International Journal of Security and Its Applications
Vol. 9, No. 4 (2015), pp. 247-258
http://dx.doi.org/10.14257/ijsia.2015.9.4.23

Research on Intrusion Detection Algorithm Based on BP Neural Network

[1] Chunmin Qiu, [2] Jie Shan

[1, First Author] *Binzhou Polytechnic, Binzhou Shandong,256603,China,*
E-mail: bzqcm@163.com
[*2,Corresponding Author] *Binzhou Polytechnic, Binzhou Shandong,256603,China,*
E-mail: shanjie828@163.com

Abstract

In recent years, the problem of network security has been more and more people's attention, as one of the most important technology of network security, intrusion detection technology has gone through nearly thirty years of development, but it still exists some deficiency factors. Aiming at the defects of the traditional BP neural network intrusion detection model in the detection rate and the convergence speed, the improved PSO-BP neural network is applied to intrusion detection system model in this paper. Experimental and simulation, verifying the improved effect of system in the false negative rate, false positives rate and convergence speed of. Detailed analysis of the standard BP neural network algorithm and improved way of common, including gradient descent algorithm and additional momentum algorithm. Local search capability of BP neural network and the global search ability of particle swarm optimization , we have a detailed description of the PSO algorithm is applied to the case of BP neural network and discusses the improved PSO-BP neural network algorithm flow.

Keywords*: Intrusion Detection , BP Neural Network ,PSO Algorithm*

1. Introduction

With the rapid development of computer technology, network communications and information industry, information technology and networks in various fields of science and education in today's society , economy, culture and e-commerce has a very large contribution. However, as society relies on computer networks increasingly, once when computer network security was damaged, it will not only disrupt the order of the whole society, but it will also bring huge economic losses. Due to computer network security has become a hot research, the network intrusion detection technology is an important part of network security technology , so the study of network intrusion detection technology adapt to contemporary needs of our country .

In recent years, the Internet, online information and application is increasing, the network has more and more influence on the whole society, so we need a series of more perfect network security technology to support, in today's network security technology market, many network security products are based on passive protection is given priority to prevention technology. Because the traditional network security technology is given priority to with protection[1], it cannot satisfy the current trend which the development of the large scale and complicated network, therefore, in network intrusion produced prevention is active protection technology .Network intrusion detection system is based on the concept of dynamic and change, the implementation can improve the performance against the attack of network and information system, in order to ensure that the network information data

ISSN: 1738-9976 IJSIA

confidentiality, data integrity, information availability, controllability, and non-repudiation.

With the establishment and development of the Internet, the development of the world's economic, political, and social is inseparable from the network. At present, China's Internet users and the number of broadband Internet came second in the world, more and more computer users can never leave home to access to the global network to provide rich information resources, the Internet users in the home or the company can through the Internet to send and receive E-mail, online entertainment, network call, e-commerce transactions on the Internet[2], and bank transfer, etc. Online login process only identify data information ,and deny user, if the network security is not good, the attacker through stealing the related user account and password to get the corresponding system permissions, doing illegal operation, it will cause great losses to the user. Even military network system whose security is tight also has attacked many times. In recent years, computer viruses, Trojan attack has caused great harm, classic virus damage events have caused loss amount over billions dollars. Numerous events show that the network information security is facing a big challenge in the 21st century, it has become a key problem restricting the development of global informationization, and needed to be solved.

In recent years, neural networks begin to apply to intrusion detection technology. Neural network is a kind of engineering system based on the understanding of brain tissue structure and running wit to simulate its structure and intelligent behavior[3]. In the 1930s, psychologist McCulloch, mathematician Pitts proposed the first mathematical model of artificial neural network, which has pioneered the research of theoretical neuroscience. Subsequently, F. Rosenblat, Widrow and Hopf, J. J. Hopfield and other scholars also proposed successively multilayer apperceive model, so that the artificial neural network technology begin to flourish. Research and application of more than half a century, it is not difficult to see that neural network because of its self-learning and adaptive, self-organizing, function approximation and the large-scale parallel processing ability, so it has strong vitality and has been widely used in pattern recognition, signal processing, detection and analysis system and optimization fields, at the same time neural network intrusion application research testing has also made great progress.

