Research on the Network Anomaly Detection and Tracking Information Methodology based on Cellular Automata

Qingru Sui
Changchun University Of Science And Technology,
Jilin Changchun 130600

Xiaoyan Liu
Changchun University Of Science And Technology,
Jilin Changchun 130600

Abstract. In this paper, we conduct theoretical research and analysis on the network anomaly detection and tracking information methodology based on cellular automata. Intrusion detection is a computer network and monitoring system to discovery of violation of security policy events. Intrusion detection system will work in the computer network key nodes in the salt system, through the real-time collection and analysis the information in the computer network or system. Our method is proved to be feasible and robust, in the near future, we will conduct more related research.

Keywords: Anomaly Detection; Tracking Information; Cellular Automata; System Modelling.

Introduction

Intrusion detection as a kind of active safety protection measures, computer network and information security protection in play an important role and with the high-speed development of Internet, new technologies such as load balancing of various kinds of intrusion detection. Protocol analysis, is to use protocol packet message format information, refer to a specific protocol specification, detailed according to protocol state detection message implied in the attack, to think the exception message, again in accordance with the method of pattern matching to match against. Protocol analysis mainly includes the state of decoding and tracking of two parts, before the protocol analysis, and a protocol recognition process. Intrusion detection is a computer network and monitoring system to discovery of violation of security policy events. Intrusion detection system to work in a computer network key nodes in the salt system, through the real-time collection and analysis the information in the computer network or system, to check whether any signs of violation of security policy and attack, and thus achieve the goal of prevent attacks, prevent attack. Application of intrusion detection system, the invasion attack can be detected before the system hazards, and use the alarm and protection system response, thus reducing the loss caused by intrusion attack. Intrusion behavior constitutes a threat to the system, and many of the safety programs are written for some kind of threat. Threat is defined as the potential harm any circumstances and events in the system, it is wider. Threats can be divided into intentional and accidental. The threat of intentional and can be further divided into active attack and passive attack. Passive attack does not result in any changes to information contained in the system, such as wiretapping, traffic analysis and the main threat to information privacy. Attack aimed to tamper with the system contained in the information, or change the status of the system and operation, so take the initiative to attack the main threat of integrity, and availability of information [1].

Cellular automata is defined on a discrete cellular space and related local updating rules as time changes, evolving a system mainly includes a complete cellular automata cellular, neighbors, cell and the space evolution rules. In daily life, many things are not clear and not accurate, and the information is not usually clear and not accurate [2]. Cellular automata component known as the basic cell, every cell in the same time only one state, all cellular automata rules is arranged in the cellular space online. Cellular automata by local rules to describe the specific behavior of each cell If we ignore this kind of situation which is not rigorous, on the basis of the obtained conclusion is often not too conforms to the real situation. Network security defense must adopt a kind of deep, a variety of means, to form a multi-level protection system which is no longer a single security technology and security strategy, but the mix of technology, the key is to various security technology can play the role of complement each other, so, even when a certain efficiency which can compensate other security measures. Using the idea of expert system to build the intrusion detection system is one of the commonly used methods. Especially the expert system with self-learning ability, realize the updating of the knowledge base and expand, make a design of intrusion detection system's defensive ability, should have a wider application prospect. The concept of application agent for intrusion detection attempts has been reported. Relatively consistent solutions should be effective under the conventional definition of intrusion detection system with intelligent detection function of the software or module used in the general combination [3].

To enhance the current method, we conduct research on the network anomaly detection and tracking information methodology based on cellular automata. Security policy in the center position, but from another perspective, the security strategy is to develop in the intrusion detection strategy is an important source of information, according to the existing intrusion detection systems need leopard security policy information to better known configuration parameter information system module, when found after the intrusion behavior, intrusion detection systems through the corresponding module change system of protective measures, improve the protection system, so as to realize the system of dynamic security model. In the following sections, we will discuss in detail.

