Network Security Situation Prediction Method Based on MEA-BP

Pu Xiao, Ming Xian, Huimei Wang
College of Electronic Science and Engineering
National University of Defense Technology
Changsha, China

565250537@qq.com, qwertmingx@tom.com, freshcdwhm@163.com

***Abstract*—At present, network attacks on networks have become very complex.As the highest level of network security situation awareness, network security stuation prediction provides effective information for network administrators to makesecurityprotection strategy. Network analysis decision-makers not only need to understand, but also need to predict the current network security situation. In the field of network security, the study of network security situation prediction has become a hotspot. According to the characteristics of network security situation value of nonlinear time series, when BP algorithm is adopted, it has been applied to the problem of local optimal solution, multiple iterations and low efficiency. In order to overcome these shortcomings, this paper improves the positive effects, optimizes its weights and thresholds, and uses the MEA to develop a MEA-BP model to predict the network security situation. An example of case prediction is provided. The results show that this method can improve the accuracy and efficiency.**

Keywords: Network security; situation prediction; BP; MEA

I. INTRODUCTION

With the development of information technology, computer technology has been developing rapidly and widely. At the same time, network security attack devices become more and more diversified, and the traditional network security protection equipment or detection equipment can't meet the demand. Network security field of the most important research topics.

Because of the adaptability of neural network and the advantage of dealing with non-linear data, neural network-based prediction method is called the most widely used network security situation forecasting method.

Tang Chenghua combined the advantages of probability and BP neural network, designed a likelihood BP neural network to calculate the probability of a certain security event in the future[1].Then he proposed a method based on dynamic BP neural with covariance.The method can make full use of the characteristics of the network more complex, finer grain size, the higher the efficiency[2].

Ren Wei[3] finds the situation after the value of the first N data and M data of the non-linear mapping through the training RBF neural network, and then uses the relationship between the situation value prediction.

Xie Lixia[4] uses neural network to identify the nonlinear relationship, according to expert experience, by constantly adjusting the weights and thresholds to narrow the gap between the perceived results and the actual situation value, and then perceive the current security situation. And use RBF eural network learning, memory security elements and the future trend of non-linear relationship between the memory function through the given future situation.

Gan Wendao[5] proposed a model of network security situation prediction based on RAN-RBF.The model uses the algorithm of resource allocating network to cluster the samples of network security situation, and get the number of the hidden layer nodes of neural network, introducing pruning strategies to remove nodes that contribute little to the network, the neural network of centers, widths and the weights are optimized by modified particle swarm optimization(MPSO) algorithm, to predict the future network security situation.

This paper presents a method to predict the security situation of the BP neural network algorithm optimization based on mind evolutionary algorithm, the method of learning from the core part of BP neural network is mature, and the introduction of mind

978-1-5090-6218-8/17/$31.00 ©2017 IEEE

evolutionary algorithm is used to optimize the network parameters, the method is used for simulation of hacker attack data Honeynet tissue were collected, and the experimental results are error the analysis, which verifies the validity of the prediction method of network security situation.

II. NETWORK SECURITY SITUATION PREDICTION BASED ON MEA-BP MODEL

A. BP network

BP neural network belongs to the feedforward neural network, and adopts error back propagation algorithm to study. Data from the input layer input, through the hidden layer processing and finally reach the output layer output. However, a three-layer BP neural network can complete any n-dimensional to m-dimensional mapping by appropriately increasing the number of neurons, while the number of BP neural networks in multi-hidden layer Will increase a lot, so in practice, the general use of only one hidden layer of BP neural network.