2. Related Research

After the 1970s, with the rapid development of large-scale and ultra large scale integrated circuits, high-performance computer becomes smaller, widely used in various fields of social life, thus increasing demand for computer security. The traditional firewall is difficult to meet the network hacker intrusion attack, so the intrusion detection technology is also on the application stage. It has gone through four research stages, respectively is: the early studies, host-based intrusion detection system research, based on the network intrusion detection system research and study of the intelligent network intrusion detection system based on.

(1) The early studies

In 1980, JamesAnderson write a confidential customer technical report, audit records can be used to identify the computer misuse. He thought the audit records can analyze surveillance intrusion behavior, and classify intrusion behavior.

In 1983, SRI (Stanford Research Institue) using statistical methods to analyze IBM mainframe SMF (System Records Management Facility), it is early to intrusion detection research. Because there was no connection between the network completely, so the research on intrusion detection basically based on analysis of the host of the event log.

(2) The study of host-based intrusion detection

Published in 1986, SRI Dorothy e. Denning (An Instrusion Detection Model), this paper discusses the intrusion Detection technology, for the first time the concept of intrusion Detection for computer network defense measures is put forward, and set up general intrusion detection system model, it is independent of the system[4], program application environment.

In 1989 , Los Alamos national laboratory experts in the national computer security center and the department of energy development W&S (Widsom and Sence) system, which is based on a host of anomaly detection systems.

Until 2001, SRI issued expert. BSM for Solaris, is currently the more advanced host-based intrusion detection system, it has a large number of events analysis ability, strong portability, support pluggable components etc.

(3) the study of network-based intrusion detection

With the continuous development of network technology[5][6], the original host-based intrusion detection systems are difficult to apply to a network of distributed systems, because network-based intrusion detection have also been developed.

Network security monitor that appeared in 1990, is a local area network (LAN) design of intrusion detection system, it is used to analysis a LAN packets, and detect attacks.

1996 to 1999, SRI began to study NIDES, it has a distributed and scalable new features for large networks to detect malicious intrusions, and automatically respond.

(4) based on intelligent network intrusion detection system research

Due to the continuous development of network technology, network packets based on the network intrusion detection system of large amount of data and real-time requirement is strong, but the traditional mode of network intrusion detection technology is difficult to adapt to. So intelligent intrusion detection system also will be born.

Since the early 1990s, data mining, artificial immune, neural networks, information retrieval, or fault-tolerant technology continues to penetrate into the network intrusion detection system, will push the development of network intrusion detection systems to a new height.

In the 21st century, with the common development in the field of intrusion detection technology and other disciplines, all kinds of new technology and new intrusion detection model are put forward. Many foreign countries invested heavily in supporting network security laboratory research and development of intrusion detection systems. Most of the intrusion detection system can be divided into intrusion detection system based on network, host-based intrusion detection systems and intrusion detection system based on host and network. The foreign representative products include ISS Rea ｜ Secure, Axent company Intruder Alert and NetProwler, Cisco NetRanger, open source Snort intrusion detection system, AAFID autonomous agents intrusion detection system, and so on. At present, purdue university and the university of force mouth, Davis, los alamos national laboratory, Columbia University, university of new Mexico and other institutions in the research represents the highest level of the current.

At present, research in this area of detection in Network Intrusion slower than abroad, mid and late 1980 s, led by Samuel way stage of the official start of the computer security professional committee of China computer society activities. After that, many domestic experts and scholars have also involved in research and development of network intrusion detection technologies, the state of Intrusion Detection has invested a lot of manpower and resources, and promote the

development of computer network security. Domestic computer network security companies have also research and development, including: "eye" network intrusion detection system is Beijing zhongke wangwei corporation information technology co., LTD., the development of real-time intrusion detection system based on network, hetian "day" hacker intrusion detection system is made up of stars qiming information technology co., LTD., on its own research and development of intrusion detection and response system based on dynamic, the eye of the "ice" network intrusion detection system is a green union technology co., LTD. Let the network intrusion detection of hair products, rising RIDS - 100 intrusion detection system is by the company independent research and development of network security products, which combines intrusion detection, network management, network monitoring functions in one. Do get a lot of intrusion detection technology to progress in China, in recent years have been able to keep pace with the international level.

The brain is made up of a large number of neurons after complex interconnected to form a highly complex, nonlinear, parallel processing of information system. It enables the human to quickly absorb a lot of information from the outside environment, and the processing, storage, making all kinds of response to changes in the environment in a timely manner, and constantly learn from the environment[7], so as to improve the human ability to adapt. All depends on the material base of the brain, neural network.

