input layer, hidden layer and output layer, It has the ability to learn from the back propagation, and its mathematical expression is:

$$y=\sum_{j=1}^{l}f(\sum_{i=1}^{n}\omega_{ij}x_i-a_j)\omega_j-b \tag{7}$$

Where, y is the Output value of BP neural network, $x_i(i=1,2,\cdots,n)$ are input values, ω_{ij} represents the connection weights of the input layer and the hidden layer, ω_j represents the connection weights between the hidden layer and the output layer, f is a function of the implicit layer, a_j is the threshold of j th neural node for the hidden layer, and b is the threshold for the output layer.

2.3 The excitation function

The excitation function is the input-output relationship between the neurons in the neural network. So, the type of the excitation function determines the characteristics of the neuron. It has been proved that the three layer feed forward neural network can approximate any continuous function with arbitrary precision when the excitation function of neuron satisfies the condition of monotone increasing, bounded and differentiable. The BP algorithm usually uses the sigmoid function as the excitation function. Next, we give several commonly used excitation functions.

(1) Threshold excitation function: $f(x)=\begin{cases}1 & ,x\geq 0\\ 0 & ,x\leq 0\end{cases}$ (8)

(2) Sigmoid excitation function: $f(x)=\frac{1}{1+e^{-x}}$ (9)

(3) Linear excitation function: $f(x)=kx$ (10)

(4) Hyperbolic tangent excitation function: $f(x)=\tan(\frac{x}{T})$ (11)

Below, we give a graph of four excitation functions.

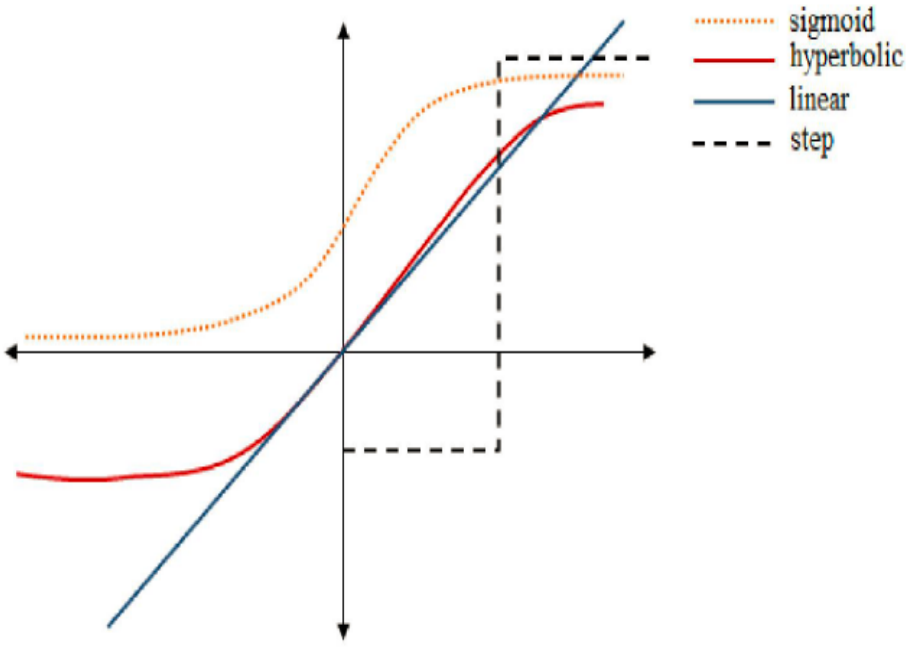

Figure 1: The excitation function

By means of an effective way, gray neural network combined with the gray system and neural network . With the gray model and neural network in series, we can get a gray neural network model of n input values and 1 output value. Its structure is shown in figure 2.

