Research on Computer Network Technology System Based on Artificial Intelligence Technology

Jinling Yao¹, * and Jie Liu², ³

¹College of Electronic Information and Engineering, Tianjin Vocational institute, Tianjin 300000, China
²Tianjin Key Laboratory for Advanced Mechatronic System Design and Intelligent Control, School of Mechanical Engineering, Tianjin University of Technology, Tianjin 300384, China.
³National Demonstration Center for Experimental Mechanical and Electrical Engineering Education (Tianjin University of Technology), Tianjin 300384, China.

*Corresponding author: jinlingyao@tjtc.edu.cn

Abstract. This article introduces computer network intrusion detection systems and their classification based on artificial intelligence technology, and points out the challenges that intrusion detection systems (IDS) are facing in wireless sensor computer networks. On this basis, a hierarchical multi-layer wireless sensor network intrusion detection system and technology based on artificial intelligence technology Agent is proposed, and its network structure, working principle and performance are analysed.

1. Introduction

Intrusion detection technology is a new type of computer network security technology based on artificial intelligence technology that actively protects itself from attacks. It collects information such as operating systems, applications, and network packets to find violations of security policies or crises in systems and data streams. System security behaviour. The system designed for this purpose is called intrusion detection system (IDS). IDS is a very useful supplement to firewalls. It can not only detect attacks from external networks in real time, but also detect unauthorized activities from inside the network, effectively making up for the lack of firewalls, and is considered the second way behind firewalls. Security gate. A successful intrusion detection system can not only keep the system administrator aware of any changes in the entire network system, but also provide support for the formulation of network security strategies.

The existing distributed intrusion detection system usually adopts the following three analysis models for distributed intrusion: central analysis model, hierarchical analysis model, and collaborative analysis model. The central analysis model has a large network load, poor scalability, long delay, and single point of failure. It is only suitable for small-scale networks [1]. The problems of heavy network load and single point of failure of the analytic hierarchy model still exist. The collaborative analysis model has increased single-point complexity, poor scalability, heavy network transmission load, and so on. This paper uses the advantages of mobile agent and applies it to distributed intrusion detection, and proposes a distributed intrusion detection system based on mobile agent, trying to solve the problem of...
excessive network bandwidth usage, low detection efficiency, and robustness of traditional intrusion
detection models. Issues such as weak sex.

2. Intrusion Detection System

2.1. Intrusion detection technology
Intrusion detection refers to the technology for discovering internal unauthorized behaviours or external
intrusions, and is a technology for detecting violations of security policies in computer networks.
Intrusion detection system refers to the combination of software and hardware for intrusion detection,
and is a computer system that realizes intrusion detection behaviour. In the traditional sense, intrusion
detection system is the second security threshold after firewall.

2.2. Mobile Agent Technology
Agent is a software entity with intelligence and adaptability. A static agent resides in a certain fixed
position throughout its life cycle, while a mobile agent is an entity that can migrate from one network
node to another network node in any state and maintain the original operating state. It can complete
certain tasks on behalf of the user [2]. Specific tasks, such as data collection, information filtering, and
data retrieval, etc. At the same time, it will carry the processing results and return to the source device
by itself. This fundamentally reduces the burden on the network, shortens the network waiting time,
reduces network congestion, and has the characteristics of autonomy, reactivity, interactivity,
communication, flexibility, and mobility. In view of these advantages of mobile agent, it is very suitable
to construct a distributed intrusion detection model.

3. Agent-based intrusion detection system function design and implementation

3.1. Overall structure
In the system's physical topology network, components such as firewalls, routers, switches, hosts and
servers, together with network hosts, partition control centres, agent libraries, and control centres form
the overall system architecture as shown in Figure 1.

![Figure 1. Overall system architecture](image)

The description of each module is as follows: For the assistance of the control centre, using a highly
professional server control centre, the system administrator can use it to complete the update task of all
the rule sets. The sub-regional control centre controls the network host processing of a certain segment of the network and sub-networks. It is responsible for the task [3]. After receiving the control centre task, it orders the host under control to perform the task of receiving the reported information from the network host, and monitors abnormalities in the diagnosis information. In case of the situation, input the intrusion characteristic pattern into the database, and then report the analysis result to the control centre.

