Research on Intrusion Detection Technology Based on Artificial Intelligence Algorithms

Jing Huayang

Yunnan Arts University Wenhua College, Kunming, Yunnan, 650000, China

Keywords: Artificial Intelligence; Algorithms; Intrusion Detection Technology

Abstract: With the rapid development of information technology and computers, the number of attacks on the network is increasing, and a single firewall can no longer meet the needs of Internet users. The application of intrusion detection technology provides a security barrier for enterprise networks to be attacked. The emergence of intelligent algorithm intrusion detection system speeds up the speed of intrusion detection and the ability to prevent information. For example, record intrusion behavior, track intrusion behavior, recover or disconnect. This paper expounds the classification of intrusion detection technology, and verifies the effectiveness of the algorithm by analyzing intelligent detection technology and combining genetic algorithm and intrusion detection technology.

1. Introduction

Internet has the characteristics of openness, interconnection and sharing. It brings convenience to people, but also causes many security problems. The common network security problem is illegal intrusion. Illegal intrusion refers to the illegal access to computer networks without the permission of users. Intrusion detection is a network security defense system that can effectively compensate for the shortcomings of a single defense system, provide real-time intrusion detection for network security, and adopt corresponding defense methods.

2. Classification of Intrusion Detection Technology

2.1 Data Sources

From the data point of view, intrusion detection can be divided into three categories: host intrusion detection, network intrusion detection and web log intrusion detection. Host-based intrusion detection is an agent running on a single host or running on multiple hosts. As a detection engine, data is collected, analyzed, and judged. By analyzing the characteristics of the host behavior library to determine whether to invade, the alarm information is sent. The control endpoint is managed by the administrator.

Network-based intrusion detection data mainly collects network data stream, extracts network data packet features and compares them with attack patterns in knowledge base, and then detects them. This intrusion mode consumes less host and is transparent to intruders, so it can protect network system in general. The object of network intrusion analysis is the network protocol. Generally, the standardization is independent of the type of the host operating system, so there is no portability problem, but the disadvantage is that the accuracy is poor, it is difficult to configure, and the anti-spoofing ability is also poor.

Based on web log-based intrusion detection, intruders will keep their traces in the system log, and using system log files and audit information is an effective means of detecting intrusions. There is systematic and unusual activity evidence on the log, which can be used to discover that someone is intruding or has intruded into the system. Log files can detect intrusion attempts and how entities communicate.

  DOI: 10.25236/isaicn.2019.011

2.2 Test Method

Intrusion detection methods can be divided into anomaly intrusion detection and misuse intrusion detection. The key problem of anomaly detection is the choice of its features. First of all, anomaly detection should establish a system that can cover the behavior characteristics of the system or users with a small number of features. Another key is the choice of reference threshold. Selection conference can improve the rate of false alarm, and smaller threshold will increase the rate of false alarm. Misuse detection mainly analyses and finds out all kinds of attack means and attacking features. After processing the data sources by the detected features or rule sets, the matching work is carried out. It is found that an attack will occur if the matching conditions are satisfied. The key to misuse detection analysis is to indicate the correct attack signature, that is, how to make the attack signature accurately represent all the possibilities of the intrusion behavior without including the intrusion behavior. Intrusion is the use of system vulnerabilities and application flaws. According to the characteristics, conditions, permutations and events of the attack, the intrusion behavior can be analyzed. Can help analyze intrusion behavior and make early warnings. Although the misuse detection has a high detection rate and a low false alarm rate, it also has the disadvantages of high false negative rate and strong correlation with the system. Different mechanisms on different operating systems have different attack methods, and it is difficult to form a unified pattern library.

2.3 Intrusion Mode of Work

According to the way the system works, it can be divided into two categories: offline detection and online monitoring. Offline detection is non-real-time. After the event occurs, the intrusion event is detected by analyzing the audit event. The advantage is that the system cost is low, and a large number of events can be analyzed to facilitate the establishment of the model. However, it can not provide timely protection for the system after the event, and if the event occurs and the audit event is deleted, it will not work. Online detection system mainly detects network data packets and host audit events. It has fast response and can protect system security in time. However, when the system is large, it can not be protected in real time.

3. Intelligent Intrusion Detection Technology

3.1 Neural Network Intrusion Detection Technology

Artificial neural network (ANN) is an intelligent information processing technology which simulates the human brain in processing, storing and processing information. ANN has a high learning and adaptive ability. It can learn the input samples and abnormal samples. ANN can recognize the known intrusion behavior characteristics in the samples, and can recognize new intrusion characteristics through existing experience. Variant patterns with existing intrusion characteristics. Through this learning, new intrusion behavior characteristics can be identified and expert detection system can break through the original limitations. Neural networks have inherent parallel computing and storage characteristics. Traditional computers are divided into two parts: computation and storage. The transmission width between memory and calculator limits the performance of the computer. In the neural network model, information storage and information processing are combined into one. Each neural network works completely in parallel, and the storage process is completed while transmitting. This calculation mode can process more detection rules in a short time and discover intrusion behavior, which reduces the loss of the system.

3.2 Data Fusion Intrusion Detection Technology

Data fusion is a multi-level and multi-faceted processing process, in which data resources are detected, combined, correlated, estimated and combined, and accurate state and identity estimates are achieved, as well as situation assessment and threat assessment. The shortcomings are as follows: firstly, the technology of IDS system is not mature enough to detect complex and covert attacks initiated by hackers. Secondly, the intrusion detection system can not identify false alarms in

time. Finally, a large number of data systems cannot be processed in time, which wastes the processing power and detection performance of the IDS system. Multi-sensor data fusion technology can solve the above problems and help to evaluate the environmental security performance of the entire network. A variety of network data packets, system log files, SNMP information, user profile information, etc. can be obtained from the sniffer. The system input can estimate the identity and location of the intruder, and perform the activity information, the danger information, and the attack information level of the intruder. Evaluation. However, intrusion detection data fusion technology is also threatened, for example, the development of a common structured meta-language to describe intrusion detection and network management objects and dynamic network attack behavior.