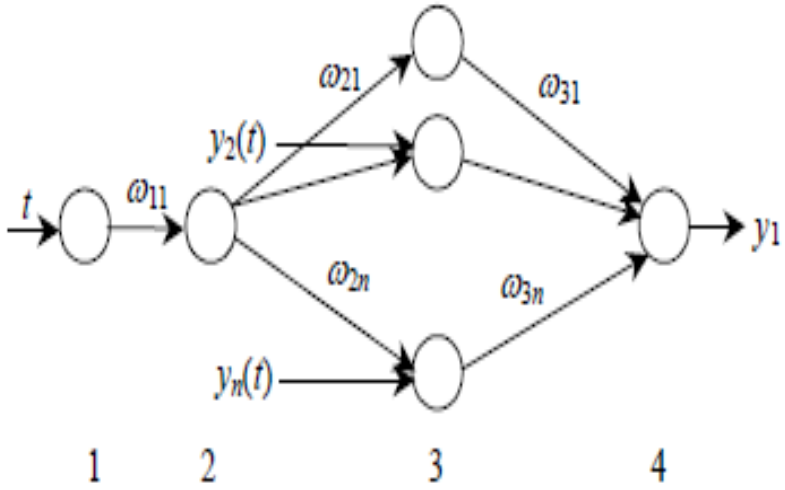

Figure 2: Topology of the grey neural network

3. Improvement of grey mode

The parameters a and u in the formula 3 are the key parameters to ensure the accuracy of the gray model prediction. In the traditional gray model, a and u can be obtained by formula 2 and the least square method. But the curve of Formula 1 is smooth in a very short time interval. Using sequences to estimate parameters is more appropriate. The sequence is generated within 1 second. Otherwise, the generated sequence will make the prediction error, and reduce the prediction accuracy of the model. In order to guarantee the accuracy of the model, we adopt adaptive methods to determine the grey parameters in this paper. According to the function of the S type curve and the existing risk index limit, it can be amended as $x^1(k)=\frac{1}{ce^{dk}}$. When, the $k+1$, $x^1(k+1)=\frac{1}{ce^{d(k+1)}}$.

Simultaneous above two equations, We can get:

$$\begin{cases} c=\dfrac{x^1(k+1)}{\left[x^1(k)\right]^{k+1}} \\ d=\ln\dfrac{x^1(k)}{x^1(k+1)} \end{cases} \tag{12}$$

The, we put the formula (12) into the $z^{(1)}(k)=\frac{1}{2}[x^{(1)}(k-1)+x^{(1)}(k)]$. The formula 2 is modified as follows:

$$z^{(1)}(k+1)=\frac{x^1(k)-x^1(k+1)}{\ln x^1(k)-\ln x^1(k+1)} \tag{13}$$

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, factors of safety technical measures and security system. 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}
	safety technical measures	Anti-virus measures	X_{12}
		System operation log	X_{13}
		Server backup	X_{14}
	security system measures	Organization	X_{15}
		Regulations	X_{16}
		Accident emergency plan	X_{17}

4.2 Setting of computer network security level

According to the comprehensive score of the index, we can evaluate the computer network security. According to the relevant research, the computer network security level is divided into 4 levels. They include that safety (A), basic safety (B), insecurity (C) and extreme insecurity (D). We set the total score of security level to 1, then the corresponding security level and the corresponding score is shown in table 2.

Table 2: Computer network security level

level	A	B	C	D
Score	1-0.85	0.85-0.7	0.7-0.6	0.6-0

4.3 Simulation experiment

In this paper, we select a company's computer network security data as sample data. Then, all the indicators of 36 months has to be marked by the experts. We put the results of the score as the input value of the gray neural network. Through this paper's excitation function, we can output the computer network security score of the enterprise in the next six months. According to figure 2, we can know that the gray neural network model is a 17-5-1 model. Then, we use this algorithm to compare with other methods which are artificial neural network prediction algorithm and gray prediction model. Experimental results show that the prediction results are more close to the expected output value of the enterprise.