In 1984, the simulated annealing algorithm, introduced Hinton and others, and use method and the concept of statistical physics, puts forward the Boltzman machine model and shows that the multi-layer network also can be trained. 1986 Rumelart famous back propagation (BP) algorithm is proposed[8], solved the multilayer network by the learning difficulty of the problems of hidden layer, thus the development of neural network, especially the multilayer network plays a great role in promoting. Two years later Rumelhart and McClelland also constructed multi-feedback learning algorithm [9], has successfully solved the single hidden layer cognitive network "XOR problem" and other identifying problems, it is once again set off artificial neural research boom of the network.

In the same year, Chum and Yallg proposed cellular neural networks (CNN) models. The network has dynamic characteristics of cellular automata, and is a large-scale computer simulation systems. Largely contributed to the development of neural network theory.

By 1990, Elman for speech processing problems put forward a kind of typical local regression network, BI ^ Elman neural network. Its characteristic is in a layer more than BP network and as a step delay operator, in order to achieve the purpose of memory. Such networks can be thought of as one who has a partial memory unit and the forward neural network of local feedback connection. Angeline in 1994 on the basis of predecessors' theory of evolution strategy, such as an evolutionary algorithm is proposed to establish the feedback neural network, and has been successfully used in pattern recognition, automatic control, etc. At the same time, Wan a FIR (FiniteImpluse Response) neural network, the FIR neural network is more similar to the improvement of standard multilayer neural networks, a time-varying, vector quantization and more satisfied to adapt to the characteristics and other characteristics, is mainly used for time series prediction. In 1995, Mitra the artificial neural network and fuzzy logic theory, combined with biological cell theory and probability theory, a fuzzy neural network is proposed. This kind of neural network is put forward, make the research of the neural network has made breakthrough progress[10]. After that, Jenkins et al. Study optical neural network, established a two-dimensional parallel optical interconnection and electronics hybrid optical neural network, it can avoid network into a local minimum value, and can

last at or near optimal solution; Sole fluid neural network is put forward, such as used to study the insect community, collective robot the immune system, inspired people use mixed pure theoretical analysis system. 1996, Shuai JW simulation of the human brain, such as the development of behavior, on the basis of mixed pure neural network were discussed from the development of neural network is proposed. More signs show that artificial neural network is a fast-growing emerging discipline, the new model, new theory, new applications are endless[11]. Neural network with its parallel processing, distributed storage, good adaptive and self-learning features for the application of it in the field of control has opened up broad prospects, especially it can learn by input and output data with the characteristic of the nonlinear function approximation, the theory become a very important technology in modern control theory and method.

The research status at home and abroad to a certain extent, shows the intrusion detection technology put forward some new models, and improve the detection ability of intrusion detection system in different degrees, response ability, application ability of intrusion behavior on a large scale. But in these solutions, there are still some problems:

(1) False positives rate, false negative rate are high

Commonly used detection method for intrusion detection system have characteristics detection, anomaly detection [12] , the state detection, protocol analysis. These detection methods have defects. For example anomaly detection commonly used statistical methods to detect, and statistical methods can not effectively determine the threshold, if the value is too small ,so it will generate a lot of false positives, but the value is too large ,it will generate a lot of false negatives. In the detection method using protocol analysis, in general, intrusion detection systems simply deal with the commonly used as HTTP, TCP, FTP , etc., other protocol packets may cause false intrusion detection systems , if considering to support multi- protocol type analysis as much as possible, then the cost of network testing will be unbearable .

(2) The lack of accurate positioning and handling mechanism

Intrusion detection technology can only identify the IP address , unable to locate the IP address , and it can not identify the data source. Intrusion detection system at the time of the attacks detected , only can across a small number of ports, including the closing network outlet and the server [13], but it will also affect other normal users. Therefore, the effective response processing mechanism is quite scarce.

(3) Performance is generally inadequate

Intrusion Detection System products now on the market are mostly used in traditional detection techniques , such intrusion detection systems cannot meet the exchange of technology and product development of high -bandwidth environment , the impact of the large flow , multi- IP fragmentation circumstances may cause collapse or loss of invasion detection system.

