Research and Implementation of Secure Industrial Communication Protocols

Wang Jingran[1,2,3], Liu Mingzhe[1,2], Xu Aidong[1,2], Hu Bo[1,2], Han Xiaojia[1,2,3], Zhou Xiufang[1,2,3]
[1]Laboratory of Industrial Control Network and System, State Key Laboratory of Robotics, Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang, China
[2]Institutes for Robotics and Intelligent Manufacturing, Chinese Academy of Sciences, Shenyang, China
[3]University of Chinese Academy of Sciences, Beijing, China
wangjingran@sia.cn, lmz@sia.cn, xad@sia.cn

***Abstract*—Industrial control systems(ICS) are widely used in national infrastructure such as electricity, water conservancy and energy to control the operation of production equipment. The ICS information security problems will cause a series of consequences. This paper focuses on the security problems existing in industrial communication protocols, studies the secure protocols to guarantee the secure transmission of industrial datas, and realizes the end-to-end identity authentication and data encryption transmission on Modbus/TCP protocol.**

Keywords—ICS information security, industrial communication protocols, identity authentication, data encryption, Modbus/TCP

I. Introduction

Recently, attacks aimed at ICS happened frequently, which has caused serious impacts on industrial manufacturing. In December 2015, three energy companies in Ukraine were attacked by the malware "BlackEnergy", causing a large power outage in the capital and western area of Ukraine, 1.4 million residents were under the influence. In December 2016, the Ukrainian power grid encountered an attack again, causing its capital powered off for more than an hour. In July 2010, the Stuxnet virus invaded the Iranian nuclear power plant. It searched for the PLC and periodically changed its operating frequency to controlled the speed of the centrifuges, destroyed one-fifth of the centrifuges in Iran, and ruined Iran's nuclear plan[1]. People attach more importance to the information security of ICS because of the rising rates of the attacts. Industrial communication protocols utilized as a media of data transmission are suffering from the hostile attacts as well.

II. Security Issues of Industrial Communication Protocols

Industrial communication protocols are widely deployed in field devices, controllers and host computers for the transmission of industrial field datas. Strengthening the security protection of industrial communication protocols is an important part of ensuring the information security of ICS.

There are many specific protocols in the industrial control system, which applies in different industrial situations. However, these industrial communication protocols are not designed to take security issues into account due to the industry-specific real-time and high efficiency consideration[2]. At the same time, the industrial control network before was an “island” and had no connection to the outside world, so it was quite safe at that time[3]. However, with the industrialization of the information technology, the security level of industry communication networks is gradually reduced. As a consequence, it is necessary to add the security functions to the industrial communication protocols.

The main reason for data tampering, data theft and replay attacks which are commonly occured in industrial control systems is that the communication protocols are lack of the identity authentication protection mechanism in the process of data transmission, and the datas are plaintext while transmission. It is convenient for illegal intruders to attack the vulnerabilities of the protocols.

III. Design of The Secute Communication Protocols

For the information security problems of ICS, the main solution is based on the improvement of Internet information security technologies to make them suitable for industrial control networks. The main protection measures include access control (identity authentication, network isolation, firewall, physical security), protection reinforcement (device reinforcement, host intrusion prevention, patch management), condition monitor (intrusion detection, security audit), and emergency response (equipment redundancy), etc[4]. The measures mentioned above are able to provide a systerm-level protection of the ICS.

For the security protection of the industrial communication protocols, the solution is utilized on the principle of cryptography. The design of a secure communication protocol can be considered in two aspects. The first option is to improve the protocol itself by adding some cryptographic protection techniques. E.g. Liu Fei et al, implemented the security requirements of Modbus/TCP protocol by using symmetric encryption and digital signature technology to achieve confidentiality requirements, identity authentication and hash chain-based anti-replay mechanism. They changed the data frame structure of the protocol to implement security features[5]. The second option is to protect the industrial communication protocol by adding an external encryption protocol.

This paper adopts the second method, and plans to achieve the goal of secure transmission of industrial field datas by adding the SSL/TLS protocol, which is widely used in the Internet for data secure transmission. Taking the traditional industrial communication protocol Modbus/TCP

as an example, developed the secure communication protocol based on the SSL/TLS technology.

IV. Development of Secure Communication Protocols

A. Industrial Communication Protocol – Modbus

The Modbus protocol is a communication protocol developed by MODICON in 1979 and is an industrial fieldbus protocol standard[6]. Because of its openness, scalability and standard features, it has now become one of the most widely used communication protocols in industrial automation field.

The Modbus/TCP protocol is a Modbus message transmission protocol running on TCP/IP[6]. Field devices can communicate via a network such as Ethernet through this protocol. The port number of the Modbus/TCP protocol is 502. Fig. 1 shows the implementation of the Modbus protocol over serial links and TCP/IP.