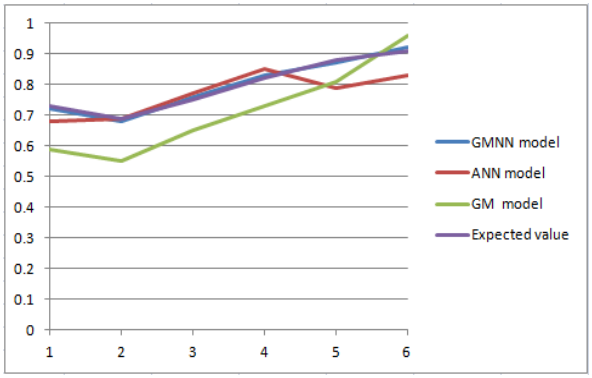

Figure 2: Comparison chart of the assessment result

5. Conclusions

This article makes an improvement on the background value of grey model, and uses the output value of the gray model to establish the neural network forecasting model. In addition, this paper presents a decision method of the importance degree of the enterprise network security evaluation index which is based on BP neural network. The main feature of this method is that the evaluation index is extracted directly from the network connection weights. Finally, this article proves that the grey neural forecasting model based on background value improvement can be used to evaluate the development trend of enterprise network security more accurately.

References

Balasubramaniyan, J.S., Garcia-Fernandez, J.O., Isacoff, D., et al. 1998, Architecture for intrusion detection using autonomous Agents [C]. Proceedings on Computer Security Applications Conference, 12(14): 13-24.

Chou L.Y., Du T., Lai V.S., 2007, Continuous auditing with a multi-Agent system [J]. Source Decision Support Systems, 1, 42(4): 2274-2292.

Crosbie M., Spaford E.H., 1995, defending a computer system using autonomous Agents [C]. Proceedings of the 18th National Information Systems Security Conference, Baltimore, MD, 10: 549-558.

Gong H., Feng X., 2010, Research and Application of a Kind of Rough Fuzzy Neural Network Model [J]. Computer Engineering and Science, 32(6): 132-134.

Jai S.B., Jose O., Isacof D., et al. 1998, An Architecture for Intrusion Detection using Autonomous Agents [J], Purdue University, West Lafayette, Cost TR 98-05.

Kaufmann K.W., Lemmon G.H., De Luca S.L., et al. 2010, Practically Useful What the ROSETTA Protein Modeling Suite Can Do for You [J]. Biochemistry, 49(14): 2987-2998

Lee J.S., Hsiang J., Tsang P.H., 1997, A generic virus detection Agent on the Internet [C]. System Sciences, 1997, Proceedings of the Thirtieth Hawaii International Conference. 4(6): 210 - 219.

Michalas A., Kotsilieris T., Kalogeropoulos S., et al. 2001, Enhancing the performance of mobile Agent based network management applications. Proceedings [C]. The 6th IEEE Symposium on Computers and Communications, 6: 432-437.

Ren W., 2006, RBFNN- based Prediction of Networks Security Situation [J]. Computer engineering and Application, 31:136-139.

Satoh I., 2002, A framework for building reusable mobile Agents for network management [J]. Network Operations and Management Symposium, 6: 51-64.

Wang G., Zhang Z.Y., 2006, Rough Set Method Combined with BP Neural Network Data Fusion [J]. Journal of Xi'an University of Technology, 22(3): 311-314.

Wu R.J., 2011, Application Research of Computer Network Security Evaluation Based on Network Security [J]. Computer simulation, 11: 126-129.

Zhang J., Luo B.Q., 2010, The harm and prevention of computer virus [J]. Economic and technical cooperation information, (20): 1039-1042.

Zhang Y.Y., Chen Q.J., Pan S.B., 2010, Cloud computing security key technologies [J]. Telecommunication science, (8): 11-15.

Zhao Q.X.F., 2010, Cloud computing environment security threats and protection [J]. China Computer Communication Society, 6(5): 47-50.