Research of computer network security evaluation based on RBF neural network

Yan-ling Zhang[1, a], Jian-liang Xiong[2,b]

[1]Computer Engineering Department, Tangshan Vocational College of Science and Technology, Tangshan, China

[2]Computer Engineering Department, Tangshan Vocational College of Science and Technology, Tangshan, China

[a]zhangyanling2005@126.com, [b]xxxx9527@126.com

Keywords: RBF neural network, Computer network security, Evaluation.

Abstract. Nowadays, computer network is widely used in many areas of daily life. Since the affectation of vulnerabilities and viruses, there will be a variety of security issues in the application process of computer network. In order to provide effective protection for computer network security, computer network security evaluation system should be established. This article will use RBF neural network to evaluate the security of the computer network, which will improve the level of computer network security.

1. Introduction

Currently, computer network is widely used in many areas of daily life [1]. The development of network technology brings convenience to people's lives, but also provide convenience for network virus attacks, Trojans and some other damaging programs, which brings growing danger to computer network security[2-3]. It has a very important practical significance to evaluate the risk accurately and scientifically, prevent the risk effectively and reduce the loss of computer network security problems. Computer network security is affected by many factors, such as intrusion, vulnerabilities, viruses, etc. These factors are related to each other, and there are complex nonlinear relationships between factors and evaluation results [4]. Traditional evaluation methods such as AHP, gray model, etc. have the characteristics of complicated operation, difficult to accurately describe the non-linear relationship, and low evaluation accuracy [5].

In recent years, neural network technology is developed widely and rapidly, which is artificial intelligence algorithms with self-learning, self-organization and strong adaptive ability [6]. RBF neural network has the characteristics of laving simple structure, learning convergence fast, training simple, which can approach any nonlinear function, and be widely used in the fields of pattern recognition, image processing, nonlinear control and time series analysis. This article will use RBF neural network for computer network security evaluation, in order to improve the level of computer network security.

2. Construction of computer network security evaluation model based on RBF neural network.

2.1 RBF neural network.

Radial basis Function (RBF) is a traditional technique of multidimensional space interpolation. The basic idea of RBF neural network is that, constituting the hidden layer space with the implicit element base, the hidden layer transforms the low-dimensional model input date to high-dimensional space, so that linearly inseparable problems in low-dimensional space can be solved in high-dimensional space. RBF neural network has the characteristics of laving simple structure, learning convergence fast, training simple, which can approach any nonlinear function, and be widely used in the fields of pattern recognition, image processing, nonlinear control and time series analysis. Since, computer

network security a nonlinear system affected by many factors, RBF neural network is an ideal choice for computer network security evaluation.

2.2 Construction of computer network security evaluation model.

(1) RBF neural network model.

Gaussian function is the most commonly used radial basis in RBF neural network, whose expression is given as follows.

$$R_i(x) = \exp(-\frac{\|x - c_i\|}{2\sigma_i^2}) \quad \text{i=1,2,⋯,m} \tag{1}$$

Where, x is the n-dimensional input vector, c_i is the center of i-th basis function, σ_i is the planning factor of i-th basis function, $\|x - c_i\|$ is nearly European norm, and m is the number of hidden nodes.

Set the inputs of input layer as $X = (x_1, x_2, \cdots, x_j, \cdots, x_n)$, and the actual output as $Y = (y_1, y_2, \cdots, y_k, \cdots, y_p)$. The 0-th input layer realizes the non-linear mapping from X to $R_i(x)$. The output layer realizes the linear mapping from *R(X)* to y_k. The k-th neural network of output layer is outputted as follows.

$$\hat{y}_k = \sum_{i=1}^{m} w_{ik} R_i(x) \quad \text{k=1,2,⋯,p} \tag{2}$$

Where, n is the number of input layer nodes, m is the number of hidden nodes, p is the number of output layer nodes, w_{ik} is the connection weights of i-th neurons of hidden layer with k-th neuron of output layer, and $R_i(x)$ is the action function of i-th neuron in hidden layer.

From the structural point of RBF neural network, we can see that the network output can be determined when the weight and threshold of hidden layer and output layer can be determined. So the RBF network learning process is a modification of each network layer's weights and thresholds. This paper selects newrb function to create an approximate radial basis function network.

(2) The process of newrb creating RBF network.

In the process of redial basis function network newrbe and newrb creating RBF network, the weights and thresholds are selected and corrected in different ways, so the radial basis function network don't have specialized training and learning function.

Newrb designs the RBF network by iterative method. In the beginning, there is no radial basis neuron, and the number of radial basis neurons is gradually increasing using the following steps.

① Simulate the network with all of the input samples.

② Find the input sample with maximum error.

③ Add a radial basis neuron, whose weight equals to the transposition of the input vector.

④ Put the output dot product of radial basis neuron as the input of network layer neurons, resigning the linear network layer and making the error the smallest.

⑤ Repeat the above steps, when the mean square error does not achieve the required error performance and the number of neurons does not reach the upper limit value, until to the mean square achieve the required error performance and the number of neurons reaches the upper limit value.

3. Construction of computer network security evaluation index system.

3.1 Principles of index selection.

The reasonable and scientific of computer network security evaluation's index is related to the evaluation function, namely related to whether can raise the level of network security through the

evaluation. In order to establish a set of sound, rational and scientific evaluation index, there are some principles should be followed.

(1) Scientific.

Only by adhering to scientific principles, the obtained information should be reliable and objectivity, and the evaluation results can be valid. The index system should comply with the relevant information , laws and regulations of information system security.

(2) Comprehensiveness.