The topological structure of BP neural network is shown in Figure.1

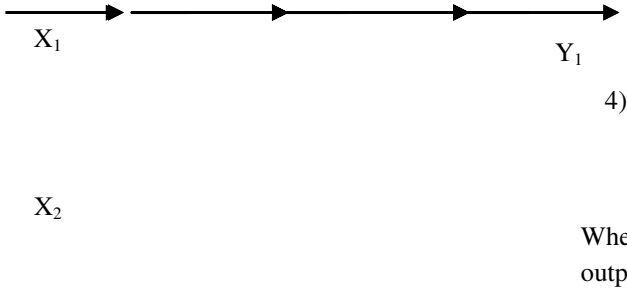

Figure.1 The topological structure of BP neural network

The three-layer neural network consists of input layer, hidden layer and output layer. The neurons of each layer are connected by weights and thresholds. There is no connection between neurons in the same layer. Its mapping and forecasting function is realized through the network training, the specific training process is as follows:

1) Initialize the network. The input weights n, the output dimension m and the number of implicit layer nodes l are initialized, and the connection weights ω_{ij} between the input layer and the hidden layer neurons are initialized, and the connection weight ω_{jk} between the hidden layer and output layer neurons. Initialized hidden layer threshold a, output layer threshold b, given learning rate and neuron activation function f (*).

2) Calculate the hidden layer output.

$$H_j = f\left(\sum_{i=1}^{n} \omega_{ij} x_i - a_j\right), j = 1,2,\mathrm{L}\ ,l \quad (1)$$

Where x_i is the input and f is the excitation function of the hidden layer. This function can be used in many ways, but it is usually a nonlinear function. The function selected in this paper is

$$f(x) = \frac{1}{1+e^{x}} \quad (2)$$

3) Calculate the output layer

$$Y_k = f\left(\sum_{j=1}^{l} H_j \omega_{ij} - b_k\right) \quad (3)$$

4) Error calculation

$$e_k = O_k - Y_k \quad (4)$$

Where O is the predicted output and Y is the desired output.

5) Weight update

$$\omega_{ij} = \omega_{ij} + \eta H_j (1 - H_j) x_i \sum_{k=1}^{m} \omega_{jk} e_k \quad (5)$$

$$b_k = b_k - e_k, k = 1,2,\mathrm{L}\ ,m \quad (6)$$

$$\omega_{jk} = \omega_{jk} + \eta H_j e_k \quad (7)$$

Where e is the error of network prediction and η is the learning rate.

6) Threshold update

$$a_j = a_j + H_j (1 - H_j) \sum_{k=1}^{m} \omega_{jk} e_k, j = 1,2.\mathrm{L}\ l \quad (8)$$

$$b_k = b_k - e_k, k = 1,2,\mathrm{L}\ ,m \quad (9)$$

978-1-5090-6218-8/17/$31.00 ©2017 IEEE

7) Determine whether the algorithm iteration reaches the

desired error or the maximum number of training times. If not, return to step 2).

B. The Mind Evolution Algorithm

Mind evolutionary algorithm (MEA) is a kind of evolutionary algorithm proposed By Sun Chengyi[6] in 1998. The system structure of the Mind Evolutionary Algorithm is shown in Figure.2.

Figure.2 The basic diagram of MEA

Here are some important concepts about MEA:

1) Groups and sub-groups.

In this paper, the evolution of MEA for each generation of all individuals in the collection Known as a group, this group will be subdivided into several sub-groups. Sub-groups are divided into sub-groups and temporary sub-groups.

2) Bulletin board. Bulletin board is equivalent to an information exchange platform, individuals and individuals, sub-groups and sub-groups are through the bulletin board for information exchange. The bulletin board is divided into a global bulletin board and a local bulletin board. There is a global bulletin board for publicizing the information of each

sub-group. There is a local bulletin board in each subgroup to announce the information of each individual in the group.

3) Convergence. Within the sub-group will compete in order to become a winner, the competition process known as convergence. A sign of the end of the convergence process is that no more winners are created within the sub-group.

4) Dissimilation:. Sub-groups compete in order to become winners. In the course of competition, some inferior sub-groups will be eliminated and the corresponding new sub-population will be detected in all solution spaces. This process is dissimilation.

