ATLANTIS PRESS

Advances in Engineering Research, volume 123

2nd International Conference on Materials Science, Machinery and Energy Engineering (MSMEE 2017)

Research on network intrusion detection technology in dynamic and complex background

Zheng Wen-kui*,Liu kun

School of Software, Henan University, Kaifeng 475004, China

zhengwenkuisja@163.com

Key word：Digital image processing;Edge detection;Algorithm;Research

Abstract.

With the advent of the Internet era, the network has been widely used in production and life, and network security has become a hot topic. Nowadays, the traditional prevention technology is difficult to prevent the various increasing network attacks. There is an urgent need for a complex network intrusion detection technology to ensure the normal use of the network. According to the above problems, this paper studies the problem of network intrusion detection technology in dynamic and complex background. This paper introduces the network intrusion detection technology under dynamic background, and expounds the basic idea of detection, detection system model and packet capture device of detection system, and then analyzes the technical advantages of the detection system. the experiment proves that the network intrusion detection system can detect intrusion quickly and accurately to prevent intrusion.

1 Introduction

In recent years, Internet technology has been rapid development, and brought a variety of problems, one of the most prominent problems is the network security issue. The most commonly used network security technology for these problems mainly includes character encryption technology and verification code recognition technology, scanning authentication and authority control technology, firewall technology and intrusion detection technology.

Intrusion detection technology is the process of detecting an attempt to commit an illegal intrusion or illegal theft. Intrusion detection technology system is composed of hardware and software systems. The intrusion detection technology can complement the firewall vulnerabilities to reduce the probability of network attack, expand the security management system functions, and effectively enhance the computer security. The intrusion detection technology system uses the network data packet as the intrusion detection information source. Intrusion detection technology mainly provides effective detection and protection for network information.

The current intrusion detection methods are divided into two types: abuse detection method and anomaly detection method. Abuse detection method is mainly carried out on the detection of various means of invasion, can be targeted to find a collection of offensive features. One main feature of the abuse detection is the detection of known attacks, and the detection results are accurate. The downside is that it can only detect attacks that have already been made, and those that have not yet been made but have a set of attack features can not be detected, and it requires real-time data updates. The advantage of the anomaly detection method is that it can detect unknown attacks, but the detection accuracy is very low [1].

Through the analysis of the above situation, the paper integrates a new type of technology with intrusion detection technology, and presents a set if implementation scenarios while describing the the performance of the detection system, and finally verify the effectiveness through experiments.

2 Network intrusion detection technology in dynamic complex background

Basic ideas of the measurement. Data mining refers to the mining of data from a large number of data sets, and the data mined generally implies some confidential messages or decisions that are useful for decision making. Integrating data mining technology and intrusion detection technology, we can automatically find the relevant useful data from the massive information, therefore reduce the amount of manual labor as well as the amount of queries to the server. In the data mining technology, the clustering analysis algorithm can simulate the data model of the normal network data packet, and can also simulate the data model with the intrusion behavior. It can judge whether the attack data is invaded by comparing the simulated data model [2 -3].

Intrusion detection method also has the exception detection function. Correctly simulating the normal network packet model is the key to the anomaly detection, and the clustering analysis algorithm in data mining technology provides us with a good solution. The clustering analysis algorithm in data mining technology can automatically generate normal network packet model to facilitate the anomaly detection. Anomaly detection can also filter the data at the same time, filter out the data of the same type as the model, and filter out the data that is different from the model, thus realizing the effect of isolation prevention.

Detection system model. According to the above theory, this paper presents a system model that combines the data mining technology and the intrusion detection technology organically. The new detection system model shown in Figure 1.