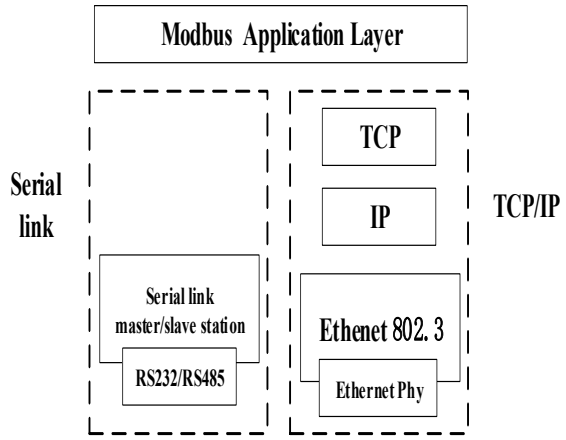

Fig. 1 Modbus protocol OSI model

B. Secure Transport Protocol - SSL/TLS

The SSL/TLS protocol is located on top of the TCP connection, providing a transparent and secure transmission channel for both parties to ensure end-to-end secure communication[7]. The protocol includes encryption mechanism and certificate authentication mechanism to provide security protection for the upper layer protocols. Currently, the SSL/TLS protocol is widely used in the fields of Internet and e-commerce.

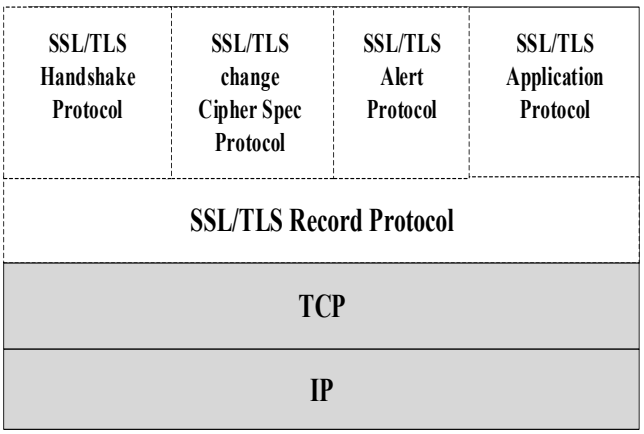

Fig. 2 SSL/TLS protocol structural model

This protocol is divided into two layers: the record protocol and its upper Handshake protocol, Change Cipher Spec Protocol and Alert Protocol [8]. Fig. 2 is the structural model of the SSL/TLS protocol.

C. Secure industrial communication protocol——sec-Modbus

The design of the secure communication protocol in this paper utilized the SSL/TLS protocol to provide a encapsulation protects of the Modbus/TCP application layer datas. The SSL/TLS protocol is transparent to the application layer and data encrypted transmission is performed through a secure channel established during the handshake process. The Record protocol is under the Handshake Protocol and performs the function of data encryption. Fig. 3 shows the OSI model of the secure Modbus protocol.

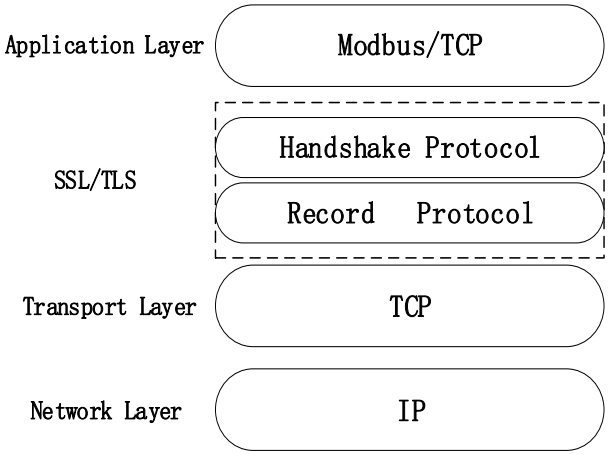

Fig. 3 Secure communication protocol OSI model

V. Implementation of Secure Communication Protocols

The solution of the security protocol proposed in this paper is mainly based on two parts: The first part is the Modbus protocol implementation. As for this part, we chose the FreeModbus protocol developed for embedded systems with an open source platform; The second part is the implementation of SSL/TLS protocol. Considering the system consumption, this paper chose to use mbedtls, an SSL protocol library developed for embedded environment. Mbeddls mainly consists of three parts: SSL/TLS protocol library, encryption library and X.509 certificate processing library. This experiment was based on the PC platform.

A. Implementation of identity authentication

In this experiment, we carried out the server-side identity authentication. The authentication process is implemented by verifying the server's digital certificate exchanged during the TLS handshake phase. