Send Orders for Reprints to reprints@benthamscience.ae

Open Access

Research on Application of Neural Network in Computer Network Security Evaluation

Shujuan Jin*

Guizhou University of Finance and Economics, Guiyang 550000, China

Abstract: Purpose: discuss the role of the neural network (NN) theory in the computer network security evaluation. Method: propose three-level and four-class indicator system suitable for network security evaluation, establish the network security evaluation system model based on NN, optimize the NN model by using the particle swarm, collect 100-group data on the computer network security evaluation of different scales via expert scoring, and normalize them; Result: the evaluation model based on NN is simple and practicable to network security evaluation and can eliminate disturbance of the subjective factors of the human being. The simulation results indicate that the system can reduce relative output error and improve correctness rate of evaluation. Conclusion: The NN model is very valuable in research on the computer network security evaluation system, which can offset weaknesses of the past evaluation methods to some extent, improve precision of the evaluation results, and provide reference to prediction and control of the network security problems in future.

Keywords: Neural network, network security evaluation, three-level and four-class indicator system, particle swarm algorithm, normalization, prediction and control.

1. INTRODUCTION

With quick development of sciences and technologies, the computer network and communication technologies quickly develop and become extensively popular. Although development of network technologies brings convenience and efficiency to life of human being, they also provide space for growth of destructive programs such as viruses and Trojans and bring higher and higher dangers to the computer network security. The computer network security indicates that the hardware, software and data in the network system are protected and are free of destruction, alteration and disclosure due to accidental or malicious reasons, the system can continuously and reliably operate, and the network service does not disrupt. The computer network security includes network equipment security, network information security, and network software security. How to accurately and scientifically evaluate the network risks, effectively prevent against the risks, and reduce the loss due to computer network security issues is discussed by all social circles [1, 2].

Now the network security issue is very severe in China, e.g. the computer system is severely infected and destructed by viruses, the PC hacker activities become important threats, the information infrastructure faces the challenge from the network security, and subversive activities such as network politics, cults and terrorist attack are frequent. The computer network security is a comprehensive subject involving computer science, network technology, communication technology, and application mathematics and number theory [3]. Since the concept of the computer network security evaluation is proposed, the scholars have investigated and studied the network security evaluation from difference views. The ANNs (Artificial Neural Networks) is an algorithm mathematical model to simulate behavior features of the animal neutral network and conduct distributed parallel information processing [4, 5]. In recent years, the NN technology is quickly and extensively developing. By using the adaptive artificial intelligence algorithm with self-learning and self-organization capability and powerful function, the ANNs model can effectively overcome the defects of a traditional statistics model, adjust the connection weights between nerve cells, capture the non-linear law between the computer network security and attributes, and accurately evaluate the computer network security, so it is very suitable for evaluation of the computer network security [6]. This paper deeply explores the role of the NN for the current network security evaluation system, and deeply studies its application in the computer network security evaluation.

2. INDICATOR AND PRINCIPLE OF COMPUTER NETWORK SECURITV EVALUATION

2.1. Principle of Computer Network Security Evaluation

The principle of the computer network security evaluation is guided by the evaluation criterions. The popular network security evaluation criterion is the trusted computer criterion and evaluation rule specified by US Department of Defense in 1985. With differences in development progress and degree of different countries, different countries develop related evaluation criterions based on their actual conditions [7, 8]. This paper mainly studies the international evaluation criterion.

1874-1290/14 2014 Bentham Open

Table 1. Classification rule for computer network security protection grade.

Class	Grade	Name	Main features
D	D	Low-level protection	No security protection
C	C1	Independent security protection	Independent storage control
	C2	Controllable storage control	Independent examination and full identifier
B	B1	Flag security protection	Mandatory access control and full identifier
	B2	Structural protection	Security-oriented architecture and stronger anti-penetration capability
	B3	Secure area	Access monitoring and anti-penetration capability
A	A	Validation and design	Formal top-level description and validation

Since the orange book became the criterion of US Department of Defense in 1985, it keeps unchanged all the time and is the main method to evaluate the multi-user hosts and small-scale OS [9]. The orange book divides the security level into four classes from low to high, including class D, class C, class B and class A. Each class is divided into several grades. The classification results are shown as the Table **1**.

