Research and Design of Subway BAS Intrusion Detection Expert System

Jianguo Yu[1], Pei Tian[1], Haonan Feng[2],Yan Xiao[3]

1.Information Engineering College,Communication University of China,Beijing,China

2.Signal and Communication Research Institute,China Academy of Railway Sciences,Beijing,China

3.Equipment Design InstituteBeijing, MTR Design Institute Corporation,Beijing,China

yjg_myzx@126.com,tianpei@263.net,fhn02212005@163.com,yanxiaooo@qq.com

***Abstract*—The information security of urban rail transit system faces great challenges. As a subsystem of the subway, BAS is short for Building Automation System, which is used to monitor and manage subway equipment and environment, also facing the same problem. Based on the characteristics of BAS, this paper designed a targeted intrusion detection expert system. This paper focuses on the design of knowledge base and the inference engine of intrusion detection system based on expert system. This study laid the foundation for the research on information security of the entire rail transit system.**

Keywords—intrusion detection; expert system; knowledge base; the inference engine

I. INTRODUCTION

As an important national infrastructure, urban rail transit is related to national security and national economy and the people's livelihood, which is an important support for many fields and industries. At present, the information security protection of urban rail transit is relatively backward, facing the following security problems: the structure is complex and some subsystems are connected to the Internet; Weak gateway protection between subnets; wireless communication is vulnerable with open frequency bands and protocols. In recent years, domestic and foreign urban rail traffic accidents have occurred many times, causing great adverse effects. For example, in March 2012, the wireless network of the station information release system and the operational scheduling system were attacked in Shanghai Shentong subway.

In the face of increasingly complex Internet, network intrusion methods are constantly refurbished, and single detection technology cannot detect network intrusion in an all-round way[1]. Based on expert system, intrusion detection system has been applied more and more in many industries, but the intrusion detection system in rail transit industry is not yet mature. This paper conducts an exploratory study on the intrusion detection of rail transit system. According to the BAS subsystem of rail transit system, a rule-based intrusion expert detection system is designed, which can use the expert system to detect the intrusion and the misoperation of equipment.

II. INTRUSION DETECTION SYSTEM BASED ON EXPERT SYSTEM

A. Rule-based expert system

The expert system can be considered as a descriptive programming language because programmers do not have to specify how to accomplish the specific algorithm[2]. Now, there are various types of expert systems, such as framework-based expert systems, reasoning-based expert systems, and the rule-based expert systems, and so on. In this paper, rule-based expert system is used to design the intrusion detection system. The knowledge of Experts in the field is used to establish the expert system knowledge base, and the pattern matching method is used to effectively detect intrusions. Any rules for device operation and intrusion, as long as their rule header matches the fact, can be activated and added to the process, and the order of the rules does not affect their activation. The knowledge in the knowledge base comes from the knowledge acquisition module. All knowledge must be manually entered by experts.

B. Structure of Intrusion Detection Based on Expert System

Based on expert system, intrusion detection system can

make full use of the knowledge of security experts, through matching the acquired data with expert knowledge and effective reasoning, we can determine whether there is any intrusion[3].According to the principle of intrusion detection system and the principle of expert system, this paper designs an intrusion detection system based on expert system. The intrusion expert detection system includes man-machine interface, Rule base, inference engine and interpreter, comprehensive database, and data packet collection and filtering module. In a few parts, the structure is shown in Fig.1.

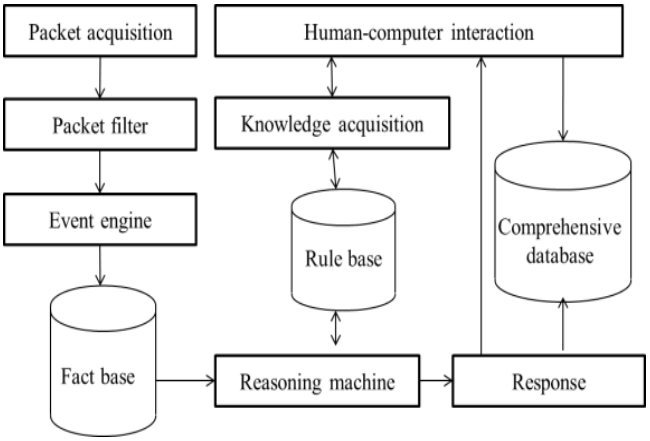

Fig.1. Intrusion Detection System Based on Expert System

C. *Intrusion Detection Expert System Workflow*

The main components of the intrusion detection expert system include at least four important parts: data source, event engine, intrusion reasoning, knowledge base, and intrusion response. Through these four necessary parts, the intrusion detection system works normally. The workflow of the intrusion detection expert system is as follows:

a) System initialization, and then wait for the arrival of the data packet;

b) After data analysis and processing, the features of collected data packets are extracted and transformed by packet filtering module, and the data is filtered through rules, then the remaining data is submitted to the event engine;

c) The event engine analyzes the filtered data packet, generates the facts from the feature data, and adds the facts to the fact base;

d) The inference engine reads the appropriate rules from the rule base, and then analyzes the new fact;

e) If there are highly suspected intrusion data or extracted feature data matches the rules in the knowledge base, relevant information is written into the comprehensive database and the administrator is alerted via the interpreter. Otherwise, wait for the next factual analysis.

