Application Analysis of Neural Network in Computer Network Security Evaluation

Qingbo Hao*, Yan Xu
Network Information Center, Qufu Normal University, Jining, 273165, China

Abstract: Aiming at the problem of low accuracy of traditional computer network security evaluation model, this paper studies the application of neural network in computer network security evaluation, and designs a security evaluation model. Based on the established computer network security evaluation index system, the basic structure of neural network is determined. AIS technology is used to realize computer network security evaluation, and the design of computer network security evaluation model is completed. Compared with the traditional evaluation model, it is proved that the designed safety evaluation model based on neural network has higher evaluation accuracy and more advantages.

Keywords: Neural network; Computer networks; Safety evaluation; Application analysis

1. Introduction

The continuous development of computer technology has brought great convenience to people's life and production, and also changed people's way of life. While enjoying the convenience of computer technology, the security of computer network has attracted people's attention. Criminals invade the computer network through holes in the computer network or in the form of viruses, steal materials and spread harmful information, etc., which have seriously affected the security of the computer network [1].

Computer network security is the use of advanced network technology, network control measures to fully ensure the availability of all kinds of data in the computer network environment, the integrity of all kinds of data information, all kinds of data confidentiality. Computer network security can be divided into logical security and physical security. Among them, logical security mainly refers to the need to fully ensure the security, integrity and availability of all kinds of data on the network. Physical security means to take physical means to fully protect the relevant equipment of the computer, so as to avoid physical damage to the computer during operation [2].

Neural network is an algorithm mathematical model that imitates the behavior characteristics of animal neural network and carries out distributed parallel information processing. By adjusting the inter-connection relationship between a large number of internal nodes, the purpose of information processing can be achieved [3]. The basic working process of neural network is to realize the user's requirements by constructing the relation between the internal nodes of the structure section of the mathematical model. Neural network system has a powerful learning function, which can automatically identify the information input by users, summarize and conclude the rules between the information and operate automatically. The neural network can also make predictions based on the identified information, which can provide scientific reference for people's decision-making and planning. Therefore, this paper will build a computer network security evaluation model based on neural network and analyze the application of neural network in computer network security evaluation.

2. A Computer Network Security Evaluation Model based on Neural Network is Established

2.1. Establish computer network security evaluation index system

Computer network itself is very complex, and there are many factors affecting computer network security, in order to further strengthen the evaluation of computer network security, need to establish a perfect computer network security evaluation system. Based on the actual process of network security comprehensive evaluation, this paper divides network security into five aspects, including management security, environment security, hardware security, software security and data security. Using Delphi method to determine the network security comprehensive evaluation index system. Through systematic analysis, the evaluation index is preliminarily formulated and classified, the evaluation index consultation table is compiled, the opinions of experts are consulted, and the indexes are screened. The series that formulates index importance degree, divide for 5 commonly, the quantity value of 5 levels takes 1, 2, 3, 4, 5 respectively, quantity value is smaller more important. Ask an expert to undertake appraisal to the importance degree of index according to formulary way. In the proposed indicator system, there are two indicators at a certain level, and experts are invited to review the degree of concentration and dispersion of statistical experts' opinions on each indicator. The concentration degree of expert opinions E_i is defined as follows:

$$E_i = \frac{1}{n}\sum_{j=1}^{n} a_j \quad ,i = 1,2,L,m \tag{1}$$

In the above equation, a_j is the score value of the JTH expert, and n is the number of evaluation indicators [4]. The dispersion degree of expert opinions can be calculated by standard deviation s_i, and the formula is as follows:

$$s_i = \sqrt{\frac{1}{n-1}\sum_{j=1}^{n}\left(a_j - E_i\right)^2} \tag{2}$$

According to the characteristics of network security, $E_i \le 3, s_i \le 0.62$ is taken as the condition to select the evaluation index of computer network security and establish the comprehensive evaluation index system of computer network security as shown in the figure below [5].

