Research and Design of Security Gateway for Industrial Control System

Yanru Chen[1, a], Qinghai Xiao[2, b] and Hua Gao[2, c]

[1] The PLA Information Engineering University, Zhengzhou 450000, China;

[2] Henan Technology University, Zhengzhou 450000, China.

[a]18239920575@163.com, [b]xiaotsinghai@163.com, [c]877054239@qq.com.

Keywords: Industrial control systems, security gateway, Load balancing, Data filtering.

Abstract. With the extensive application of information technology, Industry informatization has been developed rapidly, but the network security issues where come from business networks, the Internet or caused by other factors is increasingly appear in industrial control systems. This paper is designed a security gateway for industrial control systems ,which is mainly used for filtering data of application layer, located at the boundary of industrial control systems and office area , we can solve the security problem to a large extent. Finally, the security gateway verified by experiments, comparative analysis of results can prove the security gateway is meeting the needs of industrial control systems.

1. Introduction

Industrial control systems(ICS) is constituted by a variety of automation and control components and process control components for real-time data acquisition, monitor. With the rapidly developed of industry informatization, information, networks, and Internet of things technology is gradually applied to petrochemicals, energy, electricity, intelligent transportation, industrial production and other fields, which greatly improve the economic and social benefits.

In the case of the physical environment is isolated completely, traditional industrial control systems do not need to consider security issues, however, with the information technology, Ethernet and TCP / IP, fieldbus technology, OPC (OLE for Process Control) technology are widely used, industrial equipment interfaces is increasingly opening, the security issues are increasingly appeared in industrial control systems such as viruses, Trojans, hackers, which influence the safety of industrial production and even national security directly.

This paper use the oilfield industry control system as the study background, design a secure gateway, which located at the boundary of industrial control systems and office area, check format, protocol, content of industrial data, prevent malicious attacks add destructive data in the legal communication data structures and formats, resulting in a variety of machine malfunction, or even directly transmit virus Data infecting industrial control system through the protocol port.

Section1 of this article is the introduction, describe the background; Section2 introduce the related technologies; Section3 describe the system architecture and algorithm; Section4 compare experimental analysis; section 6 is conclusion.

2. Related Technology

The Protocol filtering which based on deep packet through extract the application layer data, analysis protocol eigenvalues to establishing the protocol eigenvalues library, distinguish corresponding data stream through eigenvalues matching of the captured data and protocol eigenvalues library, in order to achieve protocol filtering. Due to flexible, logical and functional, regular expression become a top research of protocol identification. The famous open source project — Linux application layer protocol classification -L7-filter use regular expressions to identify more than 100 kinds of application layer protocols [1], in addition, Snort intrusion detection system [2], Bro intrusion detection system [3] are using regular expressions to describe the rule set. Paper [4] use

regular expressions protocol recognition technology based on NFA engine, although efficient, but the engine need to re-match from the first byte every time, wasting a lot of time.

String matching compared the main string $M = M_1M_2M_3.....M_i$ (where $j \ll i$) to pattern string $S = S_1S_2S_3.....S_j$ which is set according to the content eigenvalues, if the same string is found, the matching success. Pattern matching algorithm such as efficient single pattern matching algorithm -KMP, BM and multi-pattern matching algorithm -AC. Chen Ying and other bring mathematical statistical methods to pattern matching algorithm [5], collect successful sampling points from a text string through use of statistical sampling theory. Yao Yafeng put forward AC-BM algorithm [6], which combined the advantages of the AC algorithm and BM algorithm, improving efficiency significantly. Liu Shengfei, Zhang Yunquan proposed BMH2 algorithm[7] on the basis of BMH algorithm, the algorithm adds a moving distance of an array of eigenvalues to assist pattern string of the most significant shift.

3. System Structure

Industrial control systems include data acquisition and control, Zigbee transceiver, RTU terminals; office network include regional operation monitoring system, control terminal, display industrial data, as shown in Fig.1 Data exchange between the two parts including the office network send control information to the industrial control systems, industrial control systems send feedback information to the office network in accordance with the requirements of the control information, and timing of return monitoring information. Security gateway in the middle of the Industrial control systems and the office network, responsible for these application-layer data filtering, to ensure the data security and integrity, wherefore industrial control system will not be destroyed illegal intruders, data filtering is constituted by protocol filtering, content filtering.