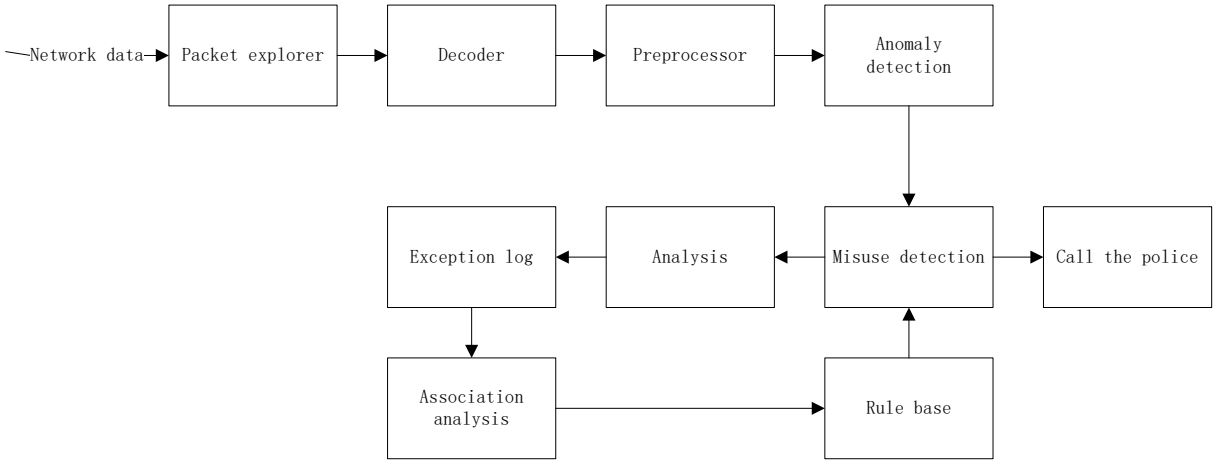

Figure 1 System model

Intrusion detection technology already has a packet search device, programming converter, data simulator, rights search engine, information alarm system and effective database. Through the above research, we know only a model comparison module, clustering analysis module, and data record analysis system need to be added.

Packet capture for detection system. The packet capture system is the preparation for intrusion detection. With the rapid growth of current network traffic, conventional packet capture methods have been unable to meet the needs of intrusion detection. The study found that the average size of the normal packets in the network is typically up to 500 bits. According to this ratio, the gigabit bandwidth network can capture about 300,000 packets per second. In the peak period, the number of captured packets will be much higher than this value, so the task is quite difficult to be completed. Therefore, it is necessary to use the high-speed packet capture device to effectively capture the packet. At the same time, the packet capturer need to be upgraded [4-5].

3 The technical advantages of the new detection system

Clustering analysis. First, the data need to be preprocessed, which makes the cluster analysis and calculation easier. The packets captured by the data capturer of intrusion detection technology system will have many attributes, some of which do not meet the requirement for cluster analysis calculations. Therefore, a certain type of attribute exclusion is needed. After that, we need to quantify the different data packets, so as to effectively reduce the impact of different attributes on the calculation. In this article, the following formula is used to effectively quantify the data packets [6].

$$X = \frac{B - M_1}{S_d}$$

In the formula: X represents the data packet quantization parameter; B is the value coefficient of the packet attribute; M1 and Sd are the average coefficients and the average error coefficient corresponding to B [7-8].

2 Similarity calculation. Conventional calculation methods can only be applied to the calculation of continuous data, when encountered discrete data, the conventional calculation method can not effectively calculate the results [9]. For discrete data, the Manhattan distance can generally be used to compare the similarity between the data models.
For continuous data generally use the following formula for comparison.

$$f_a(i, j) = \left|X_{i1} - X_{j1}\right| + \left|X_{i2} - X_{j2}\right| + \cdots + \left|X_{iP} - X_{jp}\right|$$

For discrete data, the following formula is used for comparison

$$sim(ir, jr) = \begin{cases} 0, & \text{if} y_{iz} = y_{jz} \\ 1, & \text{f} y_{iz} \neq y_{jz} \end{cases}$$

$$f_b(i, j) = sim(y_{i1}, y_{j1}) + sim(y_{i2}, y_{j2}) + \cdots + sim(y_{iq}, y_{jq})$$

In the formula: y_{iz} and y_j are the p-th discrete coefficient values of data i and data j, and F (i, j) is the sum of all the similarity of the discrete coefficients between data i and data j. The similarity between i data and j data is f (i, j), that is,

$$f(i, j) = f_a(i, j) + f_b(i, j)$$

Anomaly Detection. The data processor of the intrusion detection technology system accepts the form of the plug-in. We can connect search engine of the anomaly detection in the form of plug-ins, thus facilitating the abnormal detection for the intrusion detection technology system. We compare the data from the anomaly detection engine and the simulated data model calculated by the cluster analysis, while recording and editing the source of the data to facilitate the effective tracking [10].

Figure 2 is the flow chart of the anomaly detection. It can be concluded from the chart that the anomaly detection process can be divided into following steps

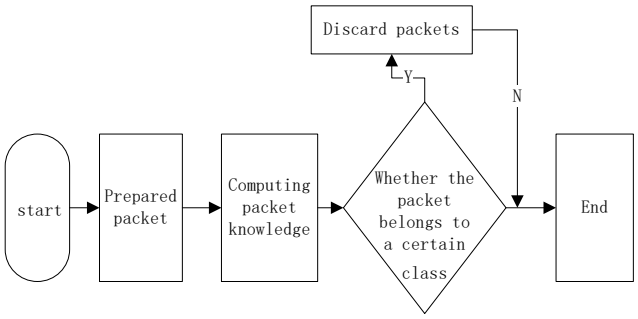

Figure 2 flow chart of the anomaly detection

1 Quantify the searched packets;
2 Compare the similarity between the data packet and the simulated data model;
3 If the similarity is less than a certain value, abandon the packet, otherwise alarm.