3 Proposed Scheme

3.1 Research of BP Neural Network Algorithm

Multilayer perceptrons (MLP) is composed of input layer, hidden layer (a layer or multilayer) and output layer. The excitation mode of each source node (input vector) units of multilayer feedforward neural network input layer applied to the second layer (such as the first hidden layer) neurons (compute nodes) of the input signal ,the output signal of the second layer becomes the input of the third layer, similar to the remaining layers. Neurons in each layer contains only as their input

that output signal of the previous layer, the output signal of network output layer (stop layer) consisting of all the neurons which the source node of the input layer (the initial layer) generated the excitation model .That is the signal from the input layer, from the hidden layer transmitted to the output layer, and we will obtain the output signal from the output layer.

In the external input sample stimuli, neural networks changed network connection weights, in order to make the output of the network constantly close to the desired output.

BP neural network learning process:

(1) Operating signal forward propagation: an input signal from the input layer through the hidden units, transmitted to the output layer, produced an output signal at the output , which is a positive propagation of the work signal .During the forward pass, the network weights are fixed , the state of neurons in each layer is only effect the state of next layer neuron.

(2) The error signal back propagation: the difference between the actual network output and the desired output is the error signal , the error signal begins to propagate from the output terminal step by step back , which is reverse spread of the error signal. In the process of back-propagation of error signals, the network weights were adjusted by the error feedback . For example, BP network which contains three hidden layer.

BP neural network in the stimulation of the external input samples changing network connection weights, in order to make the output of the network constantly close to the desired output , the input layer has n neurons , the hidden layer has p neurons, the output layer has q neurons .

Variables are defined as follows :

Input vector : $X=(x_1,x_2,...,x_n)$

Hidden layer input vector : $hi=(hi_1,hi_2,...,hi_p)$

Hidden layer output vector : $ho=(ho_1,ho_2,...,ho_p)$

Output layer input vectors: $yi=(yi_1,yi_2,...,yi_p)$

Output layer output vector : $yo=(yo_1,yo_2,...,yo_p)$

Desired output vector : $d_0=(d_1,d_2,...,d_q)$

The connection weights of the input layer and the intermediate layer : w_{ih}

The connection weights of the hidden layer and the output layer : w_{ho}

Hidden layer neuron threshold: b_h

Output layer neuron threshold: b_0

The number of sample data : $k=1,2,...m$

Error function as shown in equation 1 :

$$e=\frac{1}{2}\sum_{o=1}^{q}\left(d_0(k)-yo_0(k)\right)^2 \qquad (1)$$

BP neural network learning procedure is as follows :

First, the network initialization, each connection weights were assigned a range of random numbers (-1, 1), and set the error function e, given the precision value S and the maximum number of learning M;

Second, randomly selecting sample of the k th input and the corresponding desired output ;

$$x(k)=(x_1(k),x_2(k),...,x_n(k)) \qquad (2)$$

$$d_0(k)=(d_1(k),d_2(k),...,d_q(k)) \qquad (3)$$

The third step, calculating input and output of each hidden layer neuron;

$$ho_h(k) = f(hi_h(k)) \quad h = 1,2,...,p \tag{4}$$

$$yo_h(k) = f(yi_h(k)) \quad o = 1,2,...,q \tag{5}$$

The fourth step, using the network desired output and the actual output , calculating the partial derivative $\delta_0(k)$ of the error function for each neuron output layer

$$\frac{\partial yi_0(k)}{\partial w_{ho}} = \frac{\partial\left(\sum_h^p w_{ho} ho_h - b_0\right)}{\partial w_{ho}} = ho_h(k) \tag{6}$$

The fifth step , using the connection weights of hidden layer to the output layer, $\delta_0(k)$ of the output layer, and the output error function of the hidden layer to partial derivatives of hidden layer neurons $\delta_h(k)$;

The sixth step, using $\delta_0(k)$ of the output layer neurons and the output correct connection weights of each hidden layer neuron ;

$$w_{ho}^{N+1} = w_{ho}^N + \eta\delta_0(k) ho_h(k) \tag{7}$$

The seventh step , using $\delta_h(k)$ of hidden layer neurons and the input correction connection weights of each input layer neurons ;

The eighth step , calculating the global error ;

$$E = \frac{1}{2m}\sum_{k=1}^{m}\sum_{o=1}^{q}(d_0(k) - y_0(k))^2 \tag{8}$$

The ninth step , determining network error meets the requirements or not. When the error reaches a preset accuracy or learning time larger than the setting maximum times, the algorithm ends . Otherwise , selecting the next learning samples and corresponding desired output , returns to the third step, the next round of learning .