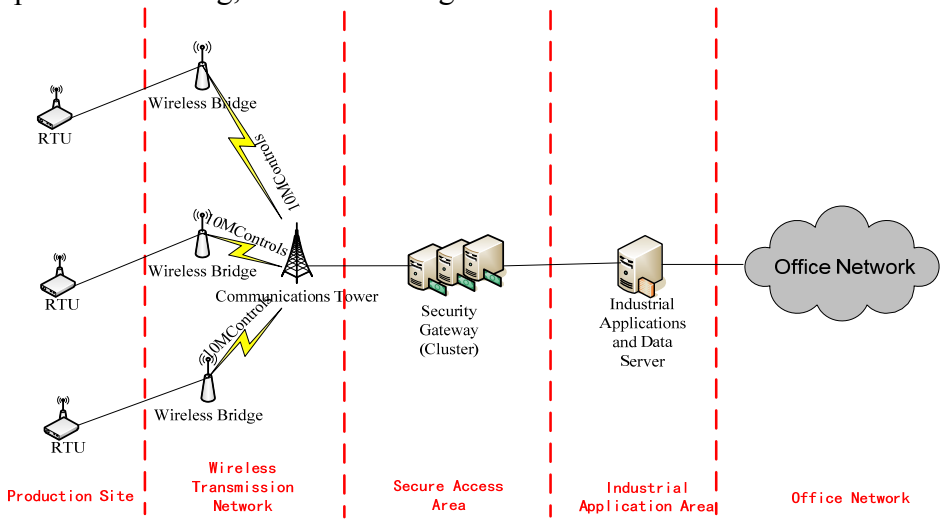

Fig.1 system structure

3.1 System Filtering Model.

In actual operation, the amount of data transmission in industrial control systems is large, and require real-time, if use a common system filtering model will cause excessive load of security gateway and data filtering rate is too slow, inefficient, which do not meet the needs of industrial control systems. The paper propose a suitable filtration system industrial network mode to solve these problems, which use load-balancing technology, security gateway arranged in the form of load balancing, as shown below figure 2 (security gateway by APG) .

