The Research on Computer Network Security Defense System Based on GABP Neural Network Algorithm

Han Feng

College of Computer Engineering, Shenzhen Polytechnic, Shenzhen, Guangdong Province, China
518055hanfeng@szpt.edu.cn

Abstract. With the rapid development of the network era, the environment of computer network has become more complex, and the problems of network security are increasingly prominent. In this context, how to ensure the security of data information and network system in the open network environment has become a problem need to be discussed and solved by relevant personnel. Therefore, in this paper, a research of the applications of GABP algorithm in the evaluation of computer network security is proposed according to the influence factors of computer network security and combined with the characteristics of GABP neural network algorithm. What's more, the construction scheme of computer network security defense system is fatherly discussed, aiming at improving the security of computer network system.

Keywords: computer network security, defense system, GABP algorithm, network era

1 Introduction

As the network era comes, computer network has been widely used in more and more fields. It has had a profound influence on people's life and work. However, with the continuous development of network technology, network security issues have also begun to emerge, which has seriously affected the development of society and economy and the public order and administration. Some lawbreakers use advanced technology to break into the computer network defense system, resulting in information leakage and serious tampering problems. In this context, how to scientifically evaluate computer network security and establish a complete computer network security defense system has become a problem that should be discussed and solved by relevant personnel.

At present, the major method to evaluate the computer network security is comprehensive evaluation (CE) based on analytic hierarchy process (AHP) [7], fuzzy method [8-9, 11] and grey relational analysis (GRA) [10]. The AHP-based CE can take all factors which influence the computer network security in to consideration, which benefits the accuracy of evaluation. The fuzzy CE can solve some problem which is fuzzy or hard to quantize, and hence has advantage in solving many nondeterministic problem. The GRA-based CE can deal with the problem in which the parameter evaluation value is indeterminate during the evaluation. However, the ability to solve nonlinear problem of all these methods is relatively weak, and the judgment and recognition capability of them in the complicated situation is not strong.

In recent years, with the development of deep learning, the CE based on neural network has drawn great attention of researchers [1-6, 12-14]. The BP-based CE is one of the most classic neural-network-based CE. Compared with the traditional method mentioned above, the ability of solving nonlinear problem of BP-based CE is strong. Besides, it performs well in the complicated situation due to its strong judgment and recognition capability. Combined with Genetic Algorithm (GA), the BP-based CE has more faster rate of convergence, which makes it more suitable for real-time computer network security evaluation [15].

The factors affecting computer network security are mainly listed as following: firstly, there is problem existing in the expansion and stability of computer network operation. The reasons are that the design of computer network system is not standard, the structure of computer network system is unreasonable, and the expansion and upgrading of computer network system are difficult. Secondly, the

hardware configuration of computer network system is uncoordinated. At present, the connection of some computer network file servers is not good, and the operation of the network center is not stable, which has affected the operation of the computer network security system. Thirdly, the operation of the computer network system lacks a scientific security management strategy. In multiple network sites of the computer, the firewall configuration expands the access right of the system virtually and ignores the setting of the network permission during the operation of the system, thus leading to a serious problem of abusing the computer network resource. Therefore, in this paper, a research of the applications of GABP algorithm in the evaluation of computer network security is performed according to the influence factors of computer network security and combined with the characteristics of GABP neural network algorithm. What's more, the construction scheme of computer network security defense system is fatherly discussed, aiming at improving the security of computer network system.

The rest of this paper is organized as follows. In Section 2, modeling of complex computer network security evaluation method based on GABP algorithm is introduced.

Section 3 first introduce the design of computer network security test and evaluation system, after which the requirements analysis of computer network security defense system is introduced. Based on these, the specific design of computer network security defense system is proposed at the end of Section 3. In Section 4, we conclude our work.

