Design and Implementation of Industrial Firewall for Modbus/TCP

Wenli Shang[1*], Quansheng Qiao[2], Ming Wan[1], Peng Zeng[1]

[1] Shenyang Institute of Automation Chinese Academy of Science, Shenyang and 110016, China.
[2] Shenyang Jianzhu University, Shenyang and 110168, China.

* Corresponding author. Email: shangwl@sia.cn

Manuscript submitted May 7, 2015; accepted November 23, 2015.
doi: 10.17706/jcp.11.5.432-438

Abstract. For the fragile security status and the growing threat of attack on industrial control systems, it is particularly important to strengthen the technology of security protection. After a detailed study of the characteristics of industrial control systems, this paper put forward design scheme of industrial firewall based on Modbus/TCP protocol, combining "white list" security policies with deep packet inspection technology, and realizing on the Linux platform. The experimental results show that the firewall can effectively intercept illegal data stream and ensure the normal operation of the industrial control system.

Key words: Industrial control systems, cyber security, industrial firewall, Modbus/TCP protocol.

1. Introduction

With the integration of industrialization and information technology, industrial control systems increasingly adopt a common standard communication protocols as well as hardware and software systems, which broke the previous closed nature on the physical environment and special of the software and hardware. Industrial control systems have to face the traditional information security threats [1], [2]. The security protection technology of industrial

The security protection technology of industrial control systems become more and more important [3], Especially in 2010 the ”Stuxnet” attacking Iran Bushehr nuclear power plant.

Firewall, asnetwork security guards, controls the communication between networks to prevent unauthorized users to access the internal important information resources. Scholars have been carried out for firewall design at different levels of theory. The literature [4] proposed a new firewall architecture design method mainly for the IT network application protocol but lack analysis and design of industrial network application protocol. The literature [5] proposed a rule-based firewall design only matches to the network layer, but lack of application layer data flow analysis which is prone to error interception. The literature [6] builds a firewall can effectively resolve application layer packet of information, but it is difficult to meet the industrial control systems for real-time requirements because of the delay.

Currently, firewall technology research mainly focused on information networks, less in industrial networks. Different from traditional IT system focusing on the protection of data confidentiality, industrial control system focuses on availability and real-time. Therefore, this paper combines "white list" strategy with the deep packet inspection technology and implements in the Linux platform. It proves the feasibility of this method and offers the theory and technical guidance for the safety and protection of the industrial control system.

2. Industrial Control System Architecture

Industrial control system is the product of combination between industrial control components and computer network. It also based on network which is widely used in automation systems manufacturing operations and national critical infrastructure [7]. Typical industrial control system components include controllers, HMI, DCS (distributed process control system) and SCADA (Supervisory Control and Data Acquisition). Industrial control systems in the actual deployment can be divided into the enterprise network, process control and monitoring network and control system network. The typical topology is shown in Fig. 1:

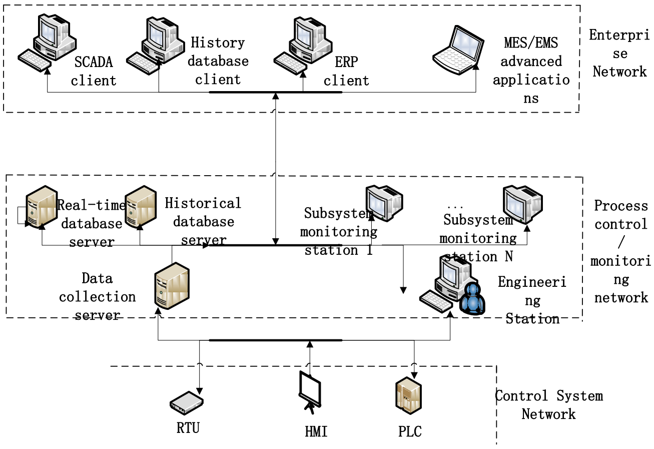

SCADA client
History database client
ERP client
MES/EMS advanced applications
Enterprise Network
Real-time database server
Historical database server
Subsystem monitoring station 1
...
Subsystem monitoring station N
Process control / monitoring network
Data collection server
Engineering Station
RTU
HMI
PLC
Control System Network

Fig. 1. Typical topological structure of industrial control system.