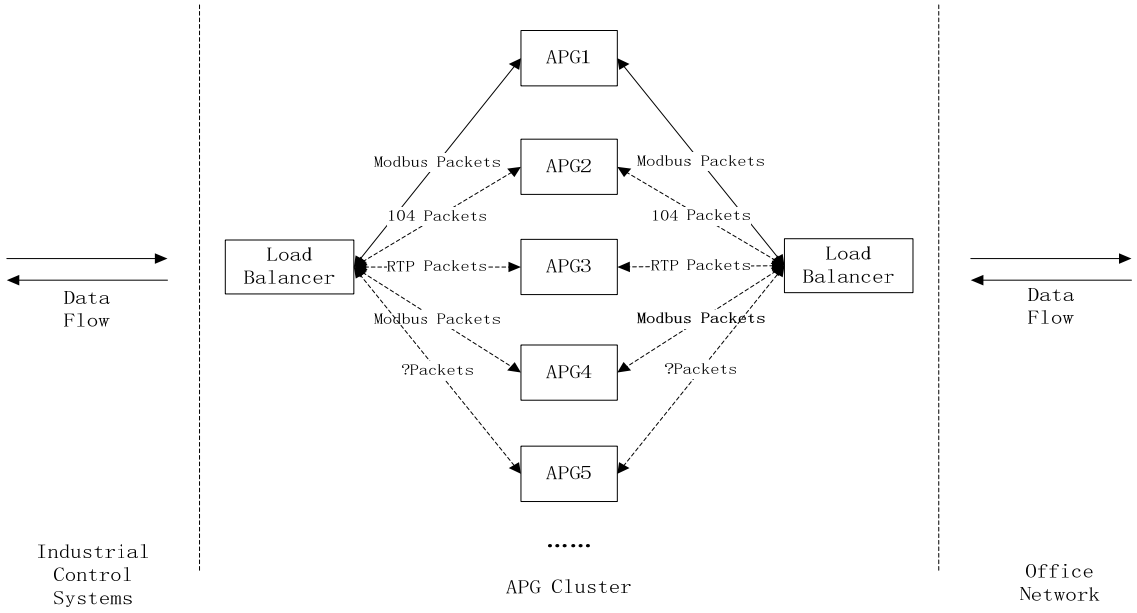

Fig.2 System filtering model

Load balancer is set protocol filtering model, different application proxy gateway to filter different protocol packets, such as APG1 and APG4 filter Modbus protocol, APG2 filter 104 protocol. When the data stream reaches the load balancer, through protocol filtering firstly, and the protocol which is matching whitelisting can sent to the corresponding security gateway, carry on content filtering secondly; discard mismatched data packets directly. Since the filtering tasks are assigned to the multiple security gateways through a reasonable load balancing, it increases the efficiency of data filtering greatly, to achieve the efficient operation of the industrial control system.

3.2 Algorithms.

Common regular expressions based on DFA is used to protocol filtering, improved string matching algorithm is used to content filtering. This paper improves the string matching algorithm, the first character, inclusive character spacing and last character as the eigenvalues, use compromise matching algorithm to shorten the length of pattern which can judge match is success or failure rapidly. Algorithm implementation process is as follows:

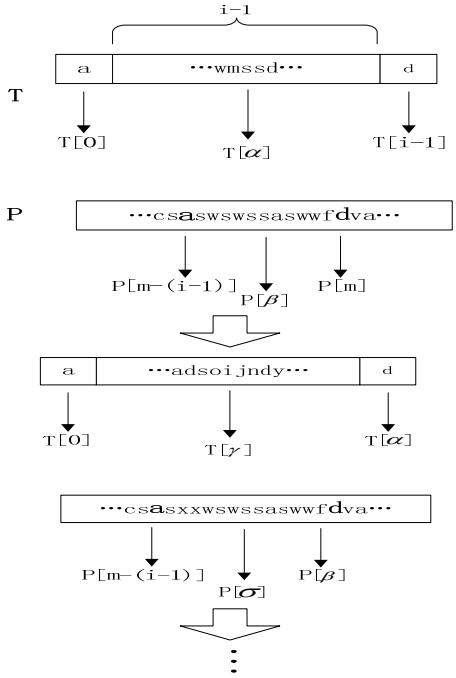

Fig.3 String matching workflow

As shown in figure 3, select the first character, inclusive character spacing and last character of the pattern string T as the eigenvalues firstly, denoted $(T[0], i-1, T[i])$. Find the first character $T[0]$ in the text string pattern string P, if not found, the match fails; if found, the location of the character set $P[m]$, then compares whether the value of $P[m+(i-1)]$ and $T[i]$ is equal, if not, then find according to the head and tail characters of the mode string, until the first character and last character are equal respectively; if equal, then the pattern string P T offset to a text string of characters at the end of the eigenvalues of alignment, using compromise matching method to define an intermediate point:

$$P[\alpha] = P[m + \frac{i}{2}] \qquad (m \geq i \geq 0) \tag{1}$$

And the intermediate point of the pattern string T:

$$T[\beta] = T[\frac{i}{2}] \qquad (i \geq 0) \tag{2}$$

If the result is not an integer, drop the decimal point and integer plus 1. If $P[\alpha]\ T[\beta]$ not equal, the match fails, packet filtering is not passed, discarded directly; if equal, $P[\alpha]\ T[\beta]$ will as tail byte of the text string and the pattern string respectively, continue forward (backward) to take an intermediate point, compare two intermediate points is whether same; and so on, until all the characters are the same, in the case of $P[m]$ is the last character $P[m]$ in a text string, the match is successful; if not, continue to repeat the above steps.

4. Experiment Analysis

Test environment configuration: Three servers as an application proxy gateway, two as a load balancer, a simulation as the sender sends a request, one as the receiving end, all the servers are installed Cent OS 6.X system. The network topology is shown in figure 4.

