Network Intrusion Detection System and Its Cognitive Ability based on Artificial Immune Model

WangLinjing[1], ZhangHan[2]

[1] Henan University of Traditional Chinese Medicine, Zhengzhou 450008,China;

[2] Peking university, Beijing 100871, China

Xuexi123@163.com

Keywords: Artificial immune model, Network intrusion detection, Security, Network information security.

Abstract. With the rapid development of science and information technology, computer and network technology have made jumping progress, which not only speeds up the global information, but also brings more serious information security issues. Information network security has become a new term, which is related to social stability, the inheritance of national culture and the national information security level, so it can't be ignored. Information secrecy, security and controllability are related to research of information network. Although the traditional network defense style can maintain the security of network information, but it is passive and can't detect and prevent network attacks. Therefore, active detection and implementation has become a hot spot for network information security technology, which is one of the most important fields of information network expert research. Aiming at the defects of the traditional network detection technology, this paper designs and explores the network intrusion detection system based on artificial immune model. This system can effectively screen and defend the illegal and intrusion events, and prevent the important core secrets. The system is flexible and has strong portability, which has a more practical protective effect on the important information of the privacy.

Introduction

With the rapid development and the depth application of internet technology, it has completely changed people's traditional computing mode-one machine [1,2]. The internet technology changes the people's life mode and thinking mode, people began to rely heavily on the internet. Information network promotes the construction of the earth village, which has a great effect on the progress of the society. Compared with developed countries, the development of network information technology in our country is relatively late, and the starting point is lower, but the speed of development is very alarming [3-5]. According to the statistics of Ministry of Industry, China has more net name and the number has been broken million, so the internet has relatively high penetration rate. In network aspects, people's daily life has come to a series of security problems, the problems of exposure network security information are increasing [6,7]. Network information is generally more sensitive, including some personal privacy and even state secrets, so it is necessary to prevent hackers to steal network information, avoiding the outflow of private information. This paper studies the network intrusion detection system based on artificial immune model, which has certain recognition and learning ability, and can actively search and defense malicious code to ensure that the network equipment can work properly, so that it can protect the personal privacy and state secrets.

Intrusion Detection System

Concept of intrusion detection. Intrusion is illegal behavior, without formal authorization, the foreign network attempts to access the client to gather information, process information and even control the client system [8-10]. In the early stage of network information security, the firewall has obvious shortcomings, which mainly adopts the technology of strengthening protection and isolation protection, and it can't take the initiative protective measures against the new attack method. At the

early of the eighty's in the last century, there are threat and intrusion, and the intrusion mainly refers to the collection of damage the security and reliability of the data resource [11]. Intrusion detection is to obtain the data packets of the network nodes, and filter and detect these packets, finally judge whether there is sign of intrusion according to the results.

Types of intrusion detection. Intrusion detection is a hardware or software system which can make real-time judgment, online preservation and defense against the illegal activities on the host resources. There are many types of intrusion detection, which can be classified by different methods. According to the different technology application, they can be divided into anomaly detection and feature detection [12-15]. Anomaly detection means when the intruder activity is not normal, it needs to establish normal activities. If the detection activities violate the normal statistical laws, then it can be determined as the illegal behavior; feature detection means the identified intruder activity can be de described with a fixed means, and then it needs to further determine whether the main activities are in compliance with the standard of these fixed patterns.

According to the nature of the system monitoring, intrusion events can be divided into two systems, host computer intrusion and network intrusion [16]. The former mainly refers to the detection and analysis of the audit records of the host to detect intrusion. Whether it can timely collect audit is one of the weaknesses of these systems, the intruder will make host audit subsystem as a target to avoid intrusion detection system; while the latter is to collect communication data on the shared network to analyze suspicious behavior. The process of intrusion detection system is as shown in Figure 1.