After deployment of industrial control systems, the host and control device are less likely to be added or removed from network. Therefore, industrial control network is static and stable and its traffic generated mostly by automated production processes is a certain period and regularity for "white list" strategy [8], [9]. Also, hierarchical network structure is suitable for sub-regional management.

Industrial control systems cyber threats are mainly from the following aspects:

1) Industrial control networks use the TCP/IP protocol to have to face traditional IT systems similar network attacks, such as, Idle Scan attack, ARP spoofing / poisoning attacks, SYN Flooding attacks [10].
2) The control protocol attacks are often application layer data because it lack of authentication [11].

3. Modbus/TCP Protocol Field Analysis

Modbus protocol as an industrial fieldbus protocol standard is widely used in industrial control systems. As an application layer transmission protocol, it provide client/server communication model and specific function code operational services with a master/slave communication structure. Modbus dialog is established by sending Modbus/TCP application data unit (ADU), which is embedded in the TCP frame data report containing the Modbus application protocol (MBAP) and protocol data unit (PDU). PDU consists of function code and data composition. MBAP header consists of 4main parts: transaction identifier, protocol identifier, length and unit identifiers. Data frame structure is shown in Fig. 2:

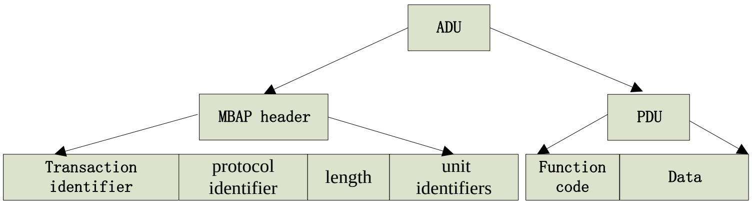


Fig. 2. Modbus/TCP data frame format.

As long as the attacker use a valid Modbus address and legal function code can build a Modbus dialogue, but no role-based access control mechanism is prone to unauthorized operation and the address and command without encrypted are easy to break. To solve these problems, industrial firewall designed in this article deep analysis of Modbus / TCP protocol, which make full use of the PDU field values to set the rules to strengthen the security and reliability of the firewall.

4. Industrial Firewall System

Based on the Linux platform, industrial firewall is developed by using iptables tools in this paper [12]. The firewall administrators add, delete, modify rules and replace operations with this tool, which can combine rules into a single list to achieve the access control function. The realization process is shown in Table 1:

Table 1. Industrial Firewall Implementation Process

Algorithm 1: Industrial firewall implementation steps
Step 1: Build ICS "defense in depth" system and the regional enclave and boundary setting Step2: Make clear legal data flow between different regions with the "white list" strategy; Step3: Depth analysis the data stream without "white list" of to determine its legitimacy by deep packet inspection technology

4.1. "Defense in Depth" Architecture Design

Aiming at the security problem of the complex industry control system, industrial control network is divided into different security zones to deploy security measures form overall defensive capabilities with "defense in depth" architecture [13], [14]. According to the topological structure of industrial control system in the first section, the specific form of protection area is shown in Table 2:

Table 2. Industrial Firewall Protection Zone Lists

Region Name	Network layer	Function	security level
internal network	Process control network	Deploy the device and the host	Credible zone
external network	Enterprise network	Protect equipment and hosts of external internet	Non-credible zone
DMZ	Arbitrarily	Protect shared components of enterprise networks and the process control network	Between credible and non-credible zone

Different zones have different security policies. For trusted zone, any external access is prohibited unless expressly permitted; DMZ zone allows intervals devices access each other in credible and non-credible to a certain extent; non-credible zone can't access the trusted zone, but can visit the DMZ. This design can better protect the internal network resources and reduce the likelihood of being attacked. Network structure is shown in Fig. 3:

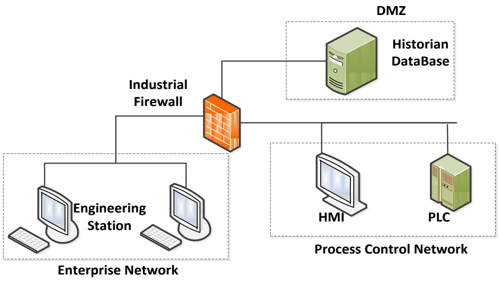


Fig. 3. "Defense in depth" network structure.