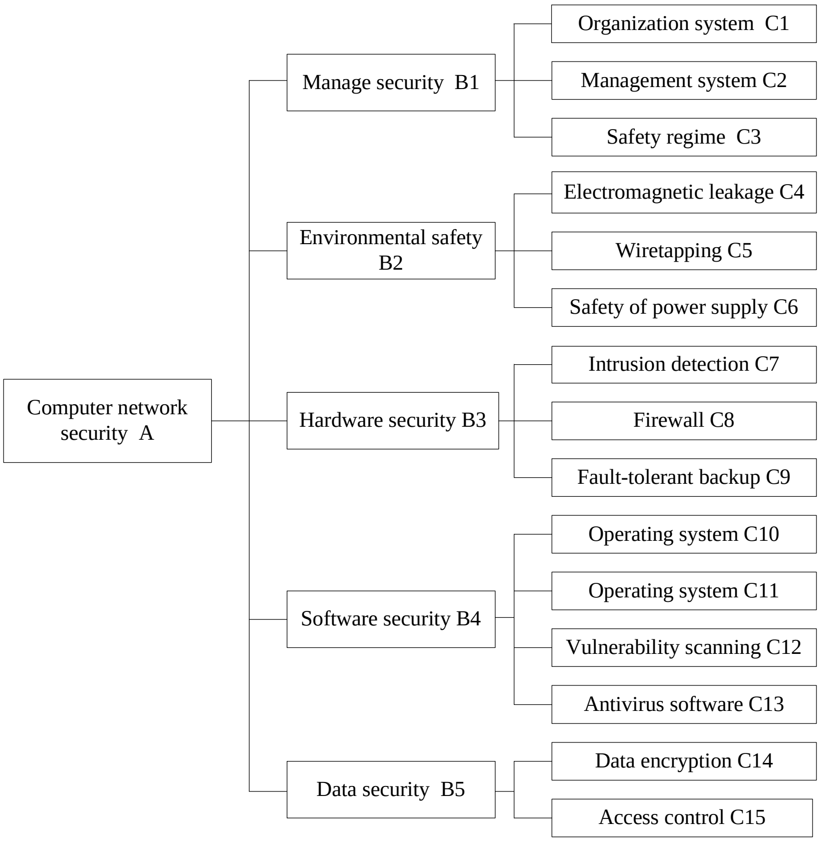

Figure 1. Comprehensive evaluation index system of computer network security

Network security is the target layer (A), and the first-level index layer (B) is composed of management security, environmental security, hardware security, software security and data security. The secondary index layer (C) consists of organizational system, management system, security education, anti-electromagnetic leakage, anti-wiring eavesdropping, security power supply, intrusion detection, firewall, fault-tolerant backup, operating system, application software, vulnerability scanning, access control, data backup and other indicators. According to the established computer network security evaluation index system, the neural network structure of the security evaluation model is determined.

2.2. Determine the structure of the neural network

This paper chooses BP neural network composed of input layer, hidden layer and output layer. The number of input nodes of BP neural network is consistent with the number of computer network security evaluation indexes. 15 evaluation indexes are set in the computer network security evaluation system established above, and the number of neurons in the input layer of BP neural network is 15.

The BP neural network selected in this paper adopts a single hidden layer, and the number of nodes in the hidden layer has a great influence on the performance of the entire computer network. If the number is too small, the nonlinear mapping and fault-tolerant performance of computer network will be seriously affected. If the number of nodes is too large, the learning time of the network will be greatly increased and the learning efficiency will be affected [6]. Therefore, the number of hidden layer nodes should be selected reasonably according to the empirical formula. The empirical formula for calculating the number of hidden layer nodes is as follows:

$$k < \sum_{1}^{n} C\begin{pmatrix} n_1 \\ i \end{pmatrix} \quad (3)$$

In formula (3), k is the number of samples, $k < \sum_{1}^{n} C\begin{pmatrix} n_1 \\ i \end{pmatrix}$ is the number of hidden layer nodes, when $i > n_1$, take $C\begin{pmatrix} n_1 \\ i \end{pmatrix} = 0$. Where, the relationship between the number of nodes in the hidden layer n_1 and the number of nodes in the input layer and output layer is shown in the following formula [7].

$$n_1 = \sqrt{k+h} + d \quad (4)$$

In the above equation, k is the number of elements in the input layer, h is the number of nodes in the output layer of the neural network, and d is the constant on the interval [1, 10]. The nodes of the output layer of BP neural network are designed as two. If the output result is (0, 0) or (0,1), it means that the computer network is unsafe. If the output result is (1, 0) or (1, 1), it means that the computer network is in a safe state. In neural network, each layer is connected by connection weights, and the output of each layer is taken as the input of the next layer. The calculation formula of connection weights is as follows [8].

$$w_{ij} = \frac{1}{1+\exp(E_i)} \quad (5)$$

If the input of the ith neuron in the upper layer is u_i, and the output of the JTH neuron in the lower layer is h_j, then the relationship between input and output is shown as follows.

$$h_j = u_i \times w_{ij} \quad (6)$$

After the basic structure of the neural network is determined, the training samples are used to train the neural network so as to minimize the mean square error between the actual output value and the expected output value. The neural network was initialized, and training samples were input to the neural network by using gradient search technology. The input signal was processed from the input layer through the hidden layer and transmitted to the output layer. Each layer of neurons only affected the state of the next layer of neurons. If the desired output cannot be obtained at the output layer, the back propagation is carried out to return the error of the output signal along the original connection path. The training of the neural network is completed by modifying the connection weights between neurons at each layer to minimize the error. When the security evaluation model is used, the trained parameters are used to evaluate the security of the computer network.

