International Journal of Security and Its Applications
Vol. 10, No. 8 (2016), pp.435-446
http://dx.doi.org/10.14257/ijsia.2016.10.8.38

Network Intrusion Detection Based on Stochastic Neural Networks Method

Yunfeng Yang and Fengxian Tang*

College of Computer & Information Engineering, Hechi University, Yizhou, 546300, China
hcxyyang@163.com

Abstract

With the rapid development of the Internet, especially the development of mobile Internet, network size and network infrastructure changes, especially the more random access node to detect network attacks challenges traditional detection algorithm using neural networks, so that the calculated volume increased dramatically, and will detection accuracy is not high, for this problem, we use the stochastic process theory hidden Markov chain transformation neural network, so that the convergence of a substantial decline, while improving network attack detection accuracy degree.

Keywords: *Neural network; Intrusion detection; Network security; Hidden Markov Chain*

1. Introduction

To the Internet as the representative of the global wave of information technology increasingly profound application of information network technology is increasingly popular and widespread, the application level is deep, applications from the traditional, small business system gradually to large, business-critical systems expansion, such as the typical government information systems, financial business systems, enterprise business systems. With the popularity and rapid development of the network,

Internet has an open, international and freedom while increasing application of freedom, network security issues are also increasingly obvious that it is more vulnerable to attack and destroy the outside world, the security and confidentiality of information severely affected, network security proposed higher requirements. Network security has become one of the world's governments, enterprises and the majority of network problems users are most concerned about.

Trying to undermine the integrity of information systems, confidentiality, credibility of any network activity called network intrusion. Network intrusion prevention most commonly used method is a firewall. A firewall is a combination of a series of components provided in the network security field between different networks (such as a trusted internal network and the untrusted public network) or it belongs to the network layer security technology, its role is to protect connected to the Internet enterprise network or individual nodes. It has a simple and practical features, and high transparency, can reach a certain safety requirements without modifying existing network applications situation. However, the firewall is a passive defensive network security tools, just use a firewall is not enough. First, the intruder can find loopholes in the firewall, bypass the firewall attack. Second, the firewall is assumed that the network boundaries and services, inability to attack from the inside, it provides service mode is either refused or have passed, and this is far from satisfying users increasingly complex application requirements. With the development of technology, the increasing complexity of networks, the shortcomings of traditional firewalls and weaknesses are constantly

ISSN: 1738-9976 IJSIA

exposed. Intrusion Detection is defined as: the identification process for malicious intent and behavior of computer or network resources, and to respond to the. Intrusion Detection System is a stand-alone system to complete the above functions. Intrusion Detection System can detect unauthorized objects (person or program) for the system intrusion attempts or behavior, and monitor system resources authorization object illegal operation. Intrusion detection as a proactive security technology, provides internal attacks and external attacks and misuse in real-time protection to help cope with the system network attacks, expanded the system administrator's security management capabilities (including security auditing, monitoring, attack recognition and response), improve the integrity of the information security infrastructure. It collects information from a number of key points in the computer network system, and analyze the information. Before the network is compromised system to intercept and respond to the invasion. Intrusion Detection System can make up a good firewall deficiencies, is a logical addition to the firewall, intrusion detection system is considered to be the second security gate behind a firewall, without affecting network performance can be monitored on the network, it can be prevented or alleviate the above Internet threats. If the network to be protected likened to a villa, a firewall is a walled villa, hidden internal structure, to prevent the invasion of criminals; however, there are light walls and can not guarantee the safety of the villa, with a need to monitor, to monitor the situation in the regions, Once the invasion of criminals, you can record the invasion process down criminals and respond. In network security, firewalls like villa walls, intrusion detection systems like monitors, complement each other to make the network more secure.