4.2. "White List" Security Policy

"White list" is a list of rule libraries for storing legal rule set. "White list" policies are used in industrial firewall can effectively reduce the load on the firewall, since it can handle proprietary application protocols without detecting the data content of the packet. Traditional IT firewall's White list configuration is very difficult because of huge demand and massive connection to access the application services. However, the industrial network has static and stable network architecture, which makes white list policy become easy. Based on the "defense in depth" network structure of Fig. 3, steps of white list strategy are shown in Table 3.

Table 3. Steps White List Policy

```
Algorithm 2: white list policy settings
Step1: the default policy is set to DROP.
Step2: all legal rules to specify IP address TCP ports and services agreement.
Step2.1: determine IP address DH_IP and listening port number DH_PORT of the history database server;
Step2.2: determine the legal IP address set of history database server in the enterprise network;
Step2.3: determine legal IP address P_IPS of history database server in the process control network;
Step2.4: determine legal IP address A_IPS of passing through the firewall in enterprise network;
Step3: Specifies the path of legal rules.
Step3.1: allows P_IPS to DH_IP and DH_PORT port to connect to the TCP;
Step3.2: allows E_IPS to DH_IP and DH_PORT port to connect to the TCP;
Step3.3: allows A_IPS to DH_IP and the port number 502 to connect to the Modbus;
```

4.3. Depth Protocol Analysis

Firstly, capture the real-time data traffic and data preprocessing in network; secondly, determine whether the data is in the white list, if it is, directly through, otherwise depth protocol analysis. Finally, match characteristics of the database fields. Analysis process is shown in Fig. 4.

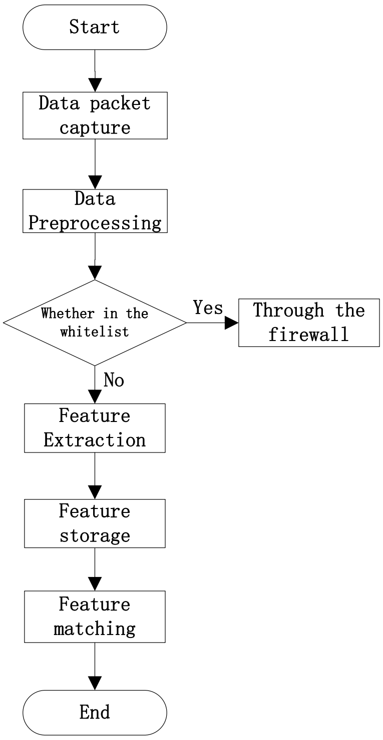


Fig. 4. White list-based deep packet inspection (DPI).

Function code and data values of Modbus / TCP are extracted as protocol feature fields. Construction safety rules modes are as follows: [S_IP][D_IP][Port][F_Code][Data]. Among them, S_IP is said the source address, D_IP representatives destination address, Port is said TCP destination port number, F_Code is a functional code of Modbus / TCP protocol specified and Data field represents the data value associated with the function code. Deep packet inspection firewall can delve into the applications protocol and understand the application intent to stop the illegal attempt in time.

5. System Test

5.1. Experimental Environment

To validate the availability and reliability of the industrial firewall designed in this paper, we built industrial control systems simulation environment based on Modbus/TCP protocol. Simulation of motor control system experimental schematic diagram is shown in Fig. 5:

