Incremental Wavelet Neural Network based Prediction of Network Security Situation

Xiaojian LIU

School of Information Engineering, Eastern Liaoning University, Liaoning Dandong, 118003, China

power_lxj@126.com

Keywords: Network Security Situation; WNN; Incremental Learning; Generalization Performance

Abstract. Network security situation prediction can help network administrators to make security decisions, and the current network security technology cannot predict the future network security situation. Hereby, a network security situation prediction based on incremental wavelet neural network (IWNN) was proposed, which establishes the nonlinear mapping according to the time relationship of network security situation value. Meanwhile, in this method, the complexity of the future network security situation is considered by incremental learning. Therefore, IWNN has better generalization performance in network security situation prediction when considering the changes in the pattern of the future network attack, the network scale and the network security technology, etc. Finally, the performance of the proposed method is verified by the experimental data processing results.

Introduction

Network security is the premise to ensure the normal operation of the network and provide services to the user and the security of networks is more and more important with the opening, sharing and interacting of the network [1]. With the diversification of network attacks, the traditional single network defense equipment or testing equipment has been unable to meet the needs of the network security. Network situational awareness is a comprehensive application of data fusion technology, Bayesian technology and knowledge base, which can obtain the information of the network intrusion behavior of network itself exception, etc. by the network data, traffic information, system logs and other raw data [2]. And then network situational awareness can obtain the whole state of the network. In this way, the network security awareness can make reasonable and accurate prediction of the network security situation in the future, and provide a trend chart of the network security situation. Network security situation prediction makes network security management from passive to active, and can provide a reference for network administrators to understand the situation of network security, make network security decision or command control. So the network security situation prediction has important significance in network security management [3].

In view of the importance of network security situation prediction, many experts and scholars have carried on the research to the network security situation prediction method, and a lot of research results have been reported. Neural network has been widely used in network security situation prediction because of its good nonlinear fitting ability. To further improve the accuracy of neural network in the prediction of network security situation, the algorithms combining genetic algorithm (GA) and particle swarm optimization (PSO) were proposed [4]. Although these methods use the time data information of network security situation, they do not take into account the factors that affect the network security situation changes. With the continuous development of network technology, network intrusion means and style will continue to change, and the scale of the network will be changed with the actual needs. The network security situation prediction model often cannot adapt to the change of the network technology, which results in the degeneration of the network security situation prediction result. That is the generalization performance of the network security situation prediction method is not good. Aiming at the defects of the existing network security situation prediction method, this work proposed a network security situation prediction method based on incremental WNN. WNN takes advantages of wavelet transform and neural network, which has faster convergence rate and higher convergence accuracy compared with traditional BP neural network. The training of neural network can be divided into two models, which are period learning and incremental learning. The periodic learning algorithm tends to use the training sample set to obtain the steady state of the network, so that the average error of the network output converges to a minimum value. Incremental learning training the network weights by the sample data in order, which adapt to the new sample data by adding or removing the hidden layer nodes of the neural network during the training process. Therefore, the periodic learning method is suitable for the static system, while the incremental learning is suitable for the dynamic system. Because of the dynamic characteristics of network security, the incremental learning algorithm is more suitable for the network security situation prediction.

Network Security Situation Prediction by WNN

Network security situational awareness is a technology to obtain, understand and predict the security elements which influence the situation of network security in the large scale network environment. Calculation of network security situation and network security assessment constitute the whole network security situation technology [5]. Fig.1 shows the layered model of network security situational. The layered model of network security situational shows that the network security situation depends on the network service provided by the network system, and the various exceptions in the network system directly affect the normal operation of network services.