It consists of two parts, the chi-square flow determination model and the chi-square flow monitor. The chi-square flow determination model will further process the data in the SIP feature database to obtain the data used for the calculation of the chi-square statistic value. The chi-square flow monitor uses these data to calculate the chi-square statistic and judge whether an abnormality occurs. A detailed description of this process is given below. The analysis of the SIP session establishment process shows that the distribution of the number of SIP messages under normal conditions shows a stable distribution. These messages include INVITE, ACK, 200. In this article, it is shown that in the case of SIP single-source flooding attack, the attacker cannot complete the process of session establishment, which leads to the abnormal distribution of SIP messages [4]. Therefore, flooding attacks can be detected through changes in SIP message distribution. We use chi-square statistics to measure the similarity of SIP message distribution based on sliding time window sequence. The calculation method of chi-square statistics is as formula (1). Among them, \( k = 3 \), \( n_i \) represents the proportion of message \( msg \), in the current time window, and \( n'_i \) represents the proportion of \( msg \), in the previous time window. \( msg \) are three types of SIP messages: INVITE, ACK, and 200.

\[
\chi^2 = \sum_{i=1}^{k} \left( \frac{n_i - n'_i}{n'_i} \right)^2
\]

The web host is a mobile agent platform that can provide an operating environment for mobile. If the web host prioritizes the suspected situation, but cannot judge by itself, then the relevant data will be fed back to the district control centre, and then a deeper analysis and processing will be carried out to discover whether the host computer invades the network. Agent library plays an important role in the process of intrusion detection system [5]. Especially in the execution operation, the control centre directly controls the management part, so that the new configuration that can be generated can perform corresponding work according to actual needs, and the original execution can be reconfigured and deleted. What is no longer needed can be achieved. Figure 2 is a schematic diagram of the relationship between the various modules.

![Figure 2. Schematic diagram of the relationship between the main modules](image-url)
3.2. Function analysis

3.2.1. Detector layer. This layer provides multiple types of detectors to collect raw data from the network, host, and other devices.

3.2.2. Collaborative analyser layer. This layer provides a corresponding analyser for each detector. Each analyser can identify intrusions based on the knowledge of the ontology, and send collaborative analysis commands to other analysers when needed. Each cooperative detector and its corresponding detector form an intrusion detection agent. For example, a host detector and a host cooperative analyser form a host intrusion detection agent. Each collaborative analyser has a local ontology knowledge base, which can complete detection tasks independently, and can also work with other intrusion detection agents [6]. The intrusion detection agent can automatically cache the relevant data of the global intrusion detection ontology knowledge base to the local according to the different management probes, forming its own local ontology knowledge base, reducing a lot of communication burden.

3.2.3. Knowledge management. On the one hand, this layer maintains the ontology knowledge base and maintains the consistency of ontology knowledge; on the other hand, it alarms when an attack is detected and takes corresponding response measures. This layer includes knowledge base update component, blackboard, alarm fusion component and alarm console. The knowledge base update component is used for administrators to maintain and update the knowledge base of intrusion detection ontology; the blackboard is mainly used for the collaboration of multiple detectors to store each agent Access addresses, alarm message lists, and data required for collaboration; the alarm fusion component mainly merges alarm information; the alarm console provides a user interface with the network administrator, and outputs alarms or sends alarm emails on the screen. The knowledge management agent composed of knowledge base update component, blackboard, alarm fusion component and alarm console complete functions such as collaborative data forwarding, alarm fusion, and maintenance of the intrusion detection ontology knowledge base.

4. Experimental simulation

MADIDS is compatible with traditional detection algorithms. In order to make a more comprehensive and representative MADIDS test, network-based and host-based detection algorithms are used.

4.1. Network-based detection

Analyse the flow direction of the control packet, the flow and content of the data packet by checking the data packet information flowing through the server, the gateway and the shared network. In the experiment, the statistical method is used to detect. The statistical method is based on the statistical data to create the user profile. When the difference between the new statistical data and the reference profile exceeds a certain threshold, it is considered that a suspicious event has occurred [7]. This type of algorithm uses an anomaly detection model based on statistical analysis, and uses group behaviour to build behaviour patterns to match individual behaviour. Individuals who are excessively beyond the group are considered abnormal.

4.2. Host-based detection

Host-based detection, that is, in-depth detection inside the system, in order to obtain more accurate data related to intrusion behaviour, the detection accuracy is high, but it will have a certain impact on system performance. Because there are various parameters/objects available for testing inside the host, a variety of host-based testing can be designed to achieve system status monitoring testing in experiments. The system state monitoring detection method finds intrusion events by obtaining the usage of various resources of the system and analysing the change curve over time. If in a period of time, the frequency of use of system resources is very high, it is considered that the system is under some kind of attack.
The objects that can be monitored include CPU consumption, disk occupancy, number of open files, etc. The test results are shown in Table 1, Table 2 and Table 3.