The workflow of intrusion detection expert system is shown in Fig.2 below.

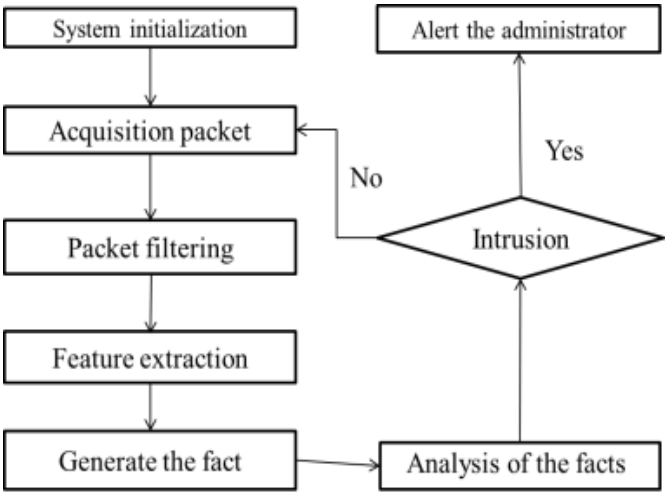

Fig.2. Intrusion detection expert system workflow

D. *Design of knowledge base*

In the intrusion detection expert system of this paper, it represents a knowledge as a rule. In this way, the knowledge base is the rule base, which is used to store knowledge about the characteristics of intrusion. Intrusion detection by expert system, is often targeted at characteristic intrusions. So extraction and expression of intrusion feature is the key to intrusion detection expert systems. In the system, the rule base adopts the production rule representation, transforms the knowledge about intrusion into if-then structure, which the condition part is the intrusion feature and the conclusion part is the measure to be taken after the invasion is found[4]. The system obtains the data by collecting the communication packet between the host computer and the PLC and the system log record of the host. The rules are triggered when the collected data shows suspicious activity. When the suspicious degree exceeds a certain threshold, it is judged that an intrusion occurred.

According to the structure of BAS, in this paper, the equipment misoperation is regarded as an intrusion behavior, and the rule base is divided into three sub libraries, namely equipment wrong operation rule base, intrusion detection rule base and rule base, black and white list respectively for testing equipment misoperation, misuse intrusion and anomaly intrusion. Rules in the rules library should follow the following three principles: there is no conflict between fault rules; The rules are as independent as possible; the definition of rules should avoid redundancy and simplify as much as possible.

1) Equipment misoperation rules base

The operation and maintenance of BAS contains complex knowledge, such as expert experience, maintenance manuals, and so on. These existing knowledge are difficult to describe using precise theoretical models. Equipment misoperation rules base contains all rules for misoperation of devices. The rules are mainly entered through the system's human-machine interface. The rules mainly come from expert experience and BAS time running rules and pattern running rules. Rules are stored in the rules table, includes rule numbers, rule conditions, rule conclusion facts, device status and so on. When the host issues an instruction, when the rule condition in the run rule does not match the instruction, a misoperation is detected.

2) Intrusion detection rule base

The intrusion detection rule base is the focus of this study. It is used to detect known intrusions. The intrusion detection rule base mainly stores the following data: known intrusion behavior characteristics, and set the analysis strategy for the data packets collected in the fact base. For example, in the rules, the protocol, IP address, port number are analyzed in different situations, and the rules are set and the execution order of association rules is set. Each intrusion detection rule is divided into two parts: rule headers and rule options. The intrusion detection rules in this paper are constructed in the form of binary tree. The network address and port information are taken as the rule header, which is the main chain of the rule tree. The characteristics of attack behavior constitute the slave chain of the rule tree. The intrusion rule matching algorithm uses pattern matching algorithm to match the collected factual features with the rule tree. If it is found that the rule matches a data message, it means that an intrusion behavior is detected [5].

3) Black and white list rule base

There is not too much information transmitted by the entire BAS. After the black and white list rules are added, the fast communication between the host computer and the PLC can be better achieved, and the possibility of invasion is strongly reduced. In this paper, black and white list rules are added to the intrusion expert system in order not to affect the rapid response capability in subway operation accidents. Through the creation of its own internal white list database by experts in related fields, Whitelisting technology allows the system to approve which processes are allowed to run on the system by identifying the processes or files in the system that have approved properties, common process names, and digital signatures. After the white list is enabled, users who are not listed in the white list cannot pass. The security and speed are greatly improved.