2 Modeling of Complex Computer Network Security Evaluation Method Based on GABP Algorithm

2.1 Neural Network

Based on the characteristics and structure of human brain, neural network forms a large-scale nonlinear dynamics and parallel distributed information processing system by connecting each simple processing unit. In terms of its usage, the neural network consists a number of simple processing units. The changes in the neural network are described in (1).

$$Yi = f(\sum_i w_{ij} x_i - \theta j + Sj) \tag{1}$$

(Xi is for input signal, Wij is the weight value of the connection between the i-th neuron and the j-th neuron, and the j-th neuron threshold is θ_j)

2.2 BP Algorithm

BP algorithm divides the learning process into two stages: forward propagation and reverse propagation. Forward propagation is to transmit the input information from the input layer to the hidden layer, and process and calculate the actual output value of each unit. The reverse process is to calculate the difference between the actual output value and the expected value in a hierarchical recursive manner when the expected output value is not obtained in the output layer. The basic description of BP algorithm is shown in Fig. 1.
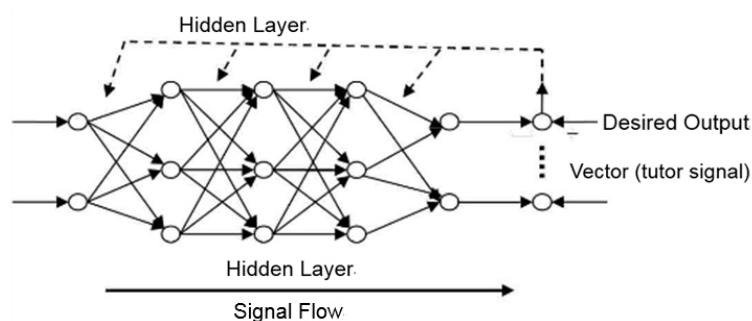
Fig. 1. Basic description of BP algorithm

2.3 Improvement of Modeling of BP Algorithm by GA Algorithm

The idea of GA algorithm for BP algorithm is to adjust and change network weight algorithm relying on gradient information by BP algorithm of, and use genetic algorithm to search global points. Modeling and reconstruction samples determine the number of the nodes of input layer and output layer. Therefore, it is necessary to optimize the number of hidden nodes when optimizing the BP network structure. The mathematical description of GA algorithm improving the modeling of BP algorithm is shown in (2) and (3). The genetic algorithm can be used to solve the problem of quadratic nonlinear optimization, supporting the obtained connection weight and structure of the network to be substituted into formula (4) to obtain E2. If the final value of E2 is less than the assumed error, the model can be applied in the actual prediction of the system.

$$\min E\ (w,\ v,\ \theta,\ r) = \frac{1}{2}\sum_{k=1}^{N1}\sum_{t=1}^{n}\left[y_k(t)-\hat{y}_k(t)\right]^2 \tag{2}$$

$$St\ \ w\in R^{mxp},\ v\in R^{pxn},\ \theta\in R^p, r\in R^n \tag{3}$$

$$o_{jk}^{L} = f(net_{jk}^t) \tag{4}$$

BP network is used for a preliminary identification of the basic solution space in the formula. First of all, set the times and error of network training. Then input the information of training sample to carry out the training. After that, input the errors of test sample and mark the connection weight value of minimum and maximum for Umin and Umax when both are available, and the connection weight value in [Umin-$\delta 1$, Umax+$\delta 2$] are the basic solution space. Considering that the maximum value of the objective function will be taken as the fitness function during the initial optimization of genetic algorithm, the fitness function can be defined as:

$$F(w,v,\theta,r) = \frac{1}{\sqrt{\sum_{K=1}^{N_1}\sum_{i=1}^{n}[y_k(t)-\hat{y}_k(t)]^2}} \tag{5}$$

For the operation of computer network security evaluation system, a comprehensive analysis of the changing rules of network security states should be performed when designing and applying the computer network security evaluation system. The basic function of the system is to monitor the whole process of the operation, and recognize the monitoring results for further analysis. Computer network security evaluation model based on CABP algorithm can make scientific verification and analysis of system operation, so as to offer an effective security evaluation method for computer network system operation.

3 Implementation of Computer Network Security Defense System

The computer network security defense system is built on the computer network security test and evaluation system. In this section, computer network security evaluation based on GABP will be introduced. After this, we analyze the specific requirement of computer network defense system. Based on the above two points, the concrete design of computer network defense system will be introduce.