3.2 MPSO_BP neural networks intrusion detection

Based on the study on PSO algorithm , we presents an improved algorithm of MPSO and MPSO optimization algorithm with BP neural network , this paper presents an intrusion detection model based on neural network MPSO_BP : MPBIDS models. The model advantages : the ability to monitor the entire network segment timely; can handle massive amounts of data , improving the efficiency of intrusion detection ; has the capable of autonomous learning , updating the regular database ; able to adapt to the needs of today's networks of distributed intrusion detection system .

We proposed intrusion detection model MPBIDS shown in Fig.1. The model can be divided into six parts: data acquisition module, data preprocessing module, a rule base module , MPSO_BP neural network module , response and alarm module and normal events.

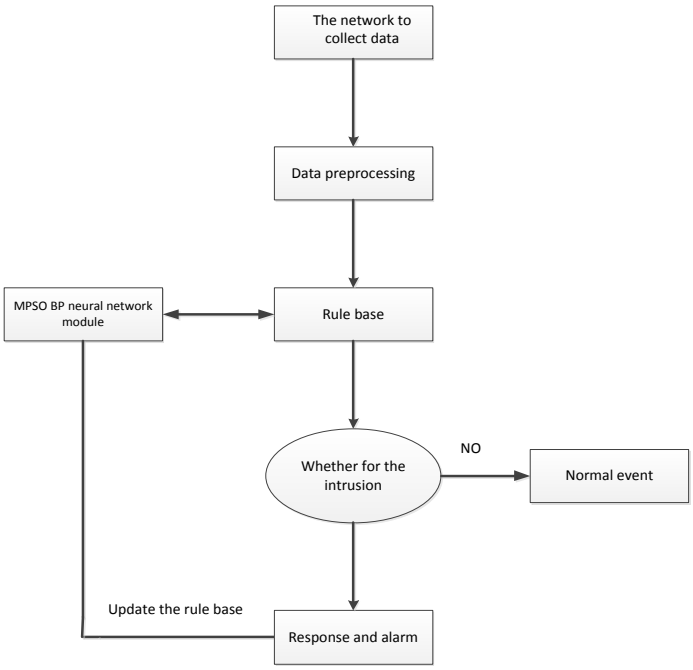

Figure 1. A Neural Network Intrusion Detection Model based on MPSO_BP

Where:

(1) Data Acquisition Module: mainly responsible for collecting network data .

(2) Data preprocessing module : mainly responsible for the processing of the raw data to the network , the network of the original data into the neural network can recognize data

(3) the rule base : saving the rule by the neural network module obtained .

(4) MPSO_BP neural network modules: the core function of the whole intrusion detection system by the module for data processing , developing a new rule base , and achieving intrusion detection system which has self-learning function.

(5) Response and alarm modules: the behavior of contrary to the intrusion detection rules base, taking appropriate measures or corresponding alarm in accordance with the response of user-defined , including the alarm is displayed on the screen , sound an alarm , paging and e-mail notification reconfigure routers or firewalls , and closing the connection .

(6) Normal event : the event that detected by the rule base, and did not cause harm to the system .

2. Related Research

(1) False positives rate, false negative rate are high

Commonly used detection method for intrusion detection system have characteristics detection, anomaly detection , the state detection, protocol analysis. These detection methods have defects. For example anomaly detection commonly used statistical methods to detect , and statistical methods can not effectively determine the threshold , if the value is too small ,so it will generate a lot of false positives, but the value is too large ,it will generate a lot of false negatives. In the detection method using protocol analysis, in general, intrusion detection systems simply deal with the commonly used as HTTP, TCP, FTP , etc., other protocol packets may cause false intrusion detection systems , if considering to support multi-

protocol type analysis as much as possible, then the cost of network testing will be unbearable .

(2) The lack of accurate positioning and handling mechanism

Intrusion detection technology can only identify the IP address , unable to locate the IP address , and it can not identify the data source. Intrusion detection system at the time of the attacks detected , only can across a small number of ports, including the closing network outlet and the server , but it will also affect other normal users. Therefore, the effective response processing mechanism is quite scarce.

(3) Performance is generally inadequate

Intrusion Detection System products now on the market are mostly used in traditional detection techniques , such intrusion detection systems can not meet the exchange of technology and product development of high -bandwidth environment , the impact of the large flow , multi- IP fragmentation circumstances may cause collapse or loss of invasion detection system.