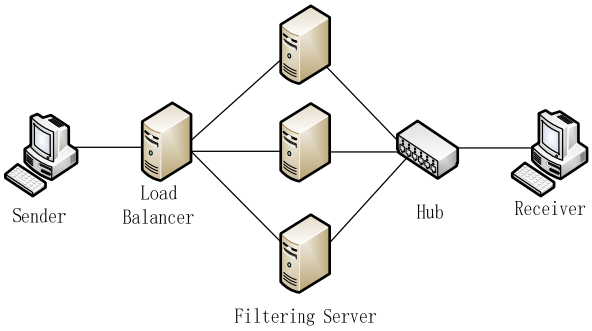

Fig.4 Experimental topology

To ensure accurate and effective of experimental data, use the Visual C++6.0 language programming, experiments were divided into three cases, the first two cases: BMHS matching algorithm and compromise matching algorithms were coded to achieve in the topology map on all three filtering server, load balancer random load balancing algorithm; third case: APG filtering model deployed as designed. Experiments were sent contained modbus protocol, 104 agreements and rtp protocol packet, in the same amount of data sent and malicious code number of cases, through statistical malicious packet detection rate and packet arrives at the receiving end of all the turnaround time, analysis and comparison of three cases, as shown below:

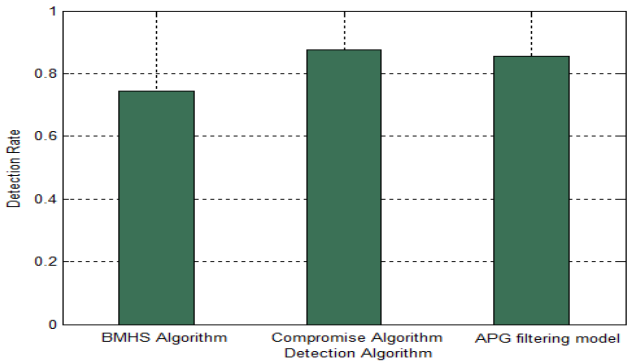

Fig.5 Detection rate comparison chart

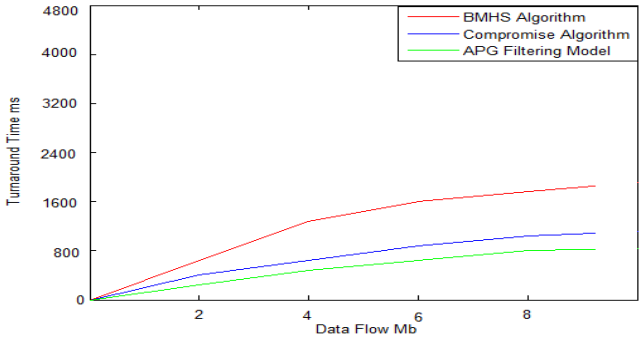

Fig.6 Turnaround time Comparison Chart

Experimental data analysis and comparison of figure 5 shows that malicious code is detected in the same amount of data, the compromise matching algorithms and filtering model APG detection rate difference is small, but in contrast to BMHS algorithm, it still has an obvious advantage. Figure 6 shows data filtering turnaround time in the three cases, the turnaround time of BMHS matching algorithm and compromise matching algorithm all showed slow growth, but the compromise matching algorithm filtering rate was significantly better than BMHS matching algorithm. And after using APG filtering model, data filtering required turnaround time was significantly lower than the time required which only use compromise algorithm at the outset, After slow growth tends to more balanced state. By contrast experiment shows, APG filtering model efficient and stable, meet the actual operating environment and high performance real-time data transmission of industrial control systems required.

5. Conclusion

Aiming at specific applications of industrial control systems, this paper design a filtering model combining with load balancing to carry on data protocol filtering and content filtering, implement a large-scale data filtering efficiently, experiments show that the filtering system can complete the data filtering efficiently when compared with the common filtering systems.

References

[1]. Levandoski J, Sommer E, Strait M. Application Layer Packet Classifier for Linux. http://l7-filter.sourceforge.net/

[2]. “SNORT Network Intrusion Detection System.” http://www.snort.org

[3]. “Bro Intrusion Detection System.” http://bro-ids.org/Overview.html

[4]. Chen Xianqing.Design and Implementation for Application Layer Protocol Filtering System [D]. Electronic Science and Technology University, 2010.

[5]. Chen Ying. Improved String Search Algorithm [J]. Electromechanical Product Development & Innovation，2007(3):140-141.

[6]. Yao Yafeng, Fang Xianjin, Sai Wenli. Research of the New Content Filtering Firewall [J]. Computer Technology and Development,2010(11):3-4.

[7]. Liu Shengfei, Zhang Yunquan. An Improved BM Pattern Matching Algorithm [J]. Computer Science, 2008,35(11):164-173.