3.1 The Design of Computer Network Security Test and Evaluation System

Support platform. The support platform computer network security test and evaluation includes management control, asset identification, online monitoring, security testing, malicious attack code testing, etc. At the same time, the computer network security test and evaluation system has special requirements for the evaluation equipment of security test. Therefore, the support platform of the computer network security test and evaluation system is mainly a small switch, and each subsystem is an independent platform for the evaluation of hardware, operating on different computers.
System function. The computer network security test and evaluation system operates by applying each

test subsystem to test and evaluate the data, including risk assessment, security operation assessment and prediction, etc. Risk assessment is to test the data information by using each test subsystem, and obtain the network information system assets based on the relevant test specifications and evaluation models, so as to achieve a comprehensive evaluation of the operation of the entire network system. The security state assessment mainly refers to testing the data by each test subsystem, and then quantify of test results. The specific workflow is shown in Fig. 2.

Fig. 2. Evaluation and prediction of the security state of computer network security test and evaluation system

3.2 Requirements Analysis of Computer Network Security Defense System

The construction of computer network security defense system needs to meet the following requirements: (1) Enhance the application security of computer network security defense system as much as possible to ensure the security of computer network. (2) The design of computer network security defense system shouldn't influence the performance of the previous system, while ensuring the operation security of network transmission protocol and enhancing the security and stability of data transmission of the entire system. (3) In the process of designing the computer network security defense system, reduce operations as much as possible to avoid the interference of additional conditions on the system, so as to improve the effect of the entire system design. (4) In the application of security protection mechanism, protection password and user permissions also need to be set to ensure the security of the entire system.

3.3 The Specific Design of Computer Network Security Defense System

Computer network security defense system. When building a computer network security defense system, it is necessary for relevant personnel to fully learn about the information of the network structure and network application, then conduct comprehensive analysis of the information to understand the hidden security risks in the operation of the system and the basic security requirements of system construction, and to build a complete computer network security defense system.

Computer network security defense system mainly includes the following aspects: firstly, the physical layer. The physical layer is mainly to do protection work to ensure the physical security of the computer network system, and protect the computer network equipment from natural disaster during operation, thus ensuring its operation security. Secondly, the network layer. In the network layer of the computer network system, the physical isolation between the internal network and the external network should be done to ensure that the internal network and the external network are isolated from each other. Thirdly, the system layer. In the computer system layer, the shortcomings of the current computer network system operation can be found timely by simulating hacker attack technology, then the security risks of the entire system operation can be reduced by timely measures. Fourthly, the application layer. In this layer, it is necessary to take effective measures to prevent the network virus from attacking. The security precaution of application layer is to install some anti-virus software and monitoring system in the vulnerable system to ensure the security of the entire computer system.

The function design of computer network security defense system. Firstly, network communication management function. The implementation of the communication management function can not only ensure the users with privileges have free access to the system, but also set their own access conditions according to the importance of the system. Secondly, the mobile storage management function. The accomplishment of the mobile storage management function of computer enables people to freely use the computer network if there is any need, and records the usage information. Thirdly, the printer management function. The implementation of the printer management function can ensure that all kinds

of printed documents and their backup information are transmitted to the server. Fourthly, interface peripheral management function. Under the interface peripheral management function, the system interface can work smoothly.