Table 1. Experimental results after using the unimproved neural network

| Type of invasion | Right alarm rate | Wrong alarm rate | False negative rate | False alarm rate |
|------------------|------------------|------------------|---------------------|-----------------|
| CodeRed          | 960              | 20               | 4%                  | 0.33            |
| DOS              | 970              | 20               | 3%                  | 0.33            |
| Nimda            | 960              | 10               | 4%                  | 0.17            |
| Trojan attack    | 100              | 100              | -                   | -               |

Table 2. Experimental results after using the improved neural network

| Type of invasion | Right alarm rate | Wrong alarm rate | False negative rate | False alarm rate |
|------------------|------------------|------------------|---------------------|-----------------|
| CodeRed          | 990              | 10               | 1%                  | 0.17            |
| DOS              | 990              | 10               | 1%                  | 0.17            |
| Nimda            | 970              | 30               | 3%                  | 0.54            |
| Trojan attack    | 110              | 120              | -                   | -               |

Table 3. Experimental results without neural network

| Type of invasion | Right alarm rate | Wrong alarm rate | False negative rate | False alarm rate |
|------------------|------------------|------------------|---------------------|-----------------|
| Code Red         | 950              | 40               | 5%                  | 0.67            |
| DOS              | 940              | 50               | 6%                  | 0.83            |
| Nimda            | 950              | 30               | 5%                  | 0.67            |
| Trojan attack    | 0                | 0                | -                   | -               |

It can be seen from the data in the table that the system can detect all attack modes when the network load is light, but when the load reaches a high load or even 100%, it cannot detect attack modes. This is because when the network is working at full capacity, the data packets generated by the attack are too small compared with the network traffic, so that they are completely annihilated, and the intrusion detection system has no time to process these data packets. The reason why the CPU consumption can be detected is because the CPU consumption itself has nothing to do with the network.

5. Conclusion
The high degree of openness of the wireless sensor network makes the attacker always take the risk of entering multiple times. Even if the security technology guarantees that the network will not be breached in a short time, the attacker can obtain the network itself and its protection in several attempts. Various information of the system, and disguise itself based on this information and re-attack. If the detection system's understanding of the attack stays at a narrow level, the network will be breached sooner or later. Therefore, it is imperative to improve the identification and generalization of intrusion features in the detection system. This requires the introduction of an intelligent intrusion detection system. To realize intelligence, the most direct and effective way is to add the methods used for the identification and generalization of intrusion features, such as neural network, genetic algorithm, fuzzy technology, immune principle, etc., to the intrusion detection agent function. The paradigm of intelligent application is the expert system. For behaviours that cannot be determined by general feature detection or anomaly detection as an intrusion, expert systems can often draw credible judgments based on the update and search of its knowledge base. Therefore, the more intelligent Agent intrusion detection system should be integrated into the concept of expert system, so that it has the function of continuous self-learning and self-adaptation.
Acknowledgments
This work was financially supported by Comparative study and practice of online and offline Hybrid Teaching Mode -- Taking the course of computer culture foundation in Higher Vocational Colleges as an example (Project No.: 2020-afcec-328) fund
This work was financially supported by Natural Science Foundation of Tianjin(17JCQNJC04700) fund.

References
[1] Peddabachigari, S., Abraham, A., Grosan, C., & Thomas, J. Modeling intrusion detection system using hybrid intelligent systems. Journal of network and computer applications, 30(1) (2007) 114-132.
[2] Mukkamala, S., Sung, A. H., & Abraham, A. Intrusion detection using an ensemble of intelligent paradigms. Journal of network and computer applications, 28(2) (2005) 167-182.
[3] Elshoush, H. T., & Osman, I. M. Alert correlation in collaborative intelligent intrusion detection systems—A survey. Applied Soft Computing, 11(7) (2011) 4349-4365.
[4] Shenfield, A., Day, D., & Ayesh, A. Intelligent intrusion detection systems using artificial neural networks. ICT Express, 4(2) (2018) 95-99.
[5] Lin, S. W., Ying, K. C., Lee, C. Y., & Lee, Z. J. An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection. Applied Soft Computing, 12(10) (2012) 3285-3290.
[6] Saeed, A., Ahmadinia, A., Javed, A., & Larijani, H. Intelligent intrusion detection in low-power IoTs. ACM Transactions on Internet Technology (TOIT), 16(4) (2016) 1-25.
[7] Depren, O., Topallar, M., Anarim, E., & Ciliz, M. K. An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. Expert systems with Applications, 29(4) (2005) 713-722.