2.3. Complete computer network security evaluation

In order to evaluate the security of computer network, AIS technology is used to generate identification detector, and the output of neural network is identified and retested. AIS is a simulation of the biological immune system, to identify the damage to the computer network. The process of detecting matches is shown below.

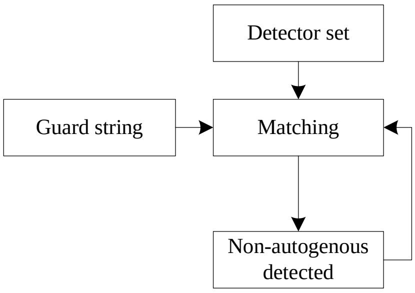

Figure 2. Detection matching process

AIS detector to distinguish "self" from "non-self". Because all the data in the computer is stored in the form of binary, take advantage of this characteristic, based on the binary string to construct Self sets: with length l, step length l and sliding window to scan the need to protect data, then these binary character string of length l is Self samples, will they add to the Self centered. Because the protected data and the generated Self set are represented in binary, a string immune matching rule for binary is used during the simulation. The best match between two binary strings is that the characters in the corresponding position are the same, that is, the two strings are identical, but the best match is rarely found in practice. Therefore, most of them are local matching for detection [9]. In this paper, r-continuous bit matching algorithm is adopted to match the string, specifically: for any two strings x and y, if at least the continuous r bits in the corresponding positions of the two strings x and y are the same, then the two strings are r-continuous bit matching.

$$\mathrm{Match}(x,y)\big| r = true \quad (7)$$

Under the r-continuous bit matching algorithm, the probability of any two strings a and b matching is

$$p(\mathrm{Match}(a,b)) = 2^{-r}\left(\frac{l-r}{2}+1\right) \quad (8)$$

Where, l is the length of the string, and the matching parameter r directly affects the matching probability between two strings. When r minus 1, the matching probability between two strings becomes:

$$p\left(\text{Match}\left(a,b\right)\right)=2^{-r}\left(l-r+2\right) \tag{9}$$

At this point, the matching probability increases exponentially [10]. Here, the parameter r essentially determines the accuracy of immune detection. The smaller r is, the higher the probability of matching and the lower the accuracy of detection. Take the limit. When r is larger, the probability of matching is lower and the accuracy of detection is higher. Take the limit, when r=1, it needs to match exactly, and the detection accuracy is the highest. According to the matching result, the security index of computer network is output. The classification of computer network security level is shown in the following table.

Table 1. Classification of computer network security level

safety index	security level	network operation
0-0.2	Safety	Running normally
0.2-0.5	Mild dangerous	Operation was slightly affected
0.5-0.8	Moderate risk	The operation was greatly damaged
0.8-1	Severe danger	Serious safety accident occurred in operation

According to the output security index, regulators judge the computer network security situation and evaluate the level of network security. Thus, the design of computer network security evaluation model based on neural network is completed.

3. Experiment

In this paper, a computer network security evaluation model based on neural network is designed. The performance of the two evaluation models is verified by comparative experiments.

3.1. Experiment content

The experimental group is the neural net-based computer network security evaluation model designed in this paper, while the control group is the traditional computer network security evaluation model. The error between the two models' output security index and expected value is compared to measure the safety evaluation accuracy of the two models. Set up the experimental environment as shown in the following figure, control the condition other than the experimental comparison, and verify it in the experimental environment. In this experiment, the attack machine will be simulated to attack the network, and the network sensor will be used to collect the attack information of the router Snort.

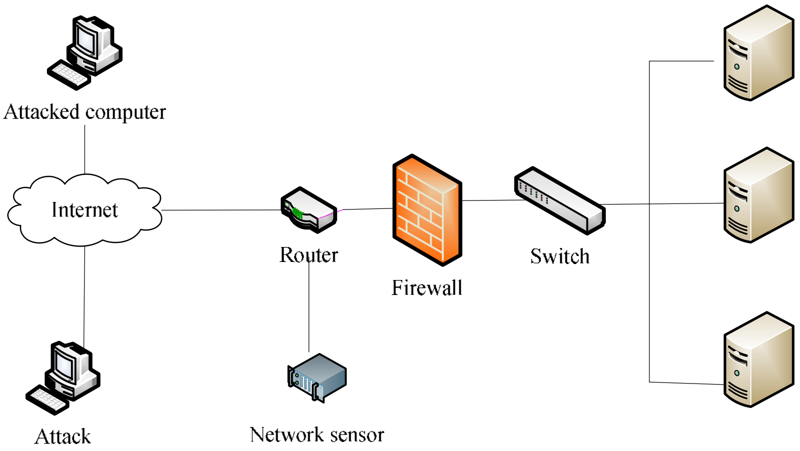

Figure 3. Experimental environment

KDD Cup99 data set was selected as the intrusion detection standard data set. The data set annotated the specific network behaviors, which could accurately detect the accuracy of the method. The attack type of the data set is shown in the following table.