4 Experimental Results and Analysis

The purpose of this experiment is to test detection rate and false positives rate of this article proposed MPBIDS. The configuration of computer used in the experiment is Intel Core Duo T6600 @ 2.20GHz, 2GB memory, 500G hard drive. Operating system is Windows Server 2003R2, the programming language selected C ++, simulation environment using Matlab2010, experimental data set using KDD CUP99.

4.1 IDS Performance Indicators

In order to evaluate the performance of intrusion detection model, the main consideration statistic associated with the intrusion detection performance : detection rate and false positives rate.

(1) False positives rate is the probability of the system looks the normal behavior as abnormal behavior and conduct alarms.

False positives rate = the number of false alarms / (the total number of normal behavior samples + the total number of attack samples)

(2) Detection rate means that the probability of when the host and network suffer intrusion , the system can properly alarms.

Detection rate = the number of intrusion alarm /the number of intrusion attraction rate

The two evaluations can fully reflect the intrusion detection capabilities of the algorithm , and the system can make the evaluation to correct classification which the number of detection and the number of attack , from this we can see, a good intrusion detection model should make the detection rate as large as possible, and the false positives rate as low as possible .

4.2 Performance Testing

The researchers proposed the algorithm based on the classic PSO_BP IDS model, and IDS model based on BP algorithm. In order to test the performance of MPSO_BP algorithm based IDS model, and ensure the effectiveness and fairness of the experiment, in the experiment , compared above two algorithms with the proposed algorithm used a unified detection model , namely single neural network detection model . Network input data fed into the neural network, by detection of the neural network, we determine the type of the network , and then compared with the actual data types , thereby obtaining detection results of specific neural network .

We selected 4 test groups sample data sets , each data set with 1200 records as the test data set , which contains 1000 normal records and 200 invasion records. 4 sample data have different number of types of attack, and we can test the ability to detect attacks of three different algorithms. As shown in Tab.1 .

Table 1. The Specific Description of the Sample Data Set

Test set	normal	DOS	R2L	U2R	Probing
Test set 1	1000	60	40	50	50
Test set 2	1000	75	25	40	60
Test set 3	1000	80	20	30	70
Test set 4	1000	90	10	20	80

In the experiment, using the same sample, the three algorithms for comparison testing ,respectively. After the experiment, the results obtained are shown in Tab 2 and 3 :

Table 2. The Intrusion Detection Comparison of Three Methods

algorithm	MPSO-BP		PSO-BP		BP	
Test set	detection rate	False positives rate	detection rate	False positives rate	detection rate	False positives rate
Test set 1	85.74%	1.92%	84.54%	2.57%	83.58%	3.45%
Test set 2	89.36%	1.43%	87.36%	2.38%	86.32%	2.62%
Test set 2	94.45%	0.81%	92.51%	1.29%	90.41%	1.73%
Test set 4	96.73%	0.39%	94.29%	0.85%	93.27%	1.32%

By analyzing the data in Tab 2. As can be seen , MPSO_BP proposed algorithm uses an improved PSO algorithm, it optimized the parameters of BP neural network, under the same conditions , compared the proposed algorithm with the previous two algorithms, the detection rate was significantly improved and the false positive rate is also significantly reduced, and we can also see from Tab 2 , the proportion of type in DOS and Probing attacks accounted for more cases , the proposed algorithm overall detection rate is higher, the main reason is because the other two types of attacks is relatively small, and less likely to be detected.

Table 3. The Intrusion Detection Results Comparison of Specific Attack Type

algorithm	MPSO-BP		PSO-BP		BP	
attack types	detection rate	False positives rate	detection rate	False positives rate	detection rate	False positives rate
DOS	93.31%	2.34%	85.35%	3.35%	80.35%	5.46%
R2L	41.36%	3.49%	41.27%	4.53%	38.51%	6.72%
U2R	27.42%	2.37%	26.46%	4.24%	25.58%	7.81%
Probing	91.28%	1.85%	90.29%	2.72%	89.12%	5.54%

Tab.3 shows the four types of attacks average detection rate and false positives rate. From the tab.3 we can see, detection rate of Probing and DoS are very high , 91.28% and 93.31% , respectively, but detection rate of U2R and R2L are not very high , only 27.42% and 41.36% . This is due to U2L and R2L type amount of attacks data are less, it is easy to form a miscarriage justice.