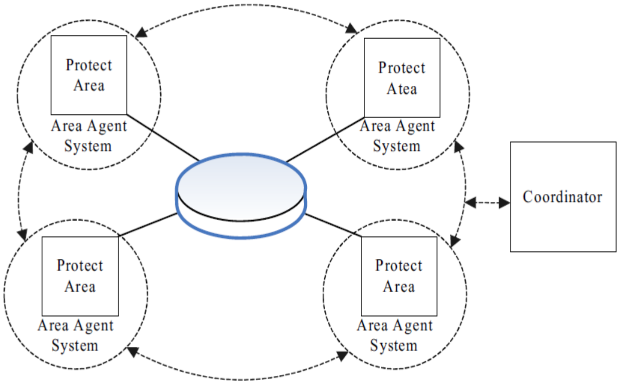

Fig. 1The General Structure of the Network Anomaly Detection System

The Proposed Methodology and Approach

The Basic Concepts of Anomaly Detection. People through the computer network, has realized the rapid spread of information and information resources sharing, not only to promote social resources are fully utilized, but also constantly increase the wealth of the society. Also because of this, led to some criminals use the technique of computer network in order to attack, attack computer network connection to the Internet and computers. Use safety engineering risk management idea and method to deal with the network security problems, network security as a whole project to deal with. Based on the network and network intrusion detection system based on host combination, these two methods have their own advantages, the two complement each other. These two approaches can find each other can't detect some of the intrusion behavior. Such as host-based intrusion detection systems using the system log as the detection basis, so they succeed in determine whether attack has been compared with the detection system based on network with greater accuracy.

According to different focus, the network intrusion detection system can be divided into different levels. According to the data source, network intrusion detection system can be divided into host-based network intrusion detection system and network intrusion detection system based on network. According to the data analysis method and the detection mechanism, intrusion detection system can be divided into abnormal intrusion detection system and misuse intrusion detection system. According to the system architecture, adopted by the detection system can be divided into centralized intrusion detection systems and intrusion detection system. Host-based intrusion detection system for the early structure of intrusion detection system, using host detection engine to gather the information of this system, can be used in a distributed, encryption, and the exchange of environment, the specific problems associated with a particular user. In the process of detection, using the active way, before the invasion attacks pose a threat to network security, detect intrusion attack, and use alarm and intercept attack way to stop the attack. Intrusion detection system, not only can reduce the loss caused by invasion of network attack events, and, by being invaded, collect information of intrusion attack and carries on the analysis, the system knowledge of the event as a knowledge is added to the knowledge base. The goal of the test is mainly the host system and local users, such as when a database server need to be protected, to intrusion detection system installed on the server, to monitor the situation of the database access by user.

Intrusion detection system based on network is to use network listening techniques to collect grouping of network transmission data packets, and on the packet source address, destination address, port, and load content such as intrusion detection analysis, to find intrusion activities. General network intrusion detection system mounted on a network segment, assuming the task to protect the safety of the network segment which is shown in the figure two.

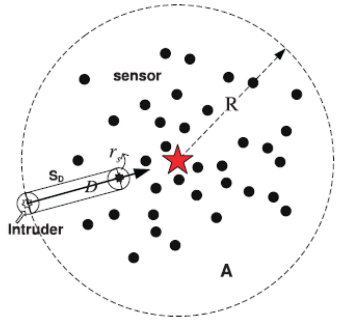

Fig. 2The General Protection Structure for the Network

The Cellular Automata. Cellular automata design idea of biology reproduce phenomenon, has been widely used in the field of computer science. Cellular automata model to study the dynamic, parallel and interactive system is very important. In recent years, along with the new concept of grid computing, cloud computing, distributed computing shows its strong vitality. However, the current distributed network generally can only provide brief and services, although there is some management ability, but it is still a lack of overall high autonomy ability, difficult to effectively manage the entire network resources, form a virtual green and efficient distributed network.

The unique cellular automaton evolution rules different from the traditional mathematical equations describing the similar biological self-configuring, self-healing, self-optimizing, protection, self-learning ability, and because of this, for the study of cellular automata more autonomy of distributed network provided. In order to improve the network distributed operation environment, this article try to mechanism of cellular automata into the distributed network, in order to achieve more efficient and intelligent distributed computing network. The dynamic evolution of cellular automata is state combination according to the overall evolution rules shown in the following formula.

$$F: S_z^t \to S_z^{t+1} \to S_z^{t+2} \ldots \to S_z^{t+n} \qquad (1)$$

Before the construction of the distributed computing model based on cellular automata, cellular automata as the basic unit of the distributed computing, its concept to expand, expand after the cellular automata model for composite cellular automata model, so as to meet the needs of actual distributed system. In previous applications of cellular automata, cellular evolution algorithm is basically a single cell as a unit, and contains only a simple state set, for the unit cell in order to realize their own evolution and parallel computing is very complicated which also ignore the cost of communication between different cell, cause deviation of actual application.