4 Test

4.1 Test environment

1 hardware environment: CPU: AMD Athlon win7 2024 + (2.66 G), memory: 1.5G.
2 Software Environment: Operating System: win7, Database System: Oracle 5.2.36, Snort Version: 2.6.1

4.2 Test methods

1 Random access to multiple data packets on the network, through simple statistical calculations, we could get the average value of the continuous attribute and the average error value for the standardization of comparison.
2 Use intrusion detection technology for one hour of network packet detection, and save the results to the specified folder. During the detection period, the computer normally uploaded and downloaded web files. Specify a key folder to hold the normal data as comparison model.
3 We use 7 ways to simulate attacks the computers, and save the attack packets to the key folder, through which we can better evaluate the established network intrusion detection system. According to the error rate of the search engine for anomaly detection, we can intuitively evaluate the established intrusion detection system.

4.3 Results and Analysis

Model evaluation: Table 1 and Table 2 records the comparison results and the error rate of the anomaly detection of the simulated data model of the intrusion data. Through analysis, we find that the error rate varies with the change of the cluster analysis, and the error rate increases with the value calculated by the cluster analysis, and vice versa. When the value of the cluster analysis is too large, the coincidence rate of the attack data packet with the conventional data comparison model becomes smaller, which is the reason for the change of the error rate of the calculated value of the cluster analysis. In addition, when the number of packets of an attack type is to large, the intrusion detection system will define this type of data packet as normal packet by default. So we have to set a certain threshold for intrusion detection, which can effectively prevent the occurrence of such vulnerabilities

Table 1 changes in error rate

θ	100	150	200	250	300	350
Error rate %	2.09	1.84	1.76	1.55	0.98	0.60

Table 2 Error rate change with clustering analysis changes in calculated values

R	1	2	3	4	5	6	7	8	9
Error rate	0	0	0	0.058	0.042	0.979	1.869	5.026	9.459

5 Conclusion

In this paper, the research of network intrusion detection technology in dynamic and complex background is studied deeply, and it can effectively detect the intrusion data by combining the data mining technology and intrusion detection technology. At the same time, for the rapid development of the network, advances data packet capture devices are used to implement rapid and effective real-time dynamic data detection. It is hoped that the research of this paper can provide an effective theoretical basis for the application of intrusion detection system.

Reference

[1] Ahmed A, Bakar K A, Channa M I, et al. A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks[J]. Frontiers of Computer Science, 2015, 9(2):280-296.

[2] Korczynski M, Hamieh A, Huh J H, et al. Hive oversight for network intrusion early warning using DIAMoND: a bee-inspired method for fully distributed cyber defense[J]. IEEE Communications Magazine, 2016, 54(6):60-67.

[3] Malialis K, Devlin S, Kudenko D. Distributed reinforcement learning for adaptive and robust network intrusion response[J]. Connection Science, 2015, 27(3):1-19.

[4] Shahrestani S A. Employing artificial immunology and approximate reasoning models for enhanced network intrusion detection[J]. Vacuum, 2016, 22(4):284.

[5] Christian B, Lozano J A, Pedro Pinacho D. An artificial bioindicator system for network intrusion detection[J]. Artificial Life, 2015, 21(2):93-118.

[6] Yu Y, Ye Z, Zheng X, et al. An efficient cascaded method for network intrusion detection based on extreme learning machines[J]. Journal of Supercomputing, 2016:1-16.

[7] Hodo E, Bellekens X, Hamilton A, et al. Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System[J]. Tetrahedron Letters, 2017, 42(39):6865-6867.

[8] Raman M R, Somu N, Kirthivasan K, et al. A Hypergraph and Arithmetic Residue-based Probabilistic Neural Network for classification in Intrusion Detection Systems.[J]. Neural

Networks, 2017.

[9] Amar M, Achheb A E, Souhel A, et al. Evaluation of a Monitoring Network of Seawater Intrusion in the Coast of El Jadida District, Morocco[J]. Applied Surface Science, 2015, 286(11 D):71-77.

[10] Bulbul R, Sapkota P, Ten C W, et al. Intrusion Evaluation of Communication Network Architectures for Power Substations[J]. IEEE Transactions on Power Delivery, 2015, 30(3):1372-1382.