2. Related Works

2.1. Intrusion Detection

Depending on the information source intrusion detection system is divided into host-based and network based on two categories. Mixed Intrusion Detection System can make up for some of the network-based and host-based one-sidedness defects. Host-based intrusion detection system is usually mounted on the focus detection by the host, mainly the host's network connection and system audit logs real-time intelligent analysis and judgment. If one of the main activities are very suspicious (characteristics or statistical law violation), intrusion detection system will take corresponding measures.

Host-based IDS into the other technologies in the development process. A common method of detection of critical system files and executables invasion is regularly checked by checking documents and to carry out, in order to detect abnormal changes[1-4]. The reaction depends on the wheel speed information length interval. Many products are listening port activity and alert administrators when specific ports are accessed. Such detection methods will be integrated into the basic network intrusion detection methods based on the detection of host-based environment. Host intrusion detection systems analysis "of possible attacks," very useful. For example, sometimes it apart from intruders trying to point out to perform some "dangerous command", they'll also tell what the intruder did, what programs they run, which opened the document, the implementation of which system call. Host Intrusion Detection System can usually provide more detailed information compared with the network intrusion detection system. Host Intrusion Detection System will reduce the efficiency of the application system. Host Intrusion Detection System is typically installed on the need to protect our equipment, for example, when a database server to be protected, it is necessary to install intrusion detection systems on the server itself, which reduces the efficiency of the application system. Host Intrusion Detection System Another problem is that it relies on the inherent server logs and surveillance capability. If the server is not configured logging, the necessary re-configuration, which will lead to unpredictable performance impact to the operation of

the business system. Full deployment of the larger costs of host intrusion detection systems, the enterprise is difficult to use all host host intrusion detection system protection, the host can only select some protection. Those host intrusion detection systems are not installed in the machine will be protected by a blind spot, intruders can use these machines to achieve the target.

Network-based intrusion detection systems are usually placed in the segment more important, kept surveillance network segment of the various data packets. For each data network intrusion detection system can detect those attacks from the network, it can detect more than authorized unauthorized access. A network intrusion detection system does not need to change the configuration of servers and other hosts. Because it does not install additional software on the host business system, so as not to affect the use of these machines, CPU, I / O and disk resources, etc[5]., will not affect the performance of business systems.

Since network intrusion detection system like routers, firewalls and other key equipment way to work, it does not become the critical path system. Failure does not affect the normal business operation of the network intrusion detection system occur. The deployment of a network intrusion detection system risk much less than the risk of host intrusion detection systems. Network and host-based intrusion detection systems have their own advantages based on the two complement each other. Both ways can be found to some other party can not detect intrusion. A local attacker sent from the keyboard is not an important server via the network, and therefore can not be detected through network-based intrusion detection system, only by using host-based intrusion detection system to detect. Network-based intrusion detection systems by examining all packets (including header information) to detect [6-7], and host-based intrusion detection system does not view the packet header information. Many IP-based denial of service attacks and debris attack, only by looking at the packets transmitted over the network when they can identify the header information. Can study the network-based intrusion detection system load content and look for commands or syntax used in specific attacks, such attacks can be quickly identified in real-time intrusion detection system inspects the packet sequence. The host-based systems can not see the load and, therefore, does not recognize the embedded load attack. Joint use of host-based and network-based two ways to achieve better detection results. Such as the use log as a detection system based on host-based intrusion detection systems, they determined attack.

Compared with network-based detection systems with greater accuracy whether or not the time has been successful. In this regard, host-based intrusion detection system for network-based intrusion detection system is a great addition, people can use to provide early warning network-based intrusion detection systems, and host-based intrusion detection system to verify whether the attack Success.

