Research and Implementation of Intrusion Detection Algorithm Based on BP Neural Network

Zhenzhen Wu
Weifang University of Science and Technology,
Shouguang 262700, China

ABSTRACT: The paper introduce the neural network technology in IDS model design, and study that neural network is successfully applied in intrusion detection, and gives a network of neural network based intrusion detection system model, expounds the design idea of the model, the model schematic diagram, and the principle of each module in the system model and give a detailed introduction. At last, through more objective analysis of the training process and detection process, the experimental results and experimental results are satisfactory, that is a great advantage in the network intrusion detection based on neural network.

KEYWORDS: Intrusion detection system; BP neural network; network security; feature extraction

1 INTRODUCTION

Internet and computer has become more and more widely used in today's society, corporations, governments and other organizations have become increasingly dependent on computer network system, so security becomes more and more prominent. Intrusion detection is a proactive security protection technology that provides real-time protection to internal attack, exterior attack and misoperation before the network is endangered interception and response to the intrusion. However with the diversity of intrusion technology, the traditional intrusion detection system (IDS) has been unable to meet the requirements of current network security. Therefore, for the means of the implementation of intrusion detection must be diversified, intelligent technology into intrusion detection system is the trend of the times.

The paper start from the basic concepts of intrusion detection, analyze existing IDS models and IDS intrusion detection methods, the shortcomings of these methods have found that the existing IDS products cannot meet the IDS need real-time character, adaptability, accuracy and the demand. By the research of neural network show that the neural network in the conception and method are suitable for intrusion detection system, research and design of intrusion detection system based on neural network will have important theoretical and practical significance. BP algorithm and neural network theory and its improved algorithm deduction and knowledge are described.

2 Overall scheme design for intrusion detection system

The system is dividing into the data packet capture module, data analysis module, pre-processing module, intrusion detection module (a neural network abuse intrusion detection module and neural network anomaly intrusion detection modules), and alarm module etc. The workflow between the modules is shown in Figure 1.

The function of each module in the system is described as follows:

1) Packet capture module

Packet capture module is responsible for each data packet capture network, and is sent into data analysis module by preliminary filter. First we set network interface into promiscuous mode, used to monitor the whole network data, and filter system required data, the data packets is sent into the data analysis module for further processing.

2) Data analysis module

We analyzed data from the packet capture module, check the IP packet format, if there is a patch, then the data is recombined. Then, the system judge it is IP packets, UDP or ICMP packet events according to the different packet protocol type and call analyzer program for semantic analysis, will meet the requirements of data package of information sent to pre-processing module.

3) Preprocessing module

Preprocessing module transforms the received data to identify the format by neural network and sent to the neural network learning and discrimination in the training phase the data format conversion (including expected output), and sent into the neural network, in the test phase will not determine the format conversion, also sent to the neural network.

4) Intrusion analysis module

Intrusion analysis module consists of a neural network misuse intrusion detection module and a neural network anomaly intrusion detection module. Neural network for misuse intrusion detection module is based on rules for intrusion detection method can detect the known attack; neural network anomaly intrusion detection module, establish the user normal behavior profile, beyond the contour deviation of intrusion detected in a certain range.

The system will abuse the intrusion detection and anomaly intrusion detection has the advantages of combining, to ensure maximum system detection accuracy, as much as possible to reduce the false positive rate and false negative rate.

5) Alarm module

The response module is the result of the synthetic classifier. When the test result is abnormal, first of all to show alarm information, alarm information includes: time, IP address, port, intrusion types, but at the same time, the discovery of new rules output to the rule database; when the intrusion level reaches a threshold, in addition to take alarm, the system take some active measures. When the detection result is normal, does not respond to a message.