Table 2. Data set attack types

Threat level	Attack types	Xi	Annotation fields
Low	D	0.3	Back, land, neptune, pod, smurf, teardrop

↓ High	U	0.5	Rootkit, buffer_overflow, loadmodule, perl
	R	0.6	Guess_passwd, warezmaster,ftp_write, imap, phf, multihop, warezclient, spy
	P	0.8	Ipsweep, nmap, portsweep, satan

In the above table, X_i is the attack threat factor. Different attacks have different threat levels according to the system permission obtained by the attack and the degree of influence on the network operation. With the increase of the threat level, different attack types have increased the degree of influence on the network security operation threat. Set the evaluation period as T, extract the data from KDD Cup99 sample set for intrusion detection within T time, and use Snort for acquisition. By comparing the error between the output and expected output of the two groups of models, the advantages and disadvantages of the two groups of safety evaluation models are determined.

3.2. Experimental results

The experimental results are shown in the following table. The information in the table is analyzed and corresponding conclusions are drawn.

Table 3. Experimental results

Sample number	Security level	Desired output	Experimental output	Control output
1	d	0.42	0.42	0.46
2	c	0.6	0.6	0.55
3	a	0.87	0.85	0.81
4	d	0.22	0.22	0.20
5	c	0.61	0.60	0.54
Root mean square error			0.01	0.051

Analysis of the data in table 3 shows that the output of the evaluation model in the experimental group is closer to the expected output value than that of the model in the control group. Although the security level is the same according to the output value of the two groups of output models, the network security is changing day by day. When the classification of the security level is more detailed, the evaluation accuracy of the two groups of computer network security evaluation models will be more obvious. The root-mean-square error of the output safety index of the two groups was calculated. The experimental group was lower than the control group, indicating that the overall accuracy of the experimental group model was higher than that of the control group model. In conclusion, the neural network-based computer network security evaluation model studied in this paper has higher evaluation accuracy.

4. Conclusion

Neural networks have attracted much attention because of their simplicity and maneuverability. This paper studies the application of neural network in computer network security evaluation, designs a model, and compares the model with the traditional model, proves the superiority of the design model. In the future, researchers should be aware of the advantages and limitations of neural network, and combine neural network with other advanced methods to better apply it to computer network security evaluation.

References

[1] Sun Baohua, Hu Nan, Li Dongyang. Analysis research of software requirement safety based on neural network and NLP. Computer Science. 2019, 46(S1), 348-352.

[2] Zhao Wenjiang, Xu Mingde, Zhang Junjie, et al. Application of BP neural network in mine ecological security evaluation. Coal Technology. 2019, 38(01), 172-175.

[3] He Rongjun, Luo Dayong. Application of improved particle-swarm-optimization neural network in coalmine safety evaluation. Industrial Safety and Environmental Protection. 2018, 44(11), 29-31.

[4] Zhang Xu, Wang Lu, Meng Fanshun, et al. Bayesian neural network approach to casing damage forecasting. Progress in Geophysics. 2018, 33(03), 1319-1324.

[5] Huang Guangqiu, Lu Qiuqin. Improved structure-parsed neural Petri-net model and its application to the haze detriment evaluation. Journal of Safety and Environment. 2017, 17(04), 1554-1562.

[6] Peng Qing, Ji Guishu, Xie Linjiang, et al. Application of convolutional neural network in vehicle recognition. Journal of Frontiers of Computer Science & Technology. 2018, 12(02), 282-291.

[7] Zhu Kun, Zhang Qi. Application of machine learning in network intrusion detection. Journal of Data Acquisition & Processing. 2017, 32(03), 479-488.

[8] Jiang Tongqiang, Ren Ye. GA-BP neural network and its application in safety evaluation of liquid milk. Science and Technology of Food Industry. 2017, 38(05), 289-292.

[9] Wen Siqin, Wang Biao. Computer network security evaluation simulation model based on neural network. Modern Electronics Technique. 2017, 40(03), 89-91.

[10] Tang Shaoliang, Zhang Xiaoxiao. Research on early-warning and evaluation of traditional Chinese medicine industry security based on BP neural network. Chinese Traditional and Herbal Drugs. 2017, 48(02), 406-418.