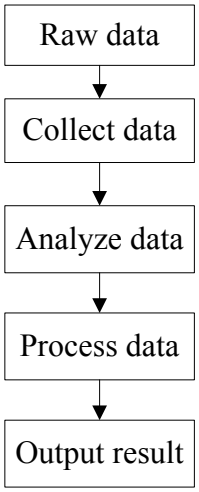

Fig. 1 The flow chart of intrusion detection system

Artificial Immune System Model

Computer immunology is a new discipline which combines electronic information, agricultural information, biotechnology, computer technology and intelligent control system. Artificial immune model is actually a bionic system of biological immune system, human immune system is mainly rely on human tissues, including human organs, nerve cells and molecules, and other parts of the human immune system. The biological immune system is very important to protect the organism from the infection of the pathogen, and it can identify any kind of foreign cells and bacteria [17-19]. Therefore, it must have the ability to recognize its own tissue cells and molecules. Artificial immune system has high level of artificial intelligence, which is the same as all kinds of classic algorithms, and they are the unique way of intelligent electronic information processing, finally began to spread slowly.

Artificial immune model mainly uses the biological immune system, and establishes a dynamic and adaptive protection network to judge the invasion and attack, and further ensure the effectiveness and availability of resource information. Artificial immune system is very powerful, because it has a variety of algorithms, including negative selection, immune learning, immune agent, immune network regulation, immune evolution algorithm [20]. The core idea is to mimic the biological immune system to produce antibodies to kill bacteria and deal with the whole process of antigen. The artificial immune system model is as shown in Figure 2.

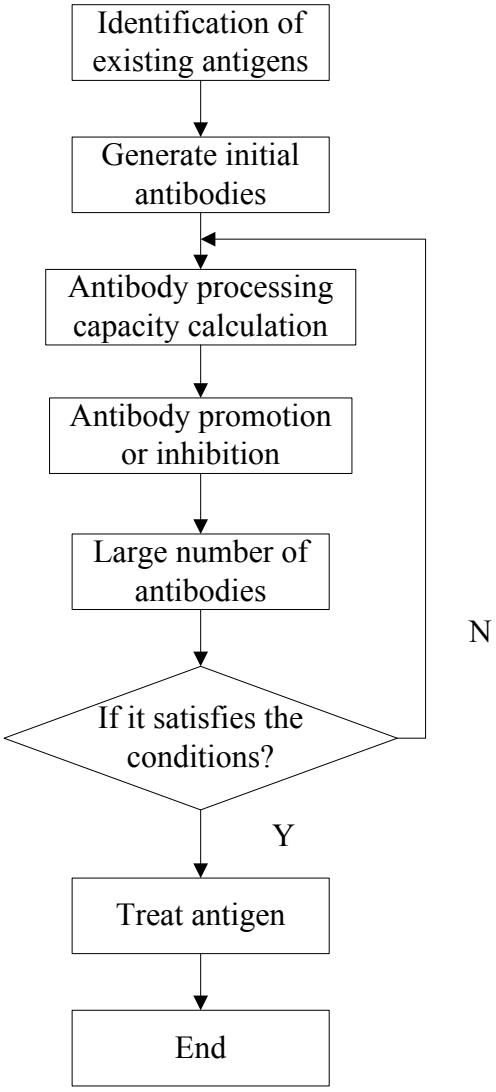

Fig. 2 The flow chart of artificial immune system model processing

The main difficulty of artificial immune system model is the calculation algorithm, and the affinity is the most difficult. Because molecular nature of antibody is the same, so the affinity between antigen and antibody is the calculation of between the antibodies.