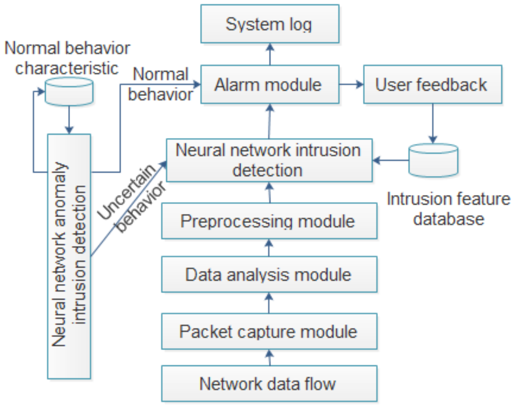

Fig.1 Intrusion detection overall scheme

3 Network intrusion model based on BP neural network

BP neural network is a feed-forward neural network, is currently used most widely used a neural network generally includes input layer, several hidden layer and the output layer three part, the network structure is as shown in Figure 2.

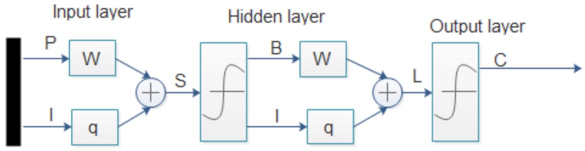

Fig.2 BP neural network algorithm

BP neural network algorithm is a supervised learning algorithm, the main idea is by using a gradient search technique known network intrusion samples for learning, and ultimate goal is the minimum error between network the actual output value and the expected output value of the mean square value. In the learning process of BP neural network, the input signal from the input layer through the hidden unit layer by layer processing, and to the B P neural network output layer, each layer B P neurons affects only a layer of neurons. If in the BP neural network output layer cannot get the desired output, then to be BP neural network backpropagation output error signal along the original connection pathway back, through continuous adjust the weights of the neurons in each layer, finally to the mean square value of the minimum error. The basic learning process is as follows:

1) Initialize the PB neural network state. Initial value of network connection weights of w ij , v jt and threshold θ j and γ t

2) Enter first P B neural network learning sample pairs;

3) Calculate input u j and output h j of each neuron intermediate layers. Using the following formula:

$$u_j = \sum_{i=1}^{n} W_{ij} X_i - \theta_j \tag{1}$$

$$h_j = f(u_j) = \frac{1}{1+\exp(-u_j)} \tag{2}$$

4) Calculate input lt and output y t of each neuron output layers. That is:

$$I_t = \sum V_{jt} h_j - \gamma_t \tag{3}$$

$$y_t = \frac{1}{1+\exp(-I_t)} \tag{4}$$

5) Calculate weighted error δ t that BP neural network is connected to the output layer of neural cells, i.e.

$$\delta_t = (c_t - y_t) y_t (1 - y_t) \tag{5}$$

Among them, tc said the expected value of the sample.

6) Calculate weighted error δj that BP neural network is connected to the middle layer of neural cells, i.e.

$$\delta_j = \sum_{t=1}^{q} \delta_t V_{jt} h_j (1 - h_j) \tag{6}$$

7) Update to the B P neural network connection weights and threshold value vjt and γ t, i.e.

$$V_{jt}(N+1) = V_{jt}(N) + \alpha \delta_t h_j \tag{7}$$

$$\gamma_t(N+1) = \gamma_t(N) + \beta \delta \tag{8}$$

8) Update to the B P neural network connection weights and threshold w j t and θ j value, i.e.

$$W_{jt}(N+1) = W_{jt}(N) + \alpha \delta_j X_i \tag{9}$$

$$\theta_j(N+1) = \theta_j(N) + \beta \delta_j \tag{10}$$

9) Enter the next sample of learning, jump to step 3), repeated one to all samples of the training is completed.

10) To be learn and train a new round of B P neural network, if the following conditions, then the training completed.

$$\left| \sum_{k=1}^{z} E_k \right| \le \varepsilon \tag{11}$$

Among them, ε represents a preset accuracy, that Ek represents square error, i.e.

$$E_k = \frac{1}{2} \sum_{t=1}^{q} (c_t - y_t)^2 \tag{12}$$

4 Application of P B neural networks in network intrusion detection

4. 1 Experimental environment

The network intrusion detection system run in window S2000 server platform, hardware environment: P4 3.0, 2G memory, 200g hard drive. Database is SQL2000 SERVER, BP neural network toolbox is matlab7.0 and genetic algorithm toolbox.