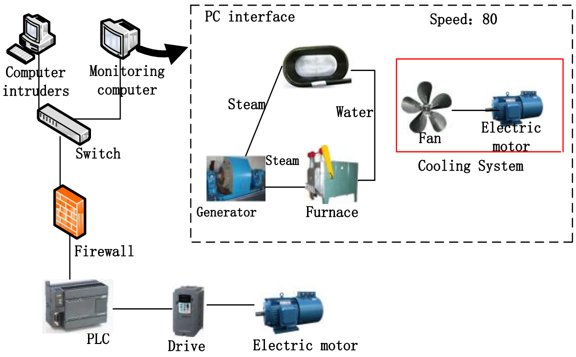
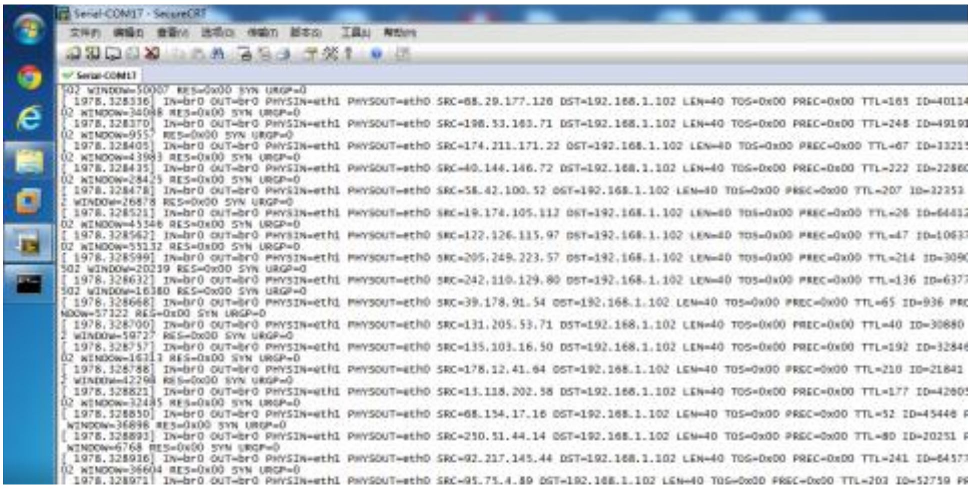


Fig. 5. Schematic diagram of experimental environment.

The experimental environment is divided into three layers, namely, data monitoring acquisition layer, the control unit layers and the execution unit layers. Data monitoring acquisition layers reflect real-time data acquisition and operation status. The control unit layers are composed by Schneider M340 series PLC. The execution unit layers include inverter and motor.

5.2. Experimental Design and Analysis

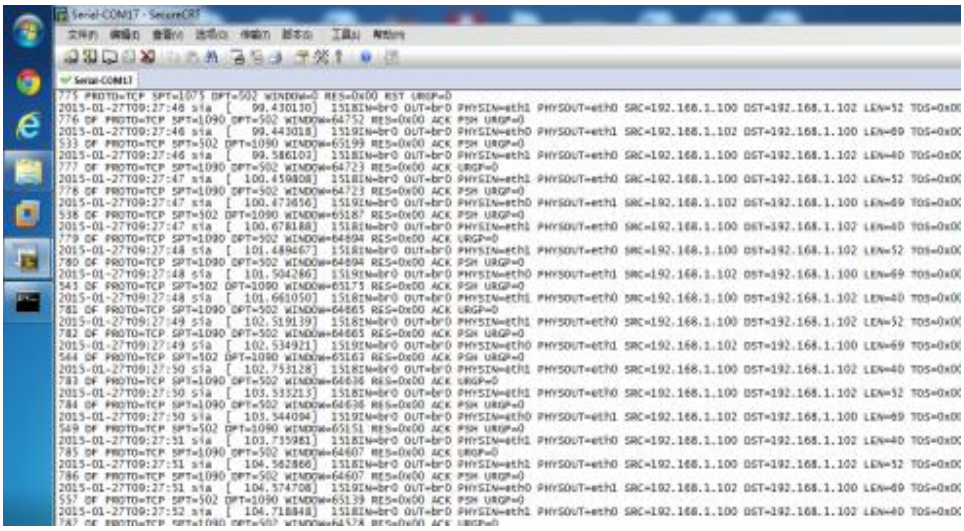
PLC 502 ports provide Modbus/TCP application services, so we use SYN / ACK Flood [16] attack on the 502 port of the PLC. It was found that host machine cannot properly control the motor because attacked PLC cannot respond to control instructions before starting the industrial firewall. However, after the industrial firewall is started, the attack was successful intercept and PLC operates normally.



```
502 WINDOW=50007 RES=0x00 SYN URGP=0
[ 1978.328336] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=68.29.177.126 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=165 ID=40114
02 WINDOW=34088 RES=0x00 SYN URGP=0
[ 1978.328370] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=198.53.163.71 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=248 ID=49191
02 WINDOW=9557 RES=0x00 SYN URGP=0
[ 1978.328405] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=174.211.171.22 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=67 ID=3321
02 WINDOW=43983 RES=0x00 SYN URGP=0
[ 1978.328435] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=40.144.146.72 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=222 ID=2286
02 WINDOW=28425 RES=0x00 SYN URGP=0
[ 1978.328478] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=58.42.100.52 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=207 ID=32353
2 WINDOW=26878 RES=0x00 SYN URGP=0
[ 1978.328521] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=19.174.105.112 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=26 ID=6441
02 WINDOW=45346 RES=0x00 SYN URGP=0