C. The basic idea of the mind evolution algorithm

1) randomly generate a certain number of individuals in the solution space, search the highest scores of several winning individual and temporary individual.

2) Winning individuals and temporary individuals are the center, in each individual around to produce some new individuals, so as to obtain a number of winning sub-groups and temporary groups.

3) Perform convergence within the sub-population until the sub-population matures. And the score of the optimal individual in the sub-population is taken as the score of the sub-population.

4) After the sub-population is mature, the scores of each sub-group will be posted on the global bulletin board. The sub-groups will perform the dissimilation operation to complete the process of substituting and discarding the superior and temporary sub-groups. The global optimal individuals and their scores were calculated.

D. The improvement of the MEA-BP

1) According to BP neural network topology, the solution space is mapped to the coding space. The encoding length s is

$$s = nl + ml + l + m \quad (10)$$

2) Define the iterator iter, the population size (popsize), pre-allocate the winner sub-community

978-1-5090-6218-8/17/$31.00 ©2017 IEEE

(bestsize) and the temporary sub-community size (tempsize), the sub-population SG size is

$$SG = popsize(tempsize + bestsize) \quad (11)$$

3) Select the score function *val* for each individual and population.

$$val = 1/SE \quad (12)$$

$$SE = mse(T - A2) \quad (13)$$

Intheformula , A2 is the output value of the output layer after each iteration: T is the expected output; SE is the mean square error. Since the population needs to score the highest score, the fitness function *val* takes the expected value and the reciprocal of the mean square of the actual output value of each iteration. The design idea of MEA-BP shown in Figure.3.

III. EXPERIMENT AND ANALYSIS

A. *Situation value calculation*

The calculation of the situation value is the key of the network security situation assessment. In this paper, the reference[7] provides a quantitative calculation method, from the service layer. Host layer and system layer to calculate the value of network security situation.

Definition 1: denotes the security situation index of service in time period t, denoted as

$$F_{S_j}(t) = \sum_{i=1}^{n} N_i(t) \bullet 10^{D_i(t)} \quad (14)$$

In the formula, n is the type of attack that receives in t time; is the number of timesreceives the i attack in t time; is the harm level of the i attack to the receives.

Definition 2: denotes the security situation index of host in time period t, denoted as:

$$F_{H_k}(t) = \sum_{j=1}^{m} V_j(t) \bullet F_{S_j}(t) \quad (15)$$

Figure.3Design idea of MEA-BP

In the formula, m represents the number of services that host opens in t time; represents the service j's weight in all open services.

Definition 3: is the network security situation index at time t, denoted as:

$$F_L(t) = \sum_{k=1}^{c} W_k \bullet F_{H_k}(t) \quad (16)$$

In the formula, c represents the number of hosts in the network; represents the importance weight of the host k in the network.

B. *The pretreatment of historical load data*

In order to verify the validity and rationality of the model, Honeynet[8] collected hacking data set as the original experimental data source. After the original data set has been pretreated. According to the above-mentioned network security situation value calculation method, the situation value is calculated and simulated. In order to avoid the data directly

used for training and easy to produce large errors, the need to calculate the situation value normalized. The normalization formula is as follows:

978-1-5090-6218-8/17/$31.00 ©2017 IEEE

$$\hat{x} = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \quad (17)$$

Wheredenotethe normal , minimumandmaximumsafetysituationvalue. The normalized network security situation value is shown in Figure.4.

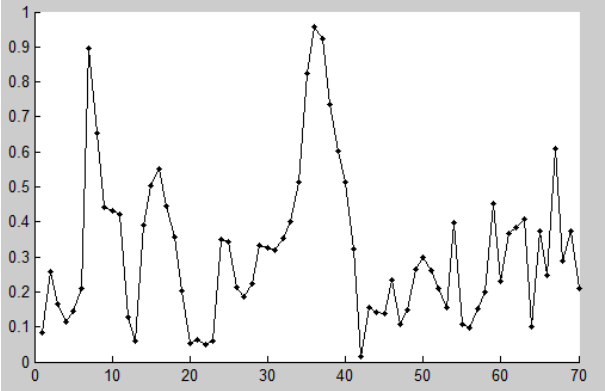

Figure.4 Normalized network security situation value sequence

C. *Experimental results and analysis*

In the experiment, the Honeynet data set of 70 days for a certain period of time is selected as the data source of the situation value calculation, and the situation value of the day is calculated by the attack data set of the day, then the total value of the situation value is obtained in 70 days. Using MEA-BP neural network after learning to predict the lastsevendays of network security situational data concentration.