4.2 Simulation data

The simulation experiment data use KDDCUP99 data network. The KDDCUP99 data set contains the normal data and abnormal data, including large network intrusion behavior: denial of service attack (DOS); unauthorized superuser privileges attack (U2R)); remote unauthorized access r2l attacks; vulnerability detection and scanning attacks (PROBING). KDDCUP99 data set contains a total of 4898431 original data, using Q s L2000 database technology to delete duplicate records, the 1074992 effective data, the distribution is:

normal is 812, 814, DOS attacks have 247267, R2L attacks have 999, u 2R attacks have 52, PROBING attack is 13860.

4.3 Experimental results and analysis

In order to reflect the genetic algorithm is proposed to optimize the neural network in network intrusion detection performance. In this paper, the standard BP neural network algorithm, genetic algorithm and the algorithm were compared. Comparative experimental results are shown in Table 1 below. Table 1 is given to PROBING, DOS, u2r and r2l, blended attacks and new attack detection rate and correct rate and false negative rate.

Table 1 Comparison of test results for various algorithms

Attack type	BP neural network algorithm			Genetic algorithm			My algorithm		
	D (%)	C (%)	F (%)	D (%)	C (%)	F (%)	D (%)	C (%)	F (%)
D0S	88.7	60.5	11.3	77.8	53	22.2	93.2	63.6	6.8
PROBNG	89.5	67.4	10.5	78.5	59.1	21.5	94.1	70.8	5.9
U2R	20.7	15.8	79.3	18.1	13.9	81.9	21.8	16.6	78.2
R2L	25.8	21.6	74.2	22.6	18.9	77.4	27.1	22.7	72.9
Hybrid attack	15.6	12.5	84.4	13.7	11	86.3	16.4	13.1	83.6
New attack	12.1	9.15	87.9	10.6	8	89.4	12.7	9.6	87.3

D: Detection rate; C: Correct rate; F: rate of missing report

From table 1 test results show, the B P neural network detection based on genetic optimize algorithm in the paper have small time, fast convergence speed, at the same time, to significantly improve the network attack detection rate and accuracy rate, false negative rate is low. It is proved that the genetic algorithm optimization of B P neural network intrusion detection performance has been significantly improved via. Hence, it can be concluded, this algorithm combines the advantages of genetic algorithm and B P neural network algorithms are both, in a certain extent, overcomes the shortcomings of them, improve the network intrusion detection system detection performance.

5 Conclusions

Aim at current network intrusion detection system that have low detection rate and high false negative rate and the problem have the low efficiency of the detection system, this paper carefully analyzed the advantages and disadvantages based on the BP neural network in network intrusion detection system, analyzed the B P neural network training algorithm that is not easy to convergence and local minimum problem under the full use of the advantages of B P neural network, and put forward the has strong global search ability for genetic algorithm were optimized algorithm parameters of BP neural network. The simulation results show that, network intrusion detection system use genetic algorithm to optimize the BP neural network have high detection rate, false positive rate have greatly improved, efficiency can be improved compared with the traditional BP neural network algorithm.

Reference

[1] Mu Chengpo, Huang Houkuan, Tian Shengfeng. Intrusion detection alert aggregation and related technology review [J]. *Computer research and development*, 43, 2006 (1): 1 -8.

[2] Zhou Quan, Wang Chongjun. Several methods of network intrusion detection based on artificial intelligence technology [J]. *Computer application research*, 24, 2007 (5): 144 -148.

[3] Yang Zhijun, et al. Overview of Intrusion Detection Technology [J]. *Computer engineering and design*, 2006, 27 (12): 2119 -2123.

[4] Song Ge, Yan Qiao. The application of neural network in anomaly detection [J]. *Computer engineering and application*, 2002, 18: 146 -148.