The formula of the artificial immune system affinity is:

$$\left(A_g\right)_k = \frac{1}{1+t_k}. \tag{1}$$

t_k is the binding strength between antigen and antibody k

Artificial immune algorithm t_k mainly includes the following several space calculation formulas:

The Hamming distance of Hamming space is:

$$D = \sum_{i=1}^{L} \delta \begin{cases} \delta = 1, & ab_i \neq ag_i \\ \delta = 0, & other \end{cases}. \tag{2}$$

The Euclidena distance of Euclidena form space is:

$$D = \sqrt{\sum_{i=1}^{L} \left(x_i - y_i\right)^2}. \tag{3}$$

The Manhattan distance of Manhattan form space is:

$$D = \sqrt{\sum_{i=1}^{L} |x_i - y_i|}. \quad (4)$$

The artificial immune system algorithm generally has the following several parts: randomly created antibodies and antigens, antibodies and antigen matching, evaluating the antibody according to the affinity, using standard genetic algorithm to evolutes antibodies. This paper mainly introduces the principle and characteristics of artificial immune system, and compares with the intrusion system, finally establishes the network attack detection system of artificial immune model.

Network Intrusion Detection System based on Artificial Immune Model

In recent years, with the rapid development of intrusion detection technology, it has been recognized, and some have been commercialized, but artificial immune system still has certain defect, it needs to explore and improve [21-23]. The high efficiency of intrusion detection system generally has the function of artificial intelligence, which can be adaptive, self-learning and handle the foreign attack. This paper combines the artificial immune model with intrusion detection system, and put forwards the network intrusion detection system based on improved dynamic clone selection algorithm. The model of network intrusion detection system is as shown in Figure 3.

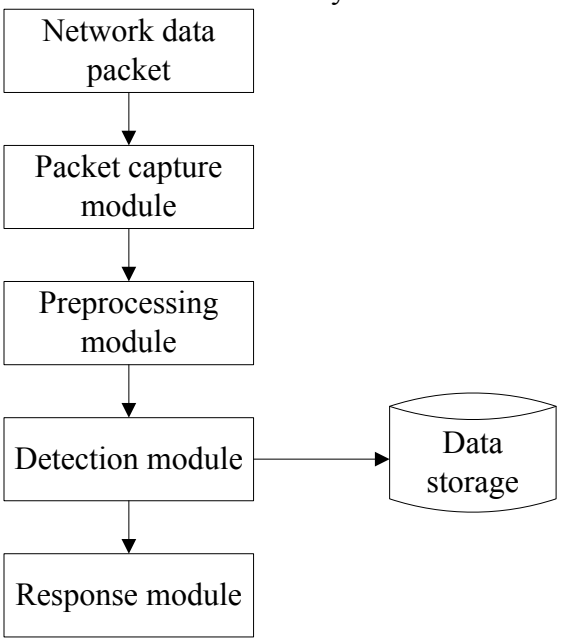

Fig.3 Network intrusion detection system model

As shown in Figure 3, the work principle of the network intrusion detection system is: the data packet capture module to acquire the information through the network for the CPU, which is equivalent to the front-end sensor of the intelligent control system; the preprocessing module analyzes and processes the information acquired by the data packet capture module, then the network state characteristics are encoded, and the encoding information is transmitted to the detection module; in the process of testing module, it improves the dynamic selection algorithm and records the optimization algorithm. If the detection module determines the data packet is an intrusion behavior, it will send out alarm information to the host and store the information in the database for verification in late time.

Simulation Experiment and Analysis

This chapter mainly uses software to do simulation on the model and algorithm, explores the feasibility of the whole system and studies the validity of the model according to the result of the experiment. Experiments are carried out in two steps, the first step is to build the model, and the second step is to test the intrusion. DOS, Probes and U-R packets are attacked in the test, which

contains a large number of ICMP packets, and then test the intrusion model in many times. Test results are shown in Table 1. The correct rate of intrusion detection in the world is shown in Table 2.

Table 1. Test results of various intrusion events

Attack type	Test correct rate (%)	Average correct rate (%)	Error rate (%)
DOS	58.62	58.12	33.12
Probes	61.23		
U-R	0		

Table 2. Internationally recognized intrusion detection correct rate

Software system	Correct detection rate (%)
DOS	55.48
Forensics	50.43
Expert1	46.72
Expert1	41.12

From the above table it can be seen, the main categories of the data attack are more, the detection accuracy of Probes is relatively high, the overall error rate is relatively low, compared with the results of the international intrusion detection system, the model has stronger learning ability, the advantage is more prominent, so it can increase the correct rate of intrusion detection.