Through the observation of Figure.5, we can clearly see that the prediction accuracy of network security situation value is higher with MEA-BP neural network.

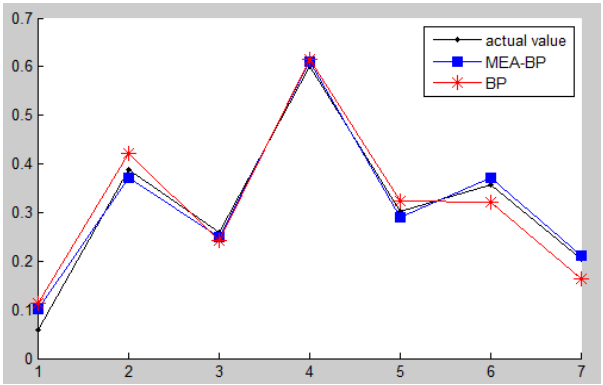

Figure. 5 Situation value prediction

IV. CONCLUSION

Network security situation assessment and prediction can reflect the security status of the network as a whole, find weaknesses and potential threats of the network system, and predict the future development trend of the network.This paper proposes an Network Security Situation Prediction model based on the MEA-BP network model. The active function is improved and the weights and thresholds of BP network are optimized using Mind Evolution Algorithm. Then the actual data of Honeynet is used as the samples to test results and verify the accuracy of the model. The simulation results indicate that the proposed method can improve the accuracy and the efficiency in prediction and has an important practical significance for Network Security Situation Prediction.

REFERENCES

[1] Tang Cheng-hua, Yu Shu-zheng. Method of Network Security Situation Prediction Based on Likelihood BP [J]. Computer Science, 2009, 36(11):96-100.

[2] TangChenghua, XieYi, QiangBaohua,Wang Xin, ZhangRuixia. Security Situation Prediction Based on Dynamic BP Neuralwith Covariance.Procedia Engineering, 2011,15,3313-3317

[3] Ren Wei , Jiang Xing-hao, Sun Tan-feng. RBFNN-based Prediction of Networks Security Situation. ComputerEngineering and Applications, 2006.31: 136-138.

[4] XIE Lixia, WANG Yachao, YU Jinbo. Network Situation Awareness based on Neutral Networks [J]. Tsinghua Univ(Sci&Tchnol), 2013, 53(12): 1750-1760.

[5] Gan Wendao, Zhou Cheng, Song Bo. Network Security Situation Prediction Model Based on RAN-RBF Neural Network.[J]. Computer Science, 2016, 43(11): 388-392.

[6] Sun Chengyi. Mind-Evolution-Based Machine Learning: Framework and The Implementation of Optimization, Proc. of IEEE Int. Conf. On Intelligent Engineering Systems (INES'98), Edts. P. Kopacek, IEEE Inc. ,Sept. 17-19, 1998, Vienna,Austria,pp.355-359.

[7] Chen Xiuzhen, Zheng Qinghua, Guan Xiaohong, Lin Cheguang. Quantitative Hierarchical Threat Evaluation Model for Network Security [J]. Journal of Software, 2006, 17(4): 885-897.

[8] Honeynet Project. Know your enemy. 2000 DARPA intrusion detection scenario specific data sets [EB/OL].[2014-12-26]. http://www.ll.mit.edu.

978-1-5090-6218-8/17/$31.00 ©2017 IEEE