3.3 Computer Immunology Intrusion Detection Technology

Inspired by the biological immune mechanism, computer immune technology has been formed. Because computer networks are prone to intrusion due to errors in computer programs, intrusion detection technology must be based on this reality. Biological immune system is a system to deal with vulnerable factors in biological systems, and to identify abnormal features to determine the allogeneic classification. Cloth condition and repair characteristics. Compared with existing computer security systems, the biological immune system has the following advantages: multi-layered protection mechanisms, natural organisms often have multiple layers of protection mechanisms to prevent external invasion, such as skin tissue on the surface of the body or internal pH acidic environment. , as well as white blood cells, lymphocytes, and the like. The current computer security system has only a single protection mechanism, such as a firewall, and the firewall only defines a layer of security boundaries. Once this layer of security is breached, it will affect the operation of the computer.

Highly distributed detection and memory systems, biological immune system detection and memory systems are highly distributed, the immune system operates by a highly distributed single detector interacting with local neural receptors, the ability to assign the number of immunizations as needed, Unlike a computer with a central control point to manage the detection and response of the entire immune system.

3.4 Diversified Individual Detection Ability

Different immune cells and molecules make up different biological individuals. Today's computer security systems use the same software to protect all the sites in the system, so that it is easy for an attacker to find a way to avoid attacks. The attack method for all sites.

The biological immune system can recognize unknown foreign bodies. It usually reacts to the types of external infections that have been discovered before it can deal with the new unknown types of infections. At the same time, the immune system can evolve new detectors for infected pathogens to identify and treat such pathogen types. Although the process of dealing with new infection types is slow, the immune system does recognize undiscovered foreign bodies. Most of the capabilities that security systems do not have.

4. Intrusion Detection Technology Based on Genetic Algorithms and Neural Networks

4.1 Genetic Algorithm

Genetic algorithm is a group search algorithm based on Darwin's natural selection and Mendel genetics principle [1], which is suitable for solving complex and nonlinear problems that are difficult to solve by traditional algorithms. The technology realizes computer by simulating the process of biological genetics and evolution. The ability of autonomous learning and independent optimization and adaptation is widely used in combinatorial optimization, adaptive control, intelligent manufacturing, and artificial intelligence. Compared with other search algorithms, it has the following characteristics: taking the coding of decision variables as the object, imitating the inheritance and evolution in nature, and facilitating the operation of genetic algorithm. It is possible

to find the local optimal solution by group optimization from multiple points. The population is selected by fitness function. Genetic algorithm is widely used and has no restriction on objective function. The search probability of genetic algorithm is high, and it has the characteristics of large-scale calculation.

4.2 Intrusion Technology Based on Genetic Algorithms and Neural Networks

Neural network has been developed rapidly in many aspects [2], and has been applied to various fields of computer. For example: intelligent recognition, pattern recognition, signal processing. However, there are still some problems, and the genetic algorithm can solve the problems in the neural network by using its powerful search function, and at the same time avoid the situation that the independent application genetic algorithm is not easy to find the optimal solution in a short time.

The first is to encode the neuron connection values existing in the neural network into binary codes to represent the individual [3], and then use an algorithm to optimize the calculation. The fitness is determined by calculating the average error produced by the samples used in the neural network. When the optimization design solves the complex problem large-scale neural network, the search space of the genetic algorithm can be increased. Secondly, genetic algorithm is used to optimize the structure of the neural network and the learning rules and related parameters of the neural network. Each selected individual is coded into a trained neural network, and then the neural network is trained to determine its connection weight, so the search space of genetic algorithm will be reduced.

5. Conclusion

According to the actual needs of intrusion detection work [4], this paper proposes to apply artificial intelligence algorithm to enterprise intrusion detection system. The system uses genetic algorithm and intelligent technology, which has practical significance for improving the efficiency of intrusion detection system. Intrusion Detection System (IDS) is a multi-disciplinary system technology, involving many complex technologies. For example: artificial intelligence technology [5], network technology, software technology and so on. This paper only deals with intrusion techniques based on neural networks and genetic algorithms [6], and with the continuous development and integration of the two, it can be applied in many fields, but in many aspects, further improvement is needed. For example, the communication problems between the agents and the target model, I hope that the relevant personnel can continue to work hard.

References

[1] Gaota, Tian Yuxin. Artificial Intelligence Application Research in Big Data Age of Computer Network Technology [J]. Management and Technology of Small and Medium-sized Enterprises (Previous Periodicals), 2018 (06): 142-143.

[2] Tan Huan-fu, Homeich. Research on a Network Intrusion Detection Model [J]. Industrial Instruments and Automation Devices, 2017 (1): 123-125.

[3] Jiao Baochen, Liu Zhenchang, Chen Shiming, et al. Intrusion Detection Algorithms, three categories [J]. China Education Network, 2015 (6): 76-78.

[4] Zhang Ling. Research on Intrusion Detection Model Based on Rough Set and Artificial Immunity [D]. Beijing University of Posts and Telecommunications, 2014.

[5] Liu Mengyong, Xin Yan. Current situation and future of intrusion detection technology [J]. Science and technology enrichment guide, 2014 (2): 119-119.

[6] Anna Wang. Research on Intelligent Intrusion Detection System in Pattern Recognition Environment [J]. Electronic Technology and Software Engineering, 2015 (14): 234-234.