Summary

Malicious code is always the cancer of the internet application, which brings a huge security threat to network users, enterprises and national departments, and it is extremely easy to cause the leakage of important information and cause significant economic losses of property. There is a lot of antivirus software on the market, they ensure the security of network information, but they are in passive position when it is against foreign invasion. In order to achieve more effective against malicious code, this paper firstly introduces and analyzes the artificial immune model and network intrusion detection system, and gives the way and strategy of network intrusion detection system to deal with foreign aggression. The intrusion detection system has the function of self organization, learning and memory, and it has important practical value for the following defense.

References

[1] L.J. Gu. Research and implementation of distributed firewall based on IPSec. East China Normal University, 2013: 1-9.

[2] Z.H. Zhu. Research and application of system calls in intrusion detection. Guangdong University of Technology, 2013: 3-11.

[3] X.S. Chen, H.B. Yin, D.J. Xiao. The event correlation analysis of intrusion detection. Journal of Huazhong University of science and Technology, 2013(4): 30-33.

[4] R. Zhang, D.P. Qian. Research on intrusion detection technology. Micro computer system, 2013(7):1113-1118.

[5] P. Jiang. Network intrusion detection technology. Journal of Zhengzhou Institute of Aeronautics Industry Management, 2013(3):108-110.

[6] L. Zhou, R.X. Li. On computer network security. Scientific and technical information, 2013(11): 79-80.

[7] Y.Q. Wang. Research status and Prospect of intrusion detection system. Communication technology, 2014(11):139-143.

[8] J.F. Wang, Hu J.. Research and exploration of Windows system security. Electronic design engineering, 2013(8): 40-43.

[9] S.L. Hou. Preliminary research on the intrusion detection system. 2014(29): 69-70.

[10] L. Yang. The design and implementation of network security monitoring system. Sichuan University, 2014: 1-12.

[11] Y. Yu. Research on real time intrusion detection technology based on neural network theory. Chongqing University, 2013: 3-12.

[12] D. Yin. Research and design of intrusion detection system based on immune mechanism. Hebei University of Technology, 2013: 2-13.

[13] L.Z. Liu. Research and implementation of intrusion detection model based on information fusion. Shandong University, 2013: 7-18.

[14] Q.J. Lu. Research on network intrusion detection algorithm of based on artificial immune. Changsha University of Science and Technology, 2014: 3-12.

[15] X.Z. Duanmu. Campus network security model based on intrusion detection technology. Shandong University of Science and Technology, 2013: 1-9.

[16] L.X. Gan. The application and its implementation of intrusion detection technology in campus network. University of Electronic Science and technology, 2013: 2-15.

[17] Y.L. Dai. The design and implementation of intrusion detection system based on support vector machine and Agent technology. Beijing University of Posts and Telecommunications, 2014: 6-13.

[18] L.J. Yao. Network intrusion detection technology. Software guide, 2013(6): 160-162.

[19] P. Deng, Z.Y. Zhao. Analysis of manual detection method and defect based on server intrusion. Office automation, 2013(14): 26-27.

[20] X.M. Wu. Research on two typical intrusion detection methods. Computer engineering and applications, 2013(10): 181-184.

[21] X.G. Pan.. Analysis of a detection and defense DDoS attack model based on user trust value. Coal technology, 2014(2): 170-172.

[22] L.L. Xie. Analysis of the application and realization of intrusion detection technology in the campus network. Computer optical disc software and applications, 2014(20): 81-82.

[23] H.S. Zhang. Research and implementation of automatic intrusion response system. Qiingdao University, 2013: 2-16.