[ 1978.328562] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=122.126.115.97 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=47 ID=1063
02 WINDOW=55132 RES=0x00 SYN URGP=0
[ 1978.328599] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=205.249.223.57 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=214 ID=309
502 WINDOW=20239 RES=0x00 SYN URGP=0
[ 1978.328632] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=242.110.129.80 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=136 ID=6377
502 WINDOW=16380 RES=0x00 SYN URGP=0
[ 1978.328668] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=39.178.91.54 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=65 ID=936 PRE
NDOW=57122 RES=0x00 SYN URGP=0
[ 1978.328700] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=131.205.53.71 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=40 ID=30880
2 WINDOW=59727 RES=0x00 SYN URGP=0
[ 1978.328757] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=135.103.16.50 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=192 ID=3284
02 WINDOW=16313 RES=0x00 SYN URGP=0
[ 1978.328788] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=178.12.41.64 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=210 ID=21841
2 WINDOW=42298 RES=0x00 SYN URGP=0
[ 1978.328821] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=13.118.202.58 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=177 ID=4280
02 WINDOW=32485 RES=0x00 SYN URGP=0
[ 1978.328850] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=68.154.17.16 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=52 ID=45448 P
 WINDOW=36898 RES=0x00 SYN URGP=0
[ 1978.328893] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=250.51.44.14 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=80 ID=20251 P
 WINDOW=6768 RES=0x00 SYN URGP=0
[ 1978.328936] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=92.217.145.44 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=241 ID=6457
02 WINDOW=36604 RES=0x00 SYN URGP=0
[ 1978.328971] IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=95.75.4.89 DST=192.168.1.102 LEN=40 TOS=0x00 PREC=0x00 TTL=203 ID=52759 PR
```

