Advanced Science and Technology Letters
Vol.134 (CIA 2016), pp.53-58
http://dx.doi.org/10.14257/astl.2016.134.09

Network intrusion detection method based on neural network research

Yang Yunfeng

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

Abstract. In the Internet age, because of the network security against the background of technical personnel to the existence of the invasion of the network, and can make use of computing tools, make procedural means of invasion, the network intrusion detection is very difficult to analyze and judge. Aiming at this problem, in this paper, on the basis of the use of computing devices, using analysis method of neural network is used to analyze the structure of artificial intelligence, the hidden markov model under the condition of abnormal behavior. Experimental results show that this method is multiple intrusion methods can rapidly accordingly, and has high detection rate, lower false alarm rate.

Keywords: Neural network; Intrusion detection; Network security

1 Introduction

With the continuous expansion of Internet users, highlighted the advantages of the Internet application in information transmission, e-government, e-commerce, online games, blogs, microblogging and other Internet business is rapidly expanding. Network in people's work, study and life of the role of more and more can not be ignored, but the openness of the network brings the security risk also increases, all kinds of network intrusion behavior abounds and rising to become the biggest hidden trouble of network security. Mainly according to the characters of known attacks and information prediction of impending attack, usually through a variety of mathematical methods network existing attack data analysis and mining, and then extract the important features of interest and related information[1-4].

2 Related works

2.1 Intrusion detection technology

Intrusion detection, as its name implies is to detect intrusion behavior, is the combination of software and hardware of intrusion detection. Intrusion detection is a

ISSN: 2287-1233 ASTL

kind of active safety technology, have to identify intrusion behavior, prevent the happening of the intrusion and the spillover effect. Intrusion detection is a rational supplement of the firewall, the help system against network attacks, expanded the system administrator safety management ability, improve the integrity of the information security infrastructure. The earliest intrusion detection model is mainly based on the host system audit record data, generate several outline on the system, and detect contour variations found invasion behavior of the system. Incident response to respond to the result of the analysis of functional units, it may terminate the process, reset the connection, change file attributes, etc., can also be simply call the police.

2.2 Hidden markov model theory

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". 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 $O=\{O_1, O_2,..., O_T\}$, cannot the observation sequence directly by state sequence $S= \{S_1,...S_T\}$, 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 [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. Is a kind of multilayer forward, using the error back propagation learning algorithm of neural network. 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.

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[8-9].

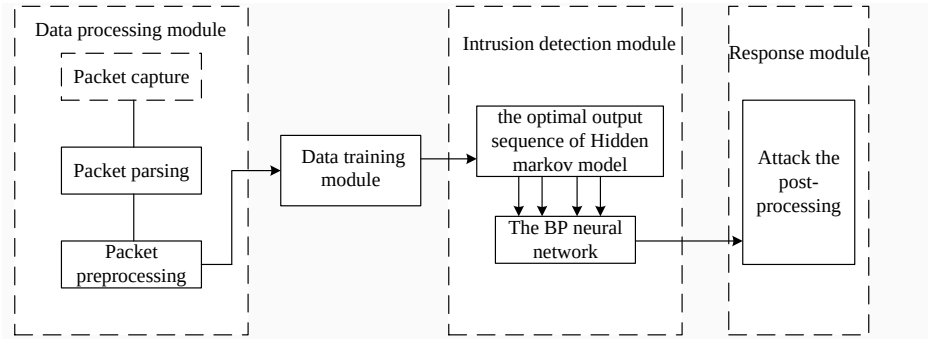

Fig. 1. Based on hidden markov model and neural network intrusion detection model

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 to train the hidden markov model, 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 [10-13].

4 The model and the analysis of experimental results

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 [14-15].

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 1. 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 2. 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 3. 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

Put forward a intrusion detection model based on neural network and the hidden markov. Currently using hidden markov model theory and neural network theory to the research of intrusion detection, and good results have been achieved, but most of the studies from the Angle of the system call to consider, and system call number of the shortcomings is big, hard training. Real combine both from the perspective of the agreement is not much, to be linked to the experimental results show that the two combine to intrusion detection than using hidden markov model and neural network has high detection rate.

6 Fund Support

(1) Hechi University New Technology of Computer Network and Software Key Lab([2013].3)
(2) The formal project of Guangxi Education Department in 2016: Research and Application of Rough Set of suspected attack in the server cluster network javascript;

References

1. Jiang, X., Adeli, H.: Dynamic Wavelet Neural Network Model for Traffic Flow Forecasting [J]. Journal of Transportation Engineering, 2014, 131(10):771-779.
2. Tsai, CP., Lee, TL.: Back-Propagation Neural Network in Tidal-Level Forecasting [J]. Journal of Waterway Port Coastal & Ocean Engineering, 2014, 125(4):195-202.
3. Hegazy, T., Ayed, A.: Neural Network Model for Parametric Cost Estimation of Highway Projects [J]. Journal of Construction Engineering & Management, 2014, 124(3):210-218.

4. Al-Jumeily, D., Hussain, AJ.: The performance of immune-based neural network with financial time series prediction [J]. Cogent Engineering, 2015, 2(1).
5. Sarkar, A., Sinha, SK., Chakravartty, JK.: Artificial Neural Network Modelling of In-Reactor Diametral Creep of Zr2.5%Nb Pressure Tubes of Indian PHWRs[J]. Annals of Nuclear Energy, 2014, 69(1):246–251.
6. Shakshuki, EM., Kang, N., Sheltami, TR.: EAACK—A Secure Intrusion-Detection System for MANETs[J]. IEEE Transactions on Industrial Electronics, 2013, 60(3):1089-1098.
7. Modi., C., Patel, D., Borisaniya, B., A survey of intrusion detection techniques in Cloud [J]. Journal of Network & Computer Applications, 2013, 36(1):42–57.
8. Modi, C., Patel. D., Borisaniya, B., Review: A survey of intrusion detection techniques in Cloud [J]. Journal of Network & Computer Applications, 2013, 36(1):42-57.
9. Liao, HJ., Lin. CHR., Lin. YC.: Intrusion detection system: A comprehensive review[J]. Journal of Network & Computer Applications, 2013, 36(1):16–24.
10. Xu, J., Shelton, CR.: Intrusion Detection using Continuous Time Bayesian Networks [J]. Journal of Artificial Intelligence Research, 2014, 39(4):745-774.
11. Acemoglu, D., Malekian. A., Ozdaglar, A.: Network Security and Contagion [J]. Social Science Electronic Publishing, 2013, 42:38-38.
12. Zhong, H.: Evaluation and Countermeasures of computer network security applications [J]. Network Security Technology & Application, 2014.
13. Yuan, Z.: On the computer network security risks and prevention strategies [J]. Network Security Technology & Application, 2014.
14. Hai-Bing, WU., Liu, P., Ming-Xi, LI.: Network Security in Secret Related Operation Classes [J]. Research & Exploration in Laboratory, 2013.
15. Dai, Z.: Study on computer network security and defense measures [J].: Network Security Technology & Application, 2014.