Computer network security assessment is a comprehensive evaluation with multiple indicators, which should be representative, and shall be selected from all aspects of network security.

(3) Feasibility.

In the evaluation index system, the data collection should be facilitation, and the index system should reflect things comparable. The evaluation work program should be as simple as possible, avoiding exhaustive, cumbersome and complex.

(4) Stability.

When establishing evaluation index system, the selected indicators should change regularly, and those factors who are ups and downs frequently influenced by chance factors should not be selected. The stable index can be meaningful.

3.2 Specific choice of indicator.

Computer network is a complex system, influenced by many security factors. In order to evaluate network's security level, we must establish a scientific and comprehensive computer network security evaluation system. On the basis of computer network system's security management, physical security and logical security, computer network security evaluation index is selected by experts. The specific indicators are shown as follows.

(1) Mange security.

Manage security includes the indicators of security organization system, safety management systems, personnel safety training and emergency response mechanisms.

(2) Physical security.

Physical security includes the indicators of anti-electromagnetic leakage measures, network room security, supply security, line security, device security and fault-tolerant redundancy.

(3) Logical security.

Logical security includes the indicators of data backup, data recovery, system auditing, access control, software security, digital signatures, anti-virus measures, data encryption and intrusion prevention.

4. Empirical analysis.

As the data sets about computer network security is not much, this paper collects 30 sets of computer network security evaluation with different scales for empirical analysis.

4.1 Indicator data pretreatment.

The index system reflects the computer network security situation from different angles. Due to the different dimensions of the various indexes, they can't be directly compared. In order to make the indicators comparable and accelerate the convergence speed of neural network, this paper will normalize the indicators. The qualitative indicators are obtained by expert scoring method.

(1) Forward-type indicator

$$x_i' = \frac{x_i - x_{i\min}}{x_{i\max} - x_{i\min}} \tag{3}$$

(2) Reverse-type indicator

$$x_i' = 1 - \frac{x_i - x_{i\min}}{x_{i\max} - x_{i\min}} \tag{4}$$

Where, x_i' is the normalized value of x_i, $x_{i\min}$ is the minimum index of the i-th predetermined, $x_{i\max}$ is the maximum index of the i-th predetermined, and i is the number of evaluation index.

4.2 Set the computer security level

This article will divide the computer network security level to four levels, which are Safety (A), Basic Safety (B), Insecurity (C) and Terribly Insecure (D). Set the total points to 1, and the several score of each security level is shown in Table 1.

Table 1 Computer Network Security Level

Level	A	B	C	D
Score	1~0.85	0.85~0.7	0.7~0.6	0.6~0

(1) Safety.

Safety level indicates that the network has a strong security capability, and the network application is safe. Scores of level A ranges from 0.85 to 1.

(2) Basic safety.

Basic safety level means that the network has certain ability of security, and the network application has basic security. Scores of level B ranges from 0.7 to 0.85.

(3) Insecurity.

Insecurity level indicates that the network security ability is limited, and the network application is unsafe. Scores of level C ranges from 0.6 to 0.7.

(4) Terribly Insecure.

Terrible insecure level shows that security ability is poorer, and network application security situation is grim. Scores of level D are below 0.6.

4.3 Evaluation and Analysis

This article uses the first 27 sets of data as the training data set of radial basis neural network model, the after 3 sets of data as the test data set. Since the too large orders of vectors' magnitudes may affect the training effect, the data should be normalized before training, and the normalized interval can be set from 0 to 1. Using the RBF neural network model of MATLAB toolbox for training and testing, the RBF neural network is created by newrb function.

The format of newrb function is shown as follows.

[net，tr]=newrb(P, T, GOAL, SPREAD, MN, DF) (5)

Where, P and T express input vector and target vector respectively, GOAL is the target error, SPREAD is extension constant, MN is the number of the maximum neurons, DF shows the frequency of the iterative process, and tr is the return value, training records.

Using the above model to evaluate the computer network security, and the evaluation results are shown in table 2.

Table 2 Evaluation Results

Sample	Security Level	Expected Output	RBFNN
28	B	0.83	0.78
29	A	0.90	0.88
30	C	0.62	0.68

From the results of table 2, we can see the expected output of the after 3 sets are 0.83, 0.9, 0.62, and the security level are B, A and C. The RBF neural network outputs are 0.78, 0.88, 0.68, and the security level are B, A and C. It means that the evaluation outputs of RBF neural network model are consistent with the expected results, which proves that it is feasible and accurate to evaluate the computer network security with RBF neural network. It is an effective evaluation method for computer network security management.

5. Summary

Evaluating the computer network security with RBF neural network, can get rid of the randomness, the subjective uncertainty, and vagueness in the understanding, to ensure the objective and accurate of evaluation results. It is an effective evaluation method for computer network security management.

References

[1] Yue Tao. Application of neural network in computer network security evaluation. *Computer Simulation*, 2011, 28(11).

[2] Xiewei Wang. Design and application of computer network security evaluation system. *Communication Design & Application*, 2015.

[3] Limin Huang. Research on safety evaluation method of computer network information systems. *Shandong University*, 2004.

[4] Zhiyong Mao. Application of BP neural network in computer network security evaluation. *Information Technology*. 2008(6).

[5] Feng Shi, Xiaochuan Wang, Lei Yu, etc. 30 cases of Matlab neural network analysis. Beijing University of Aeronautics and Astronautics Press, 2010.

[6] Wengao Lou, Li Jiang, Xianghui Meng. Neural network models of computer network security comprehensive evaluation. Computer Engineering and Application, 2007,43(32):128-130.