Fig. 6. Before starting industrial firewall.

It is verified whether industrial firewall can successfully intercept illegal packets through the firewall log data analysis. Figs. 6 and 7 respectively show changes in network data flow before and after the starting of the firewall. 192.168.1.100 is set to host machine IP address, 192.168.1.254 is the IP address of the host with the industrial firewall, 192.168.1.102 is the IP address of the PLC and 192.168.1.25 is the IP address of the attacker. It makes attack more covert because of different IP address from attackers, which proved high reliability and security of industrial firewall designed in this article.


Serial-COM17 - SecureCRT
文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(L) 帮助(H)
Serial-COM17

```
775 PROTO=TCP SPT=1075 DPT=502 WINDOW=0 RES=0x00 RST URGP=0
2015-01-27T09:27:46 sia  [   99.430130]  1518IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=192.168.1.100 DST=192.168.1.102 LEN=52 TOS=0x0
776 DF PROTO=TCP SPT=1090 DPT=502 WINDOW=64752 RES=0x00 ACK PSH URGP=0
2015-01-27T09:27:46 sia  [   99.443018]  1519IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=192.168.1.102 DST=192.168.1.100 LEN=69 TOS=0x0
533 DF PROTO=TCP SPT=502 DPT=1090 WINDOW=65199 RES=0x00 ACK PSH URGP=0
2015-01-27T09:27:46 sia  [   99.586103]  1518IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=192.168.1.100 DST=192.168.1.102 LEN=40 TOS=0x0
777 DF PROTO=TCP SPT=1090 DPT=502 WINDOW=64723 RES=0x00 ACK URGP=0
2015-01-27T09:27:47 sia  [  100.459808]  1518IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=192.168.1.100 DST=192.168.1.102 LEN=52 TOS=0x0
778 DF PROTO=TCP SPT=1090 DPT=502 WINDOW=64723 RES=0x00 ACK PSH URGP=0
2015-01-27T09:27:47 sia  [  100.473656]  1519IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=192.168.1.102 DST=192.168.1.100 LEN=69 TOS=0x0
538 DF PROTO=TCP SPT=502 DPT=1090 WINDOW=65187 RES=0x00 ACK PSH URGP=0
2015-01-27T09:27:47 sia  [  100.678188]  1518IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=192.168.1.100 DST=192.168.1.102 LEN=40 TOS=0x0
779 DF PROTO=TCP SPT=1090 DPT=502 WINDOW=64894 RES=0x00 ACK URGP=0
2015-01-27T09:27:48 sia  [  101.489467]  1518IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=192.168.1.100 DST=192.168.1.102 LEN=52 TOS=0x0
780 DF PROTO=TCP SPT=1090 DPT=502 WINDOW=64894 RES=0x00 ACK PSH URGP=0
2015-01-27T09:27:48 sia  [  101.504286]  1519IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=192.168.1.102 DST=192.168.1.100 LEN=69 TOS=0x0
543 DF PROTO=TCP SPT=502 DPT=1090 WINDOW=65175 RES=0x00 ACK PSH URGP=0
2015-01-27T09:27:48 sia  [  101.661050]  1518IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=192.168.1.100 DST=192.168.1.102 LEN=40 TOS=0x0
781 DF PROTO=TCP SPT=1090 DPT=502 WINDOW=64865 RES=0x00 ACK URGP=0
2015-01-27T09:27:49 sia  [  102.519139]  1518IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=192.168.1.100 DST=192.168.1.102 LEN=52 TOS=0x0
782 DF PROTO=TCP SPT=1090 DPT=502 WINDOW=64865 RES=0x00 ACK PSH URGP=0
2015-01-27T09:27:49 sia  [  102.534921]  1519IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=192.168.1.102 DST=192.168.1.100 LEN=69 TOS=0x0
544 DF PROTO=TCP SPT=502 DPT=1090 WINDOW=65163 RES=0x00 ACK PSH URGP=0
2015-01-27T09:27:50 sia  [  102.753128]  1518IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=192.168.1.100 DST=192.168.1.102 LEN=40 TOS=0x0
783 DF PROTO=TCP SPT=1090 DPT=502 WINDOW=64636 RES=0x00 ACK URGP=0
2015-01-27T09:27:50 sia  [  103.533213]  1518IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=192.168.1.100 DST=192.168.1.102 LEN=52 TOS=0x0
784 DF PROTO=TCP SPT=1090 DPT=502 WINDOW=64636 RES=0x00 ACK PSH URGP=0
2015-01-27T09:27:50 sia  [  103.544094]  1519IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=192.168.1.102 DST=192.168.1.100 LEN=69 TOS=0x0
549 DF PROTO=TCP SPT=502 DPT=1090 WINDOW=65151 RES=0x00 ACK PSH URGP=0
2015-01-27T09:27:51 sia  [  103.735981]  1518IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=192.168.1.100 DST=192.168.1.102 LEN=40 TOS=0x0
785 DF PROTO=TCP SPT=1090 DPT=502 WINDOW=64607 RES=0x00 ACK URGP=0
2015-01-27T09:27:51 sia  [  104.562866]  1518IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=192.168.1.100 DST=192.168.1.102 LEN=52 TOS=0x0
786 DF PROTO=TCP SPT=1090 DPT=502 WINDOW=64607 RES=0x00 ACK PSH URGP=0
2015-01-27T09:27:51 sia  [  104.574708]  1519IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=192.168.1.102 DST=192.168.1.100 LEN=69 TOS=0x0
557 DF PROTO=TCP SPT=502 DPT=1090 WINDOW=65139 RES=0x00 ACK PSH URGP=0
2015-01-27T09:27:52 sia  [  104.718848]  1518IN=br0 OUT=br0 PHYSIN=eth1 PHYSOUT=eth0 SRC=192.168.1.100 DST=192.168.1.102 LEN=40 TOS=0x0
787 DF PROTO=TCP SPT=1090 DPT=502 WINDOW=64578 RES=0x00 ACK URGP=0
```

Fig. 7. After starting industrial firewall.

After comparative analysis, malicious traffic from 192.168.1.25 can be successfully intercepted, but it is still safe from 192.168.1.100 after starting the industrial firewall. That also illustrates the industrial firewall can block malicious attackers to access to the PLC and allow normal command successfully to reach PLC to protect the PLC so as to ensure the normal operation of the motor purpose.

6. Conclusion

With the cross-integration of industrial control network and information network, industrial control system is also facing the threat of traditional IT network because of more and more open system. Based on the industrial control network "limited state" and "limited behavior", "white list" policy is applied to industrial firewall and deep packet inspection technology is used to build firewall. Good test results of this method's feasibility on the Linux platform indicated that the industrial firewall can better analyze network traffic and reasonable intercept illegal traffic.