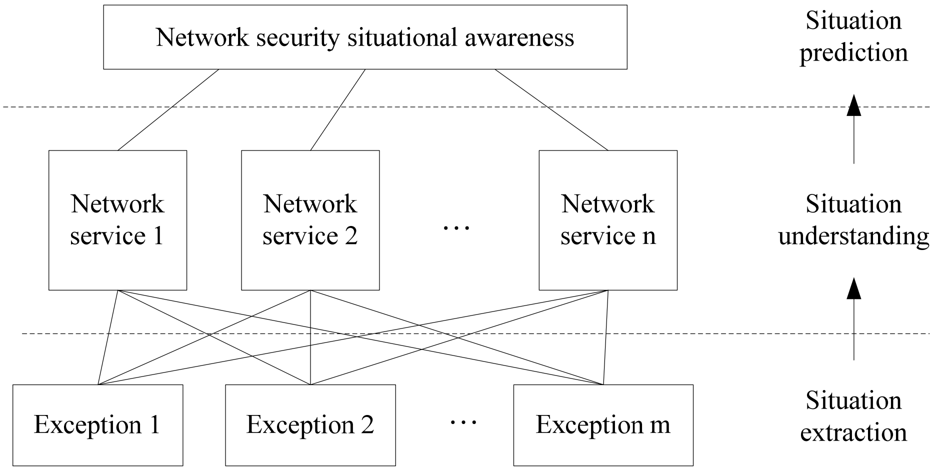

Fig.1 The layered model of network security situational

To evaluate the network security of the large scale network and analysis the influence of the network security by network attack, network security analysis and judgment must carried on according to the exception layer, network service layer and network security situational. Network security situational prediction depends on the network security situational value, which can be obtained by fusion the network security information, and the future network security situational can be drawn by the historical and current network security situational values. The model of network security situation prediction by WNN is shown in Fig.2.

The network security situation value obtained by all kinds of alarm can be abstracted as a function x of time t according to the process of network attacks and the nonlinear time sequence based on the alarm of security equipment. That is $x = f(t)$. Therefore, network security situation value can be considered as a time series processing. Assuming that the time series of network security situation value has been obtained as

$$x = \left\{ x_j \mid x_j \in R, j = 1, 2, \cdots, L \right\} \tag{1}$$

Then the network security situation prediction can be described as to predict the future M values according to the first N values. WNN can be acted as a nonlinear mapping medium to build up the prediction model [6] and the model of WNN prediction is shown in Fig.3.

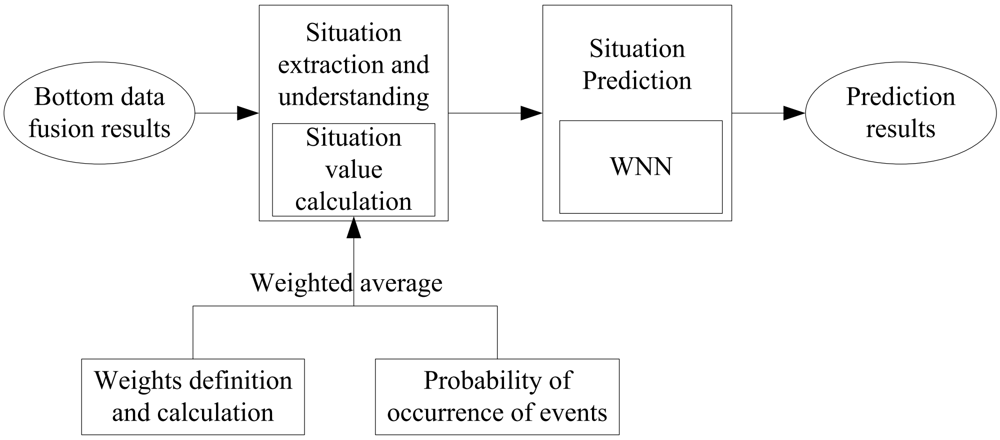
Bottom data fusion results
Situation extraction and understanding
Situation value calculation
Situation Prediction
WNN
Prediction results
Weighted average
Weights definition and calculation
Probability of occurrence of events

Fig.2 The model of network security situation prediction by WNN

In Fig.3, the input vector of WNN is x which denotes the network security situation value before time N . The output vector of WNN is y which denotes the network security situation value during the future time M . Then WNN establishes the nonlinear mapping $R^N \to R^M$. Where $\Psi(.)$ denotes wavelet transform and w_{ij} denotes the weights of WNN. Compared with the traditional BP neural network, the wavelet transform process is integrated into the hidden layer of WNN, which improved the convergence performance of the algorithm.