Because of the evolution of cellular automata flexibility, even if the yuan cell reached the edge of the network, it can still return a valid find nearby free cellular evolution, to go on distributed computing. Distributed computing model based on cellular automata is a composite use of cellular automata is the essentially similar to biological evolution mechanisms and intelligent cognitive characteristics and it has been used in distributed computing network. On the basis of the research on how to build a green and efficient distributed network, enhance network autonomous ability, improve the efficiency of the distributed network computing and reduce the time cost, can avoid some problems existing in today's distributed computing. In fact, based on the model of distributed network does not need a central server to coordinate involved in distributed computing, computer group, simply start the distributed computing on any computer, as long as the available computer resources exist in the distribution network, the distributed computing will automatically continue, not break, even some of the computer for disabled, composite cell still by the compound near the reconnection evolution rules, make the calculation to continue.

The Performance of the Cellular Automata based Technique. Protocol analysis using packet message format information and refer to the specific protocol standard, according to the protocol state detection message implied in the attack, in detail for that exception message, again in accordance with the method of pattern matching to match against. In according to the agreement, feature recognition network packets belong to some kind of agreement before without judgement, packets chain need to traverse protocol recognition, and fill the agreement in accordance with the contents of the packet data communication, sent to all the testing process. Packets to a network, according to the protocol specification, through the protocol decoding and analysis, the detection in the chain is not in conformity with the specification data packets into pattern matching. Therefore, protocol state analysis is introduced, reduces the need to detect the number of packets chain, improve the detection efficiency. Matching in order to make more accurate positioning, when parsing rules to establish detection chain, chain, not only need to be established in accordance with the port rules and should be under the rules of port chain, according to the agreement of the command key again to detect chain detailed division, in this way, it can improve the testing efficiency and accuracy. In the figure three, we illustrate the performance of the cellular automata based network anomaly detection method.

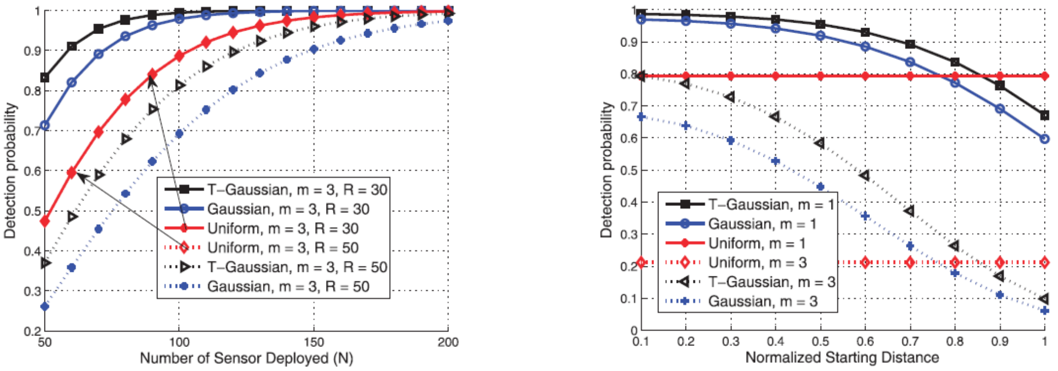

Fig. 3The Performance of the Cellular Automata based Network Anomaly Detection Method

Conclusion

In this paper, we conduct theoretical research and analysis on the network anomaly detection and tracking information methodology based on cellular automata. Due to the expanding of network size, the computer network to deal with network is becoming more and more serious in the form of internal and external threats. Firewall security model based on the original strategy has far cannot satisfy the requirement of people to network information security, intrusion detection alert natural become the hot topic of the research and development in the field of network security. In this paper, from the current status of the network security, the concept of intrusion detection and the development history and general intrusion detection model is analyzed which will be meaningful.

References

[1] Palmieri F, Fiore U, Castiglione A. A distributed approach to network anomaly detection based on independent component analysis[J]. Concurrency & Computation Practice & Experience, 2014.

[2] Yang L, Li G, Zhang P. Improved Wolf Step Prediction of Network Anomaly Flow Detection Method[J]. Bulletin of Science & Technology, 2014.

[3] Zhang T, Liao Q, Shi L. Bridging the Gap of Network Management and Anomaly Detection through Interactive Visualization[C]// Pacific Visualization Symposium (PacificVis), 2014 IEEE.