E. The design of the inference engine

Inference engine is the component that realizes knowledge reasoning in expert system, mainly including reasoning and control. The choice of inference strategies and control strategies in the inference engine is particularly important. When a fact is added to the fact base, the inference engine reads the rule set from the rule base, uses these rules to analyze this fact, and then continuously infers whether there is an intrusion conclusion. And if so, adds this fact to the comprehensive database and report to the administrator through the interpreter and displayed on the system's visual interface to guide the operation and maintenance of the relevant staff.

1) Choice of reasoning strategy

The reasoning strategy mainly solves the knowledge selection and application sequence in the whole problem solving process, that is say, what to do first and make different choices according to the current state. Reasoning strategies are generally divided into forward inference, mixed inference and reverse inference. According to the characteristics of each of the three reasoning methods and the requirements of BAS

operation and maintenance, the reasoning strategy of the BAS, forward reasoning is suitable. According to the fact, the inference engine infers the conclusion of the response, such as maintenance suggestions, intrusion handling measures, and so on.

2)Choice of control strategy

For the Equipment misoperation rules base and the black and white list rule base, each rule is independent, no separate control strategy is needed, and only the inference engine needs to perform one-by-one matching from the rule base. For the intrusion detection rule base, there are multiple rules that are related to each other. In order to make reasonable choice of a piece of knowledge to be used in a variety of available rules, this paper uses a depth-first search strategy. Depth-first search, which starts from the root node of the tree, traverses the nodes of the binary tree along the tree's depth, and searches the branches of the tree as deep as possible. In order to avoid the appearance of known conditions or occurred facts can match multiple rules, the system sets the priority for each rule in the knowledge acquisition phase, the inference engine push the highest priority rule each time for the worker, which can choose the most appropriate knowledge to complete the operation.

F. Design of other modules

This article focuses on the design of the knowledge base and inference engine of intrusion detection expert system. Other modules are no longer focused on this topic, but are simply introduced.

The data packet acquisition module mainly collects the communication information between the host computer and the PLC, the data packets filtered by the black and white list and the host log information.

The main function of the data packet filtering module is to analyze the original data temporarily stored in the original data buffer to obtain the characteristic information, filter the normal business information directly and send the information with security risks to the event engine, the event engine first checks the validity of the data packet, generates the corresponding fact, and stores it in the fact base.

The fact base is responsible for storing and managing the facts generated by the event engine.

The intrusion detection interpreter and response function module is a working platform directly facing the system management user, and the system responds according to the discriminant results and can provide detailed explanation information. If the interpreter receives the intrusion information from the inference engine, it describes the data according to the rules, and outputs the detection result to the intrusion detection system response module, and alerts the administrator through the response module and puts each set of data and The corresponding response results are stored in the comprehensive database and saved as historical data [2].

III. CONCLUSION

At present, intrusion detection in the field of rail transit has become the focus of research in the field of information security. Based on the expert system, this paper designs the BAS intrusion detection expert system for the intrusion detection and misoperation of the subway environment control subsystem, and introduces the knowledge base and inference engine design in the expert system in detail. The system uses expert systems for misoperation and misuse of intrusion detection, and adds black and white list rules to prevent anomalous intrusion, which may protect the information security of the subway environmental control system as much as possible, and at the same time lays a foundation for the information security of multiple subsystems of the subway. At present, this system is only an exploratory stage that has not yet been perfected, but it is believed that with the advent of the era of big data, intrusion detection expert systems will be applied to the entire metro area.

ACKNOWLEDGMENT

This work is supported by The Research on building energy efficiency and slurry sampling of housing and urban-rural development projects," Research and Development of Urban rail transit information security early warning defense system Based on cloud computing".(NO.2016-K4-050)

REFERENCES

[1] Zhang Ren-shang. Network Intrusion Detection System Based on Expert System and Neural Network[J]. Computer Simulation, 2012, 29(9):162-165.

[2] Zhao Wei,The study and implement of the high-speed EMU's operation and maintenance decision knowledgebase[D], Beijing Jiaotong University,2016

[3] Ma Ya-yan,Design and implementation of ananti-phishing detection system based on expert knowledge database[D], Beijing University of Posts and Telecommunications,2014

[4] Zou Xiao-hua. Research on Intrusion Detection model Based on Artificial Immune Theory[J]. *Computer Knowledge & Technology*, 2008.

[5] Zhang Hai-chun, Li Yuan, Zhang Zi-li. Design and Simulation of the System for Intelligent Intrusion Detection[J]. *Mathematics in Practice & Theory*, 2009, 39(6):162-16