The application technology of computer network security defense system. Firstly, RSA encryption technology. In the previous field of cryptography, the encrypted string m was encrypted by using encryption rules, then the encrypted information was sent to B. In this process, A must inform B of its encryption rules, otherwise B cannot decrypt the encrypted information, but it cannot pass the encryption rules to B, otherwise the information will be intercepted in the transmission process, enabling the relevant personnel to get the information timely. To solve this problem, some scholars proposed a new algorithm that can achieve asymmetric encryption under the effect of this algorithm. That is RSA encryption algorithm. The application process of RSA encryption technology in computer network security defense system is as follows: (1) Choose two unequal prime numbers p, q (the actual key is usually 1024 or 2048 bits). Here 61 and 53 were chosen. (2) Calculate the product n####. = P * q = 3233 (binary 1100100001, only 12 bits). (3) Calculate the Euler function $\varphi(n)$ of n. (4) Randomly select an integer e, which should meet the condition that $1 < e < \varphi(n)$ and e and (n) are mutually prime. (5) Calculate the modular and inverse element d of e for (n). (6) n and e are encapsulated as public keys, and n and d are encapsulated as private keys. (7) Analyze and obtain the private key. Secondly, Intrusion detection technology. Based on the IP layer of computer network, the firewall technology can be applied to monitor and analyze the WeChat information of illegal intrusion, and restrict the illegal login to ensure that users can log in the system safely. The firewall can filter the illegal attack data effectively and supervise the operation of this system. Thirdly, information encryption transmission technology. To avoid the eavesdropping of data transmission, it is necessary to strengthen the encryption of data information. Fourthly, user authentication technology. Under the function of the authentication system, the public key and secret key are set for the user who uses the computer to effectively verify the information of the logged-in user.

4 Conclusion

In summary, computer network provides convenience for people's life, but there also exists security risk. For this reason, relevant personnel need to consider the effect factors of operation security and apply the advanced technology to evaluate the operation security of the computer system. To achieve this, we analyze the GABP-based computer network evaluation method, based on which we propose a computer network defense system, however the specific realization mechanism still needs to be reflected in the follow-up work. In addition, under the background of network socialization, the security of computer network information system is not only a technical problem, but also a management problem. Therefore, while establishing the computer network security defense system, the related personnel also need to think about how to optimize its application management, in order to ensure the application security of computer network system under the function of both technology and management.

Reference

[1] X. Yang, R. Liu, S. Xu, Comparison of applications of neural network algorithm in computer network security evaluation, Computer Programming Skills & Maintenance 11(2016) 89-90.

[2] X. Liu, An analysis on the application of GABP neural network algorithm in the security evaluation of computer network, Journal of Heihe University 9(6)(2018) 211-212.

[3] S. Wen, B. Wang, Computer network security evaluation simulation model based on neural network, Modern Electronic Technology 3(2017) 97-99.

[4] X. Yang, R. Liu, S. Xu, Computer network security evaluation based on artificial fish-swarm neural network, China New Communications 18(13)(2016) 120-120.

[5] S. Xu, R. Liu, Security evaluation of computer network based on LM-BP neural network, Telecom World 14(13)(2016) 11-11.

[6] H. Chen, H. Li, Prediction method of computer network security situation based on Kalman algorithm, Electronics World 7(2016) 28-28.

[7] Y. Jiang, C. Li, Computer network security assessment based on grey hierarchy model, Measurement & Control Technology 10(2017) 114-118.

[8] Y. Zhang, X. Deng, D. Wei, Assessment of E-commerce security using AHP and evidential reasoning. Expert Systems with Applications 39(3)(2012) 3611-3623.

[9] M.C. Lee, Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method, International Journal of Computer Science & Information Technology 6(1)(2014) 29.

[10] Y. Gao, J.Z. Luo, Information security risk assessment based on grey relational decision-making algorithm, Journal of Southeast University (Natural Science Edition) 392(2009) 225-229.

[11] Su C, Li Y, W.J. Mao, S. Hu, Information network risk assessment based on AHP and neural network, in: Proc. 13th APCA International Conference on Control and Soft Computing (CONTROLO), 2018.

[12] J. Gao, Research on computer network security evaluation based on neural network, in: Proc. 4th International Conference on Machinery, Materials and Computer (MACMC 2017), 2018.

[13] L. Wang, J. Yu, B. Qiao, Intelligent evaluation of computer network security based on neural network. Journal of Intelligent & Fuzzy Systems 35(3)(2018) 1-5.

[14] J. Qiang, F. Wang, X. Dang, Network security based on DS evidence theory optimizing CS-BP neural network situation assessment, in: Proc. 5th IEEE International Conference on Cyber Security and Cloud Computing, 2018.

[15] C. Cheng, The method of the complex computer network security assessment based on GABP algorithm, [dissertation] Hefei, Anhui: HeFei University of Technology, 2007.