Above experimental data shows: the proposed algorithms and intrusion detection systems model can combine the advantages of BP neural network and PSO algorithm, so the overall effect of this intrusion detection model better than traditional detection model . Experiments show, MPSO_BP neural network model applied to the intrusion detection is effective, the MPBIDS model can effectively distinguish the normal behavior with the aggressive behavior, and it has high detection rate and low false positives rate.

MPBIDS combines the BP nerve network with MPSO algorithm, and establishes intrusion detection learning model. The training samples do the standardization and normalization of data , and using the neural network clustering MPSO_BP generate best match neurons , then making these typical characteristics samples develop a coding rule, and fed MPSO_BP network training . This will not only reduce the number of training samples MPSO_BP neural network, but also improve network learning speed , we can also take advantage of the encoding rules to determine new types of attacks . The model for the new network intrusion detection and timely updates to detect network and other aspects have very good results, it has good theoretical and practical application .

5. Conclusion

In this paper, the proposed MPSO algorithm optimized BP neural network, and proposed intrusion detection model based on neural network MPSO_BP: MPBIDS model, and we have a simple introduction to the model. This model has a strong reuse and expand ability, using the now popular support vector machine SVM instead of BP neural network r as a real-time mode classifier. Followed by detailed studies generic dataset KDD CUP99 of intrusion detection, including characterization , data preprocessing of KDD CUP99. Finally, the processed data as the training and test data tested the proposed MPBIDS model, we proved the model can improve detection rate of the test sample set and reduce the false positive rate , and it achieved the desired objectives.

6. Project

The soft science research plan project of Binzhou city in 2014.(2014BRK21）

References

[1] D. J. Welch and S. Lathrop, “A survey of 802.11 a wireless security threats and security mechanisms”, United States Military Academy West Point, **(2003)**.
[2] C. Rines, Voice over internet protocol, **(2001)**.
[3] M. Handley and V. Jacobson, Session description protocol, **(1998)**.
[4] S. Antonatos, K. G. Anagnostakis and E. P. Markatos, “Generating realistic workloads for network intrusion detection systems”, ACM SIGSOFT Software Engineering Notes, vol. 29, no. 1, **(2004)**, pp. 207-215.
[5] L. O. Damm, L. Lundberg and C. Wohlin, “Faults - slip - through—a concept for measuring the efficiency of the test process”, Software Process: Improvement and Practice, vol. 11, no. 1, **(2006)**, pp. 47-59.
[6] E. Davies, “Beyond dance: Laban's legacy of movement analysis”, Routledge, **(2006)**.
[7] S. Axelsson, “Intrusion detection systems: A survey and taxonomy”, Technical report, **(2000)**.

[8] T. H. Ptacek and T. N. Newsham, “Insertion, evasion, and denial of service: Eluding network Intrusion detection”, Secure Networks Inc, **(1998)**.
[9] W. Lee, S. J. Stolfo and K. W. Mok, “A data mining framework for building intrusion detection models”, Security and Privacy, Proceedings of the IEEE Symposium, IEEE, **(1999)**.
[10] R. Sekar, Y. Guang and S. Verma, “A high-performance network intrusion detection system”, Proceedings of the 6th ACM Conference on Computer and Communications Security, “ACM, **(1999)**.
[11] R. P. Lippmann, D. J. Fried and I. Graf, "Evaluating intrusion detection systems: The DARPA off-line intrusion detection evaluation”, DARPA Information Survivability Conference and Exposition, DISCEX, Proceedings, IEEE, **(2000)**.
[12] K. Kendall, “A database of computer attacks for the evaluation of intrusion detection systems”, Massachusetts Institute of Technology, **(1999)**.
[13] J. McHugh, “Testing intrusion detection systems: a critique of the DARPA intrusion detection system evaluations as performed by Lincoln Laboratory”, ACM transactions on Information and system Security, vol. 3, no. 4, **(2000)**, pp. 262-294.

Authors

Chunmin Qiu, he was born in 1967 in Binzhou City, Shandong Province, China,received his bachelor degree in Mathematics from Zhejiang University in 1989. Then in 2009, he got the master degree in Control Engineering from Jiangnan University.His current research fields mainly include Network Technology and Applications as well as Database Principles and Applications.

Jie Shan, he was born in 1979 in Gaomi County, Shandong Province, China, received the bachelor degree in Instructional Technology from Liaocheng University in 2004 and the master degree in Control Engineering from Qingdao University of Science & Technology in 2011. His current research field is mainly about Network Technology and Applications.