Note: The grade D is the minimal grade and the grade A is the maximal level. The maximum protection grade inherits the security performance of the low protection grade.

The network security is evaluated as follows: 1) identify the contents and scope of the network evaluation and perform initial analysis on the basic network conditions, security conditions and network vulnerabilities; 2) Establish the related mathematical evaluation model; 3) Compute the network security level by using the mathematical model. The mathematical model for the computer network security evaluation is described as follows:

$$SL = \Gamma\left(X_1, X_2, ...X_n\right) \qquad (1)$$

SL is the security level (SL). $\Gamma(g)$is the mathematical model for computer network security evaluation, and x_i is the computer network security evaluation factor.

2.2. Indicators for Computer Network Seurity Evaluation

The computer network is a very complicated system because many factors affect the network security. To simplify the network security evaluation model, this paper classifies the influence factors of the network security into 3 levels, 4 classes and 16 evaluation factors, namely 16 evaluation indicators. The selected evaluation indicators are shown as the Fig. (**1**).

This paper selects the evaluation indicators for and data security of the computernetwork system, and computer network security in management security, scores the computer network security evaluation environment security, hardware and software security indicator via the expert system, and identifies its weight.

2.3. Evaluation Indicator Nnormalization and Security Level Setup

From the Fig. (**2**), we can know that the selected indicators can reflect network security conditions from different views. The units and values of indicators are different from each other, so indicators can not be directly compared. To compare different indicators, this paper normalizes indicators by using the normalization method. The indicator value are

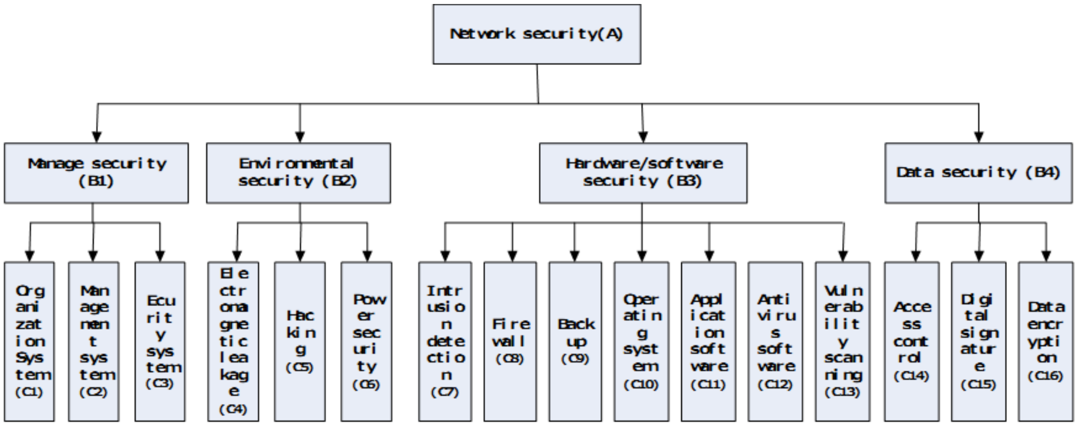

Fig. (1). Comprehensive evaluation indicator of network security.

Table 2. Security level of computer network.

Level	**A**	**B**	**C**	**D**
Score	0.85-1	0.7-0.85	0.6-0.7	0-0.6

collected by using the export scoring method. The indicators assigned with the number . The quantitative indicators are normalized as follows:

$$X_i' = \frac{x_i - \min(x)}{\max(x) - \min(x)} \qquad (2)$$

Wherein x_i' is the normalization indicator, min(x) is the expert score of the indicator i, and max(x) is the maximu of the expert score of the indicator i.

Based on the comprehensive weight of the indicator, the security performance of a computer network can be evaluated. Based on the Table **1**, we can divide the computer network security into four levels. Total score of the security level is set as 1. The corresponding values of the security levels are shown as the Table **2**.

3. SECURITY EVALUATION BASED ON NN

3.1 Basic Concept of NN

In recent years, the NN involves more and more research areas, which reflects features of the multi-subject crossing technical fields. The main research work includes biological prototype, modeling and algorithm research. A specific NN model is established based on research on the theoretical model in order to realize computer simulation or preparation and making hardware of the human being NN, including research on the network learning algorithm. The work on this aspect is also called as the technology model research.

The vector multiplication will be used in a NN and the sign function and other different approximation will be extensively used in order to realize self-learning, self-organization and self-adaptation, which just is difference between a NN computing method and a traditional method. The organization structural organization of a NN is shown as the Fig. (**2**).

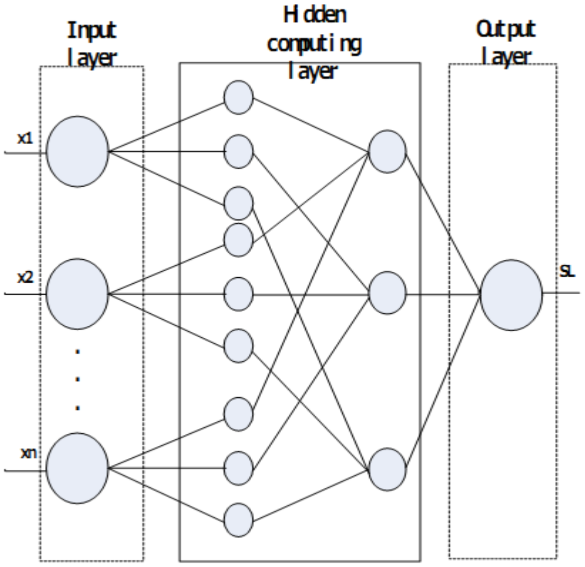

Fig. (2). NN structural organization.

3.2. Principle of NN Evaluation

The NN algorithm is a δ algorithm and a supervised learning algorithm, which mainly uses the gradient search technology on the known learning sample pairs in order to minimize the mean square value error between the network's actual output and expected output, namely train and learn via the known result test sample set, get the parameter value of the mathematical models by combining the optimal strategy, use unknown result test set for the established mathematical model, and finally identify the algorithm of the test set

Table 3. Normalization results of evaluation indicators.

Group	No.	B1			B2				B3						B4		
		C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C10	C11	C12	C13	C14	C15	C16
	1	0.95	0.87	0.81	1	0.8	0.79	0.81	0.76	0.82	0.94	0.89	0.85	1	0.8	0.8	0.9
Training set	2	1	0.95	0.8	0.8	0.9	0.81	0.85	0.72	0.83	0.94	0.9	0.81	0.99	0.79	0.85	0.92
	…	……															
	49	0.6	0.45	0.45	0.21	0.09	0.1	0.5	0.5	0.61	0.15	0.62	0.64	0.25	0.85	1	1
	50	0.81	0.5	0.45	0.79	1	0.85	0.7	0.62	0.54	0.65	0.71	0.95	1	1	0.6	0.41
	51	1	1	1	0.85	0.8	0.95	0.74	0.65	0.85	0.96	0.99	1	0.75	0.85	0.75	0.8
Test set	52	0.25	0.35	0.5	1	1	0.75	0.25	0.85	0.95	1	0.25	0.45	0.65	0.85	1	1
	…	……															
	99	0.65	0.75	0.7	0.85	1	0.95	0.56	0.6	0.6	0.8	0.85	1	0.95	0.9	0.9	0.65
	100	1	1	0.95	0.85	0.8	0.8	0.9	1	0.65	0.8	0.8	0.85	0.75	0.8	0.8	0.8

results via computing. The input signals will be processed from cells at the input layer to the cells at the hidden layer and will be outputted to the output layer. The neural cells at each layer only affects the states of the neural cells at next layer. If the output layer cannot get the expected output, the backward propagation will be launched and the error of the output signals will be returned along the old connection channel. The error is minimized by changing the weight of the neural cells at different layers.

However, the NN algorithm is easy to fall into the local extreme, so it is difficult to get global minimum. In addition, the NN uses the gradient descent algorithm based on the backward propagation and features slow convergence speed, so the learning effect is not satisfactory. This paper uses the particle swarm optimization (PSO) algorithm to optimize the NN network. The implementation steps are described as follows:

1) Initialization: initialize the structure, propagation function and target vector of the NN. The propagation function uses sigmoid function.

2) Parameter setup: set the PSO scale, dimension, iteration time, initial position and speed setup.

3) Train the NN;

4) Compare the current values of each particle with the history best values and save the optimum;

5) Computer an inertia weight;

6) Reset the model parameters and perform the step 2;

7) Determine the system fitting error. If the error reaches the set error limit or is over the maximum permitted iteration time, the training will end! At this time, the history global optimum position of the particle is the best weight and optimum threshold of the NN.

4. SIMULATION TEST

To study correctness of the established model, this paper collects 100 groups of data on security evaluation of the computer network of different scales. 15 scoring experts are selected. The test data includes 50 groups of training data and 50 groups of test data. The collected data will be normalized. The processing results are shown as the Table **3**.

The simplified PSO algorithm is implemented by using MATLAB language. The initial parameters are set as follows: node number of the hidden layer is 8, the weight adjustment parameter is 0.05, the threshold adjustment parameter is 0.01, and the self-learning precision is $1*10^{-5}$. After 10000 times of optimization training, the NN an get the convergence error. The collected data verification results are shown as the Fig. (**3**).

The Fig. (**3**) shows the check results of the collected data. The Figs. (**3a**) and (**3b**) are the check results of the training set. The Figs. (**3c**) and (**3d**) are the check results of the test set. The Figs. (**3a**) and (**3c**) reflect relative errors of the expected output and actual output of the samples. The Figs. (**3b**) and (**3d**) are the box line diagram of the training set and test set. The Fig. (**3**) indicates that the relative output error of the training set is between 0 and 2.5%. The relative output mean error is 1.19%. The check results of the sample 5 and 37 in the training set are incorrect. The check correctness rate is 96%. For the test set, the relative output error is between 0 and 5%. The relative mean output error is 2.07%. The check results of the sample 53, 57 and 91 are incorrect in the test set. The evaluation correctness rate is 94%. In addition, to compare the training set with the test set, we can find that the check results of evaluation correctness rate and relative output error limit in the training set converge better.