In the next generation of intrusion detection system, will now Web-based and host-based detection technology both well integrated together to provide integrated attack signatures, detection, reporting and event correlation function. I believe the future of integrated intrusion detection products are not only more powerful, but also on the deployment and use of more flexible and convenient. Various events were analyzed, and found in violation of security policy behavior is the intrusion detection system core functions. Technically, intrusion detection is divided into two categories: a pattern matching intrusion detection system based on another abnormal findings intrusion detection system. For detection techniques based on pattern matching, first to define the violation of the security policy features events such as some header information network packets. Detection mainly determined by the characteristics of the data collected is present in the collected intrusion patterns library. The technique based on the detection of abnormal findings is to define a set of system "normal" threshold conditions, such as CPU utilization, memory utilization, file checksums, etc. (such data can be artificially defined, you can also observe the system, and draw a statistical approach), then the value of the

system is running with the definition of "normal" threshold conditions for comparison, the signs of attack. The core of this detection method is how to analyze system operation[8-10].

Based on pattern matching detection technology and detection technique based on abnormal findings, the conclusions have a very big difference. Based on the core pattern matching techniques to detect intrusion patterns is to maintain a database for known attacks, it can be detailed, accurate reports of the type of attack, but limited effect on the unknown attacks, and invasive model database must be constantly updated. Technique based on the detection of abnormal findings can not be accurately discriminated attacking approach, but it can (at least theoretically possible) found to be more extensive, even unknown attacks. If conditions permit, a combination of both detection will achieve better results.

2.2. Stochastic Model Theory of Artificial Intelligence

Hidden markov models are widely used in speech recognition, and achieved great success. Hidden markov model is also be introduced in computer language recognition and mobile communication core technologies "multi-user detection". In recent years, the hidden markov model in biological information science, fault diagnosis, and other fields are also beginning to get used. Hidden markov model is developed on the basis of markov chain of a statistical analysis model, the markov chain model, the observed value and status is one-to-one, watchers observed value, also knew the observations of the state. And in the hidden markov model[11-13], observation and state is not one-to-one correspondence, the observer can only see observations, cannot see the state directly, only through the existence of the state of a random process to perceive and features. That is to say, the hidden markov model is a dual stochastic process, is composed of two parts: one is a markov chain, describes the transfer of state, described in transition probability. The other is a general stochastic process, describe the relationship between state and observation sequence, probability with the observed value. When get an observation sequence O={O1, O2,..., OT}, cannot the observation sequence directly by state sequence S= {S1,...ST}, if you want to get the actual state of sequence, then you have to know the distribution of observations in each state, the state of the initial probability, as well as the state transition probability. It involves the parameters as shown in table 1[14-15].

Table 1. The Parameters of Hidden Markov Model is Described

Parameter	Describe
State the number N	State of finite set $S=\{S_1,S_2,\ldots,S_M\}$
Number of observations of M	Value of finite set $O=\{O_1,O_2,\ldots,O_M\}$
The initial state distribution	t = 1 ,the probability of state S_i is $\pi_i = P(q_1 = S_i)$
State transition matrix	the probability of From state i to state j is $a_{ij} = P(q_{t+1} = S_j \mid q_t = S_i)$
Observation probability matrix	In the condition of S_j, the probability of O_k

Once a problem can be explained by hidden markov models, it must have three questions need to be solved.

(1) Evaluation: given a model and an observation sequence, how to calculate the probability of the model can be in what to get the observation sequence.Can also see the problem as a model and degree of match between a given observation sequence.

(2) Decoding: is to try to find the implicit part of the hidden markov models, namely to find the right sequence.Of course, everyone knows is, in addition to degradation model, the only correct sequence of state does not exist.Therefore, in dealing with the actual application, generally only by finding the optimal sequence to solve such problems.

(3) Study: to find the most optimal model, the model can with maximum probability for a given observation sequence.The model is used to adjust the parameter value, the observation sequence is known as the training sequences, hidden markov model that is used for training.In the solution actual problem, training problem hidden markov model is one of the most important link, because according to the observation sequence to adjust the given until the optimal model parameters, the optimal model is equivalent to create a[5-7].