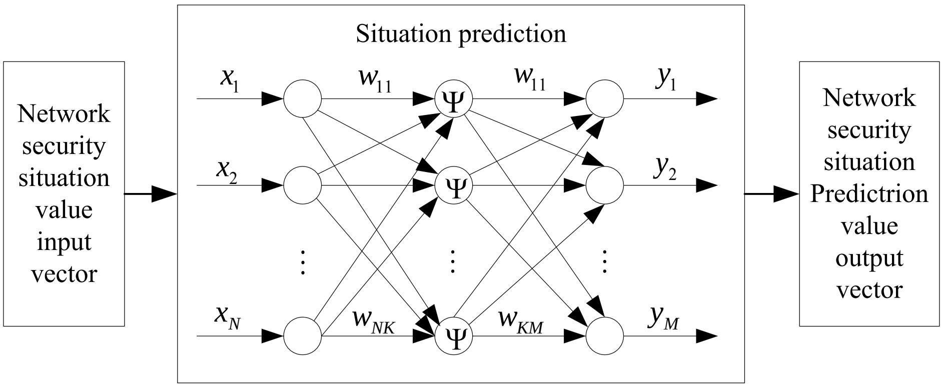
Situation prediction
Network security situation value input vector
x_1
x_2
x_N
w_{11}
w_{11}
w_{NK}
w_{KM}
Ψ
Ψ
Ψ
y_1
y_2
y_M
Network security situation Predictrion value output vector

Fig.3 The principle of network security situation prediction by WNN

Let the hidden layer input vector of the WNN is I_n （$n=1,2,\cdots,L$）, then the output of the hidden layer can be given by

$$\Psi_{a,b}(I_n)=\psi\left(\frac{I_n-b_n}{a_n}\right) \tag{2}$$

Morlet wavelet function is often acted as the hidden layer transfer function which is given by

$$\psi(x)=\left|a\right|^{\frac{1}{2}}\frac{x-b}{a}e^{-\frac{(x-b)^2}{2a}} \tag{3}$$

Where a and b is the scale factor and shift factor of the wavelet transform respectively. The object function of WNN can be given according to the mean square error criterion as follow:

$$J=\frac{1}{2}\left[\sum_{p=1}^{P}\sum_{j=1}^{M}\left(d_j^{(p)}-y_j^{(p)}\right)\right]^2 \tag{4}$$

Where $p=1,2,\cdots,L$ is the number of the training data sets. d_j （$j=1,2,\cdots,N$）is the network desired output. From Eq.4 can see that, the object function of WNN minimizes the total mean square error to achieve the training process. However the total mean square error reaches to the minimum is not equal to the output vector of WNN approach to the desired vector. That is WNN takes the traditional training method is more suitable for the statistical system. The network security situation prediction is a dynamic nonlinear system, the WNN using the traditional training method cannot obtain good performance prediction result, and the generalization performance is poor. Incremental learning can makes full use of new sample information, which can improve the generalization performance of WNN. Resource allocating network (RAN) algorithm is widely used incremental learning algorithm, RAN algorithm simulates the complexity of the function by adjustment of the hidden layer unit of neural network. The hidden layer unit is taken as isolated and the basis function is established by the criterion of the isolated point, and then the parameters of the neural network is trained according to least mean square error algorithm. This paper uses RAN algorithm to realize the incremental learning of WNN.

Test results

To verify the effectiveness of the network security situation prediction based on incremental WNN, the hacker attack data set collected by Honeynet organization [7] is adopted for simulation. For Honey net link to the Internet has not announced to the outside world, and it didn't trick hackers to attack, so the data collected by Honeynet organization can reflect the real attack by hackers, and using the Honeynet data set for network security situation prediction is reasonable. A period of 40 days Honeynet data is selected in the simulation, and the data is normalized according to the follow method. Fig.4 shows the normalized network security situation value.

$$\hat{x} = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{5}$$

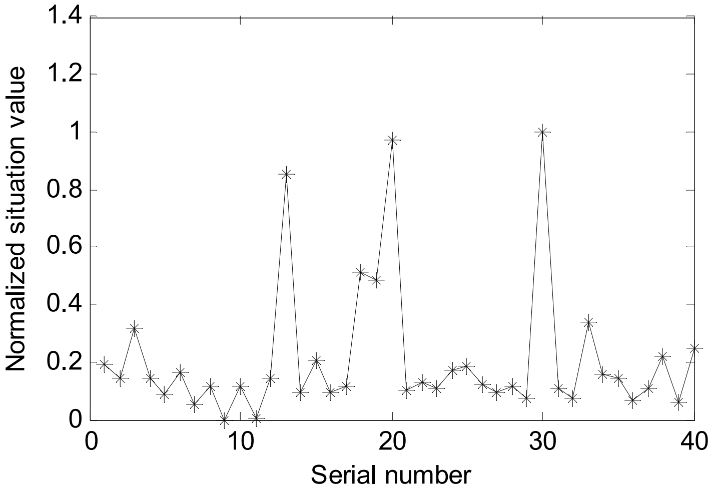

Fig. 4 The normalized network security situation value

In the training of the neural network, it uses the data of current day of the hacker attack to compute the current day's network security situation value. Let the input vector dimension of WNN is 3, that is, the network security situation prediction value depends on the network security situation value for 3 consecutive days. The output dimension of the WNN is 1, that is, it only predicts the future of the network security situation value for 1 day. After training, a week's network security situation value was taken as the test sample set to test the performance of the accuracy of the prediction result. Fig.5 shows the test result for 7 days network security situation value. The prediction results show that the network security situation prediction based on incremental WNN has high prediction accuracy. Meanwhile, by using the incremental learning algorithm, the generalization performance of the prediction method has been improved. As the network security situation prediction can be considered as a nonlinear mapping, the method proposed in this paper is practical.

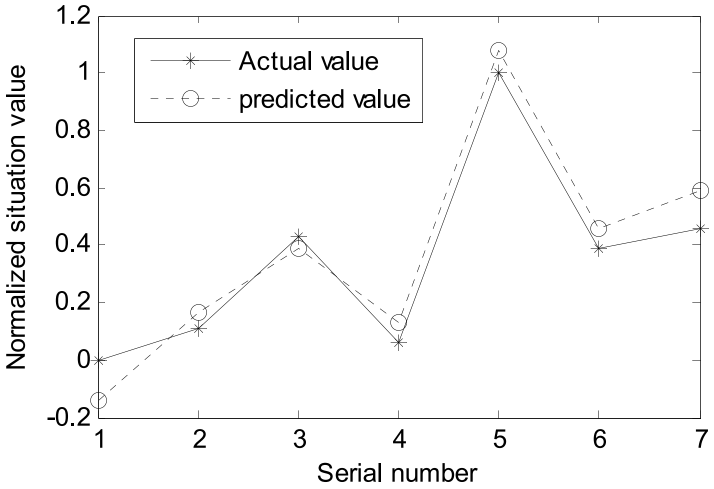

Fig.5 The network security situation prediction results

Conclusion

This work proposed a network security situation prediction method based on incremental WNN, in which the uncertainties of network security situation are fully considered, such as the change of network attack style, network protection technology and network scale, etc. The proposed method takes advantages of WNN and incremental learning algorithm, which can improve the convergence performance and the generalization performance at the same time. The simulation adopted the hacker attack data set collected by Honeynet organization and the results shows the effectiveness of the proposed method.

References

[1] LY T C. Multiple hypotheses situation assessment [C]. Proceedings of the 6th International Conference on Information Fusion, 2004: 972-978.

[2] FENG Zhaohui, FAN Ruijun, ZHANG Tong. Technology research and building example of Honeynet [J]. Computer Engineering, 2007, 33(5): 132-134.

[3] LIU Yuling, FENG Dengguo, LIAN Yifeng, et al. Network situation prediction method based on spatial-time dimension analysis [J]. Journal of Computer Research and Development, 2014, 51(8): 1681-1694.

[4] MENG Jin, MA Chi, HE Jialang, et al. Network security situation prediction model based on HHGA-RBF neural network [J]. Computer Science, 2011, 38(7): 70-72+75.

[5] WANG Geng, ZHANG Jinghui, WU Na. Application research on network security situation prediction method [J]. Computer Simulation, 2012, 29(2): 98-101.

[6] YING Guoliang, PAN Xianzhang, LI Huigui, et al. On forecasting traffic autoregression based on wavelet neural network [J]. Computer Application and Software, 2014, 31(6): 151-153+157.

[7] Honey net project know your enemy statistics [EB/OL], 2001-07-22. http://www. HoneyNetorg/papers/statis/.