References

[1] Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST Special Publication*, 800-82.

[2] Gao, W., & Morris, T. H. (2014). On cyber attacks and signature based intrusion detection for MODBUS based industrial control systems. *Journal of Digital Forensics, Security and Law*, *9(1)*, 37-56.

[3] Beaumont, P. (Sept. 2010). Stuxnet worm heralds new era of global cyberwar. *The Guardian*.

[4] Applebaum, A., Levitt, K. N., & Rowe, J. (2012). Arguing about firewall policy. *COMMA*, *245*, 91-102.

[5] Salah, K., Elbadawi, K., & Boutaba, R. Performance modeling and analysis of network firewalls. *IEEE Transactions on Network and Service Management,* 12-21.

[6] Batista, A. B., Kobayashi, T. H., & Medeiros, J. P. S. (2010). Application filters for TCP/IP industrial automation protocols. *Critical Information Infrastructures Security*, 111-123.

[7] Brendan, G., & Gerhard, P. (2013). Introduction to industrial control networks. *IEEE Communications Surveys & Tutorials*, 860–880.

[8] Rafael, R., & Ramos, R. B. (2013). Flow whitelisting in SCADA networks. *International Journal of Critical*

Infrastructure *Protection*, 150-158.

[9] Kang, D. H., Kim, B. K., & Na, J. C. (2014). Whitelist generation technique for industrial firewall in SCADA networks. *Frontier and Innovation in Future Computing and Communications*, 525-534.

[10] Eric, K. (2011). Industrial network security securing critical infrastructure networks for smart grid. *SCADA, and Other Industrial Control System*.

[11] Keith, S., Joe, F., & Karen, S. (2007). Guide to industrial control systems(ICS) security. National Institute of Standards and Technology Special Publication.

[12] Jie, P. & Li, L. (2011). Industrial control system security. *Proceedings of 2011 International Conference on Intelligent Human-Machine Systems and Cybernetics* (pp. 156–158).

[13] Peng, Y., Jiang, C. Q., & Xie, F. (2012). Industrial control system information security research. *Natural Science(Tsinghua University), 52(10),* 1396-1408.

[14] Lubna, K., & Cyiac, F. (2013). Firewall log analysis and dynamic rule re-ordering in firewall policy anomaly management framework. *Proceedings of 2013 International Conference on Green Computing, Communication and Conservation of Energy* (pp. 853-856).

[15] Hao, Y. J. (2010). Research and implementation of deep packet inspection firewall host. University of Electronic Science and Technology.

[16] Rana, D. S., Garg, N., & Chamoli, S. K. (2012). A study and detection of TCP SYN flood attacks with IP spoofing and its mitigations. *International Journal of Computer Technology and Applications, 3(4).*

Wenli Shang was born in Beian, Heilongjiang, China, in 1974. He received his master degree of mechanical design and theory from Northeastern University of China, in 2002, and his Ph.D. degree of mechanical and electronic engineering, in 2005.

He majors in manufacturing execution system, production planning and scheduling, industrial control system network security technology and so on.

Dr. Shang is currently a researcher in Shenyang Institute of Automation Chinese Academy Sciences and reviewer of several journals such as “Journal of Systems Engineering”, “Systems Engineering and Electronics”, “Information Sciences” and so on.

Quansheng Qiao was born in Baotou, Inner Mongolia, China, in 1989. He received his bachelor degree from Hebei University of Engineering in 2014. He is currently a master degree candidate of Shengyang Jianzhu University, studying in Shengyang Institute of Automation Chinese Academy of Sciences.

Ming Wan received the BS degree from Beijing Jiaotong University in Jul. 2007, and received the Ph.D. degree in communication and information system from National Engineering Laboratory for Next Generation Internet Interconnection Devices of Beijing Jiaotong University in Jan. 2013.

He is a research assistant in Lab of Industrial Control Network and System of Shenyang Institute of Automation Chinese Academy of Sciences. His research interests include the areas of architecture of future Internet, network and information security and industrial control network security.

Peng Zeng received the BS degree from Shandong University in 1998, and received the Ph.D. degree in Shenyang Institute of Automation Chinese Academy of Science.

He is a director in lab of Industrial Control Network and System of Shenyang Institute of Automation Chinese Academy of Sciences.