2.3. The Neural Network Theory

Neural network is composed of a large number of neurons by perfect link adaptive nonlinear dynamic system, composed of many simple processing units of neurons by using weighted connection, interaction of instance can be used to the adaptive or form the weight function of neural network self-learning, so that the network correctly understand and solve specific problems and achieve the best performance.Common neural network model are perceptron network and linear neural network, BP network and radial basis function network, Hopfield network, self-organization network, etc.

BP neural network as part of the neural network, is currently widely used in the function approximation, pattern recognition, classification, and data compression, *etc*. The BP neural network is back propagation network. It is a set of sample input and output into a nonlinear optimization problem, using the most common gradient descent algorithm, the optimization of the right to solve by the iterative arithmetic, join the hidden node makes the optimization problem of adjustable parameter increases, which can approximate the exact solution. Is a kind of multilayer forward, using the error back propagation learning algorithm of neural network. BP neural network topology structure including: input layer, output layer and hidden layer, hidden layer can be a layer or multilayer, and there are many neurons on each floor. BP neural network is characterized by: without any connection between neurons inside the layers, each layer neurons only have connections between neurons, and the adjacent layer without feedback connections between neurons. Input layer to receive information from the outside the network, and then through the dissemination of the information sent to the hidden layer nodes forward, after transformation by correspondence, put the information output of hidden nodes. Hidden layer does not directly receive signal of the outside world, also don't directly send signals to the outside world.

Under normal circumstances, the node of hidden layer USES the transformation function type selecting Sigmoid function, and the output layer adopts linear activation function. As there is no any coupling nodes in the tree, therefore, only accept each layer of the neural network input layer neurons before, the output of each layer neurons only under the influence of output layer neurons. Network's input data x = (xl, x2,..., xt) from the input layer through the hidden layer nodes, in turn and then to output data to get the output layer node y = (yl, y2,..., yt).Therefore, the BP neural network can be considered a highly nonlinear mapping from input to output. The BP neural network by means of learning samples, adjust the connection weights of BP neural network, can realize the nonlinear classification problem, in this paper, the model of BP neural network was adopted to detect attacks[8-9].

BP algorithm is a generalized form of least mean square algorithm, it USES the gradient search technology, according to the price rule of correspondence of the smallest recursively solving network weights, the actual output and the expected output of correspondence for the network cost of mean square error. Its pattern recognition is

divided into two different stages: the first stage as the learning phase, the network training stage, adjust the weights of neural network in order to show the problem domain; The second stage for work stage, the weights are fixed, the actual data or the experimental data input to the neural network, the network to carry on the pattern classification. Network training at the start of the initialization of a weight of a set of random values, node prescribed output value, when input training data, the cost function is calculated, by BP algorithm, the error backward propagation in the direction of input layer, one by one when the net output and desired output does not match fit error back propagation. Back propagation error through the output layer, the way accidentally fell fixed weights of each layer, the hidden layer and input layer can spread step by step. This positive cycle of information dissemination and error back propagation process, makes the adjustment of weights of each layer, the error spread to all the units in each layer, thus achieve the purpose of correction of each unit weight, until the size of the error in the acceptable range so far in advance, the output generally take sigmoid function, $f_j(x) = 1/(1+e^{-x})$.

3. Based on Hidden Markov Model and Neural Network Intrusion Detection Model

In reference to the state transfer principle of hidden markov model and BP neural network to adjust the weights of the links in the network can realize the nonlinear classification principle, this paper puts forward a kind of based on hidden markov model and neural network intrusion detection model is shown in Figure 1.

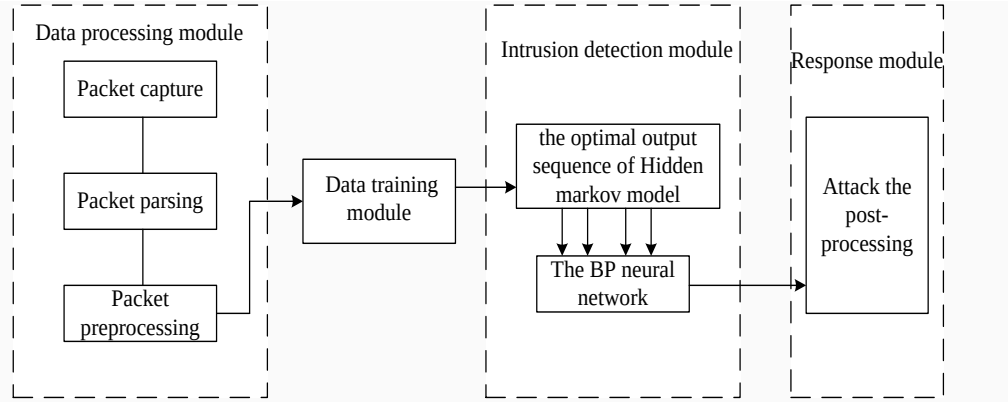

Figure 1. Based on Hidden Markov Model and Neural Network Intrusion Detection Model

The intrusion detection model is mainly composed of the data processing module, data, training module, intrusion detection module and response center four major part module. Which model is the core of intrusion detection module. Intrusion detection system is composed of two parts: the first part is the hidden markov model, and the other part of the neural network. Intrusion detection model of the working principle is as follows: first of all by the data processing module of the data (including the packet capture, packet parsing, and pretreatment is transformed into hidden markov model can identify the input) to train the hidden markov model, training after a good model can be used to detect intrusion behavior and behavior, it is important to note: the data here is outside of the BP neural network training module, here is the main application of the characteristics of the hidden markov model is easy to train. But in order to improve the detection rate, the output of the hidden markov models as neural network input, the state sequence for the

second test, real output of the neural network output is expected, according to the neural network output is given the corresponding response[10-13].

Hidden markov model is used in network intrusion detection is one of the most obvious difficulty hidden markov model is the observed value of it is difficult to determine, good parameter selection may make calculation efficiency is higher, and the choice of the observations may lead to training time is very long, even can't complete the training. In understanding the TCP/IP protocol model and several agreements on the basis of basic theory and combined with TCP/IP management model, the flow control principle and the characteristic of the agreement itself, this paper proposes a certain hidden markov model to observe the value of the method. Including the TCP, UDP and ICMP protocol packets.

1, The TCP packets, TCP state detection is a important part of the intrusion detection based on network, various intrusion way based on network protocol vulnerabilities can be early found through TCP state detection, when the TCP connection state transition is not in conformity with the TCP state in figure, the abnormal phenomena. In TCP management model, to establish and release connections required steps can be expressed in a finite state machine, each state, there are some legal events, when legal events, may take an action, when other events, the report an error. When send a datagram to send cache, and then to receive in the form of message segment cache, and after receiving the cache is in the buffer is full, just put the data sent to the application, then if send a datagram to improve efficiency.

2, UDP packets, UDP protocol is the user data packets, it is a connectionless protocol, the UDP protocol for data transmission, no connection is established, and does not guarantee that the data message must be sent to the destination, so that the transport process is greatly simplified. Here only mention the UDP no do, UDP does not consider the flow control, error control, after receiving a bad data segment it nor retransmission. All these work is left to the user process. It will only use the concept of port data segment solutions for reuse in multiple processes, this is it to do all the work. For people who need precise control, error control or need, or need time control applications, UDP especially for one area is in the client - server. The client to the server to send a short request, and expect to get a short reply back. If the request or response of lost here, clients will timeout, so it will retry just ok, as long as the two messages on the network will be enough.

3, The ICMP packets, ICMP is a control message protocol, it is a connection-oriented protocol, is used to transfer control between IP host, routers. Control message is refers to the network impassability, host, whether can reach, routing, availability, *etc*. The news of the network itself. Although these control messages are not transmitted user data, but for user data transmission, network security plays a very important role, is a very important protocol, especially when the judgment to the network connection status. When unable to access the target IP data, IP router cannot according to the current transmission rate to forward data packets, and so on and so forth, will automatically sends the ICMP message, it is an error message protocol and control, not only used for the transmission error message, also transmission control message.

To establish the BP neural network is the most main is to determine the number of input layer neurons in the network, the number of neurons in hidden layer, hidden layer and output layer neuron number, these parameters are the network model is determined. The BP neural network parameters determine the situation is as follows:

(a) the determination of input layer and output layer neuron number of the neural network output is expected output: be attacked or normal. Regulation is attacked here output is 1, the system is normal output is zero. Because the actual output of neural network is generally not as an integer 0 or 1, so the rules when the accuracy of the output value in a certain range close to 1 if you think that the system is under attack, so there is

only one output neurons. In this paper, design of neural network is a vector to point mapping. The normal map to 0, abnormal process of system call vector map to 1.

(b) the determination of number of hidden layer. Hidden layer of abstraction, that is, it can extract features from the input samples. Increasing hidden layer can increase the processing capacity of neural network, but also will increase the complexity of the training and the training time. In addition, increasing Numbers of hidden layers, the network in the process of learning will be more easy to fall into local minimum point and can't get rid of, the error of the network adjustment to meet the global minimum of error, seriously affect the learning effect. About the influence of the hidden layer of network capacity, Kolmogorov theorem proving for any continuous function on closed interval can use contains a single hidden layer of BP neural network approximation; A hidden layer can be achieved arbitrary decision classification problem, if you want to enter any output function of the graphics, said only two hidden layer. Because just want to use in this paper the characteristics of the decisions of the neural network classification, involves the problem is relatively simple, so there is no need to use more hidden layer structure of high complexity, using single hidden layer structure is enough.

(c) The determination of number of hidden layer neurons. Determination of hidden layer neurons number compared to determine the number of hidden layer is a lot more complicated, because the number of neurons in hidden layer will affect the whole network of the final output. Reduce the number of hidden layer neurons, the network's ability to obtain information from the sample is bad, difficult to summarize and reflect learning samples are in the process of law. Increase the number of hidden layer neurons, may make the network learning and some need to master the knowledge, not only can increase the time of network learning, but also reduces the detection capability of the network.

4. The Model and the Analysis of Experimental Results

4.1. The Model

In this paper, the research based on hidden markov model and neural network intrusion detection model is mainly using hidden markov models mature excellent pattern recognition algorithm and neural network to design. First capture network transmission of all packets, extract interested in packets. Then, training module of capture packets through the Baum Welch - hidden markov model algorithm for training, training model after through the Viterbi algorithm, the output an optimal sequence consisting of N different symbols. These sequences can well judge whether to attack. But in order to improve the detection rate, excellent classification using neural network features, to further judgment, the state of the output sequence of the hidden markov model output as the input of neural network with BP algorithm to make the final output is expected as a result, in order to achieve further judge the invasion. Mainly includes the data processing module, training module, intrusion detection module, the corresponding module [14-15].

1. Packet processing module is the basis of the model, all the data flow passes through the module can be identified, and the module is mainly composed of packet capture, packet parsing, and pretreatment of three parts.

(a) Packet capture. So far, there are two kinds of packet capture method, which are frequently used is a kind of network data capture use special equipment;Another kind is to use ordinary general network adapter hardware of computer and network connection, the network card to capture.If you want to capture all the packets, you have to bypass the system to work normally, the processing mechanism of direct access to the underlying network, generally is the nic set to mixed mode, mixed mode of computer can receive all information through the network segment.

(b) Packet parsing. Parsing module mainly is to capture the packet's IP, TCP, UDP, ICMP packet parsing, through the analysis of its structure, inspection packet header, which is to determine the type of packet, which can extract the characteristics of this packet.

(c) Packet preprocessing. Data preprocessing is the data format conversion for Cain marko markov model can identify the format, to capture the packets feature coding processing.

2. Training module. That measures the performance of intrusion detection system as a very important part of training degree determines the detection rate of high and low, specific algorithm steps has been given in Chapter 4.Training module is mainly using hidden markov model and Baum Welch algorithm for the forward algorithm, the specific implementation of training is through continuous adjustment parameters,

3. Intrusion detection module. Intrusion detection module as the core of this article, main points of two parts: one is the hidden markov model, the other is neural network part.Part of hidden markov model is used to output the optimal sequence, this paper is through the Viterbi algorithm to calculate observation sequence, the optimal state and state of the optimal sequence as neural network input, the output of the neural network is the desired result.

4. The response module. Response module is: by calling the sound file and play some music to achieve the purpose of the alarm, at the same time will alarm events recorded in the log. Voice call the police need to audio audio files, specific implementation steps are (1) locate the position of the sound file (2) acquire the sound file and play.

In this paper, the design of based on hidden markov model and neural network intrusion detection model" after encapsulation system can be run separately in the protected hosts. The specific function of system implementation are: capture, training, detection and response, *etc*. The operation of the system starting from the "capture", click on the "configuration" menu, select network card and you can begin to capture the packet type. TAB, click on the "real-time statistics" in a system will perform the detection function, when the attack was found, will be prompted to find the invasion, and report to the police.

4.2. Experimental Analysis

Because of the large amount of data, this study selected the only part of the data for testing. Comparable to experiment, to extract the five kinds of typical attack as the experimental data of this model, five kinds of attacks to Neptune, Satan, PortSweep, Buffe - overflow, Guess - passwd, the experiment selected four categories contains attacked.

Experimental steps are as follows:

1 Use 60% of all the data for training, these data include intrusion data and normal data;

2 After the training, with another 40% of the data to test the model;

3 The output. In order to judge the invasion, the optimal sequence in the output when set up a sliding window, so that the optimal sequence is divided into a number of fixed length of short sequences as neural network input, and then by judging from the neural network to determine whether the actual amount of 0/1, the invasion. If by a sequence of 1 more than a predetermined threshold method, is considered to be an invasion. On the other hand, is considered normal. For the threshold, in the experiment, it is obtained by

setting different values to compare a series of values, the final test results as shown in Table 2:

Table 2. Based on Hidden Markov Model and Neural Network Intrusion Detection Model Experiment Records

Types of attacks	Normal	Neptune	Satan	Portsweep	Buffe-overflow	Guess-passwd
Normal	5930	0	18	3	5	4
Neptune	2	3735	27	8	0	0
Satan	3	17	805	0	0	0
Portsweep	0	6	4	178	0	0
Buffe-overflow	8	0	0	0	9	0
Guess-passwd	1454	0	0	0	0	14
Detection rate(%)	80.17	99.39	94.26	94.17	62.29	77.78

Finally the experimental results and the source of the same data testing based on neural network intrusion detection research and hidden markov model of intrusion detection system based on protocol research.

Table 3. The Experimental Records of BP Neural Network Model Experiment

Types of attacks	Normal	Neptune	Satan	Portsweep	Buffe-overflow	Guess-passwd
Normal	5987	0	17	2	0	0
Neptune	2	3921	27	8	0	0
Satan	1	17	787	0	0	0
Portsweep	0	8	3	169	0	0
Buffe-overflow	16	0	0	0	8	0
Guess-passwd	2046	0	0	0	0	0
Detection rate(%)	74.35	99. 37	94.36	94.18	0	0

Table 4. The Experimental Records of Hidden Markov Model

Types of attacks	Detection rate(%)
Portsweep	91.3
Neptune	93.2
Guess-passwd	72.8
Buffe-overflow	49.3

By comparing the test results can be seen that based on hidden markov model and neural network intrusion detection model of Buffer overflow and Guess - passwd detection effect is not very good, mainly because both attack is to use the system vulnerabilities, get the local access to the target host or administrator privileges, but this system relies on the analysis of network packets to find the invasion, but in general this kind of intrusion detection based on hidden markov model and neural network model than using a hidden markov model or neural network intrusion detection system detection rates still higher.

5. Conclusion

This paper constructs the neural network hidden Markov chain theory, this method can focus on the transition probability and stochastic point of attack for analysis and neural networks to detect this, after tests showed that the proposed network attack detection the system can quickly and accurately detect network attacks, and the accuracy rate is also greatly improved.

6. Fund Support (1)(2)

(1) Guangxi Education Department (KY2016YB380;KY2015LX336).

(2) Hechi University(2014ZD-N002).

References

[1] X. Jiang and H. Adeli, "Dynamic Wavelet Neural Network Model for Traffic Flow Forecasting", Journal of Transportation Engineering, vol. 131, no. 10, **(2014)**, pp. 771-779.
[2] C. P. Tsai and T. L. Lee, "Back-Propagation Neural Network in Tidal-Level Forecasting", Journal of Waterway Port Coastal & Ocean Engineering, vol. 125, no. 4, **(2014)**, pp. 195-202.
[3] T. Hegazy and A. Ayed, "Neural Network Model for Parametric Cost Estimation of Highway Projects", Journal of Construction Engineering & Management, vol. 124, no. 3, **(2014)**, pp. 210-218.
[4] D. Al-Jumeily and A. J. Hussain, "The performance of immune-based neural network with financial time series prediction", Cogent Engineering, vol. 2, no. 1, **(2015)**.
[5] A. Sarkar, S. K. Sinha and J. K. Chakravartty, "Artificial Neural Network Modelling of In-Reactor Diametral Creep of Zr2.5%Nb Pressure Tubes of Indian PHWRs", Annals of Nuclear Energy, vol. 69, no. 1, **(2014)**, pp. 246-251.
[6] E. M. Shakshuki, N. Kang and T. R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transactions on Industrial Electronics, vol. 60, no. 3, **(2013)**, pp. 1089-1098.
[7] C. Modi, D. Patel and B. Borisaniya, "A survey of intrusion detection techniques in Cloud", Journal of Network & Computer Applications, vol. 36, no. 1, **(2013)**, pp. 42-57.
[8] C. Modi, D. Patel and B. Borisaniya, "Review: A survey of intrusion detection techniques in Cloud", Journal of Network & Computer Applications, vol. 36, no. 1, **(2013)**, pp. 42-57.
[9] H. J. Liao, C. H. R. Lin and Y. C. Lin, "Intrusion detection system: A comprehensive review", Journal of Network & Computer Applications, vol. 36, no. 1, **(2013)**, pp. 16-24.
[10] J. Xu and C. R. Shelton, "Intrusion Detection using Continuous Time Bayesian Networks", Journal of Artificial Intelligence Research, vol. 39, no. 4, **(2014)**, pp. 745-774.
[11] D. Acemoglu, A. Malekian and A. Ozdaglar, "Network Security and Contagion", Social Science Electronic Publishing, vol. 42, **(2013)**, pp. 38-38.
[12] H. Zhong, "Evaluation and Countermeasures of computer network security applications", Network Security Technology & Application, **(2014)**.
[13] Z. Yuan, "On the computer network security risks and prevention strategies", Network Security Technology & Application, **(2014)**.
[14] W. U. Hai-Bing, P. Liu and L. I. Ming-Xi, "Network Security in Secret Related Operation Classes", Research & Exploration in Laboratory, **(2013)**.
[15] Z. Dai, "Study on computer network security and defense measures", Network Security Technology & Application, **(2014)**.

Authors

Yang Yunfeng, (1975), male, Dali Yunnan, lecturer. His research interests include Computer Network, Network Security.

Tang Fengxian, (1977), Female, Duan Guangxi, Associate Professor. Her research interests include Pattern Recognition, Image Processing