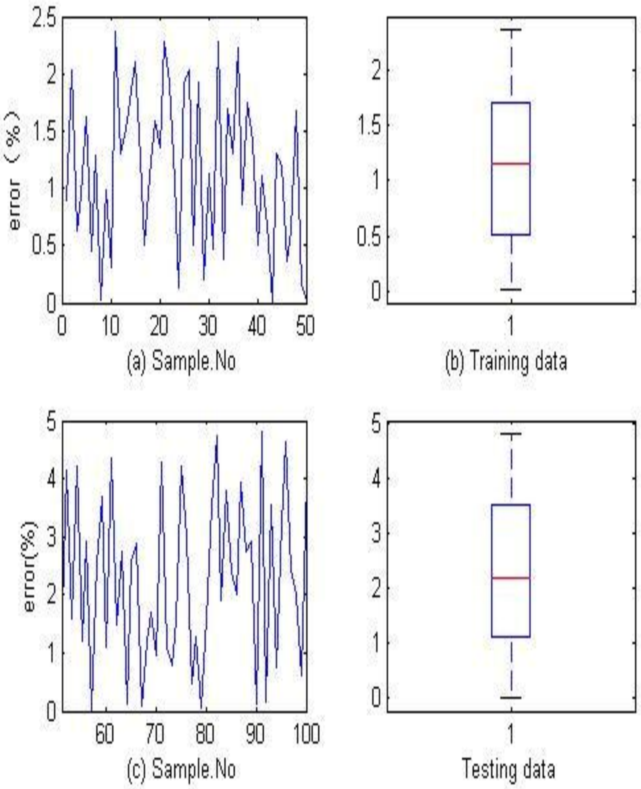

Fig. (3). Test results.

CONCLUSION

This paper studies how to introduce the NN theory into the evaluation system of the computer network security, discusses its role in the evaluation system, and aims to propose an accurate and scientific network risk evaluation system. Based on the previous research, the author selects three-level and four-class indicator system for the network security analysis, establishes a model for the network security evaluation system by using the NN theory, and optimizes the NN model by using PSO algorithm, which can realize quick iteration of the NN and non-linear approximation capability of the NN. In addition, the author collects 100 groups of data on the security evaluation of the computer networks of different scales, divides them into the training set and test set by SN, and normalizes them. The model simulation results indicate that the relative output error of the training set is between 0% and 2.5%. The relative output error of the test set is between 0% and 5%. The correctness rate of the whole evaluation of the training set and test set is 96% and 94%. The check results of evaluation correctness rate and relative output error limit in the training set converge better.

However, the NN theory and our PSO optimized NN theory have their weaknesses, e.g. the converged results cannot be obtained, the iteration time is too plentiful, and the computing duration is too long, which should be further solved. The NN model is very valuable in research on the evaluation system of the computer network, which can off set the weaknesses of the past evaluation method, reduce errors in the traditional evaluation, and improve precision of the evaluation results. This paper discusses and analyzes the related issues to attract attentions to the NN, gradually perfect it, and make it play bigger role in the computer network security.

CONFLICT OF INTEREST

The author confirms that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] Y. Sun, “Face recognition algorithm based on particle swarm BP NN”, *Computer Simulation*, vol. 25, no. 8, pp. 201-204, 2008.

[2] K. Deng and Z. Y. Zhao, “Research and simulation on stock market prediction model based on generic BP network”, *Computer Simulation*, vol. 26, no. 5, pp. 316-319, 2009.

[3] R. J. Wu, “Research on application of NN in the security evaluation of the computer network”, *Computer Simulation*, vol. 26, no. 5, pp. 316-319, 2009.

[4] D. M. Zhao, H. F. Liu, and C. G. Liu, “Information security risk evaluation based on BP NN”, *Computer Engineering and Application*, no. 11, pp. 139-141, 2007.

[5] S. Z. Guo and G. Chen, *Software computing method in information science*. Shenyang: Northeastern University press, 2011.

[6] S. S. Guo, "Research on computer network security analysis", *Modern electronic technology*, vol. 23, no. 6, pp. 65-66, 2011.

[7] M. E. J. Newman, "Properties of highly clustered networks", *Phys. Rev*, vol. 68, 026121, 2003.

[8] M. E. J. Newman, D. J. Watts, and S. H. Strogatz, "Random graph models of Social Networks", *Proc. Natl. head. Sci*, vol. 99, suppl. 1, pp. 2566-2572, 2002.

[9] P. Romualdo, "Epidemic Spreading in Scale-Free Networks", *Alessandro V.Phy. Rev Lett*, vol. 86, no. 14, pp. 107-109, 2001.

Received: February 18, 2015 Revised: March 22, 2015 Accepted: March 31, 2015

© Shujuan Jin; Licensee *Bentham Open.*

This is an open access article licensed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0/) which permits unrestricted, non-commercial use, distribution and reproduction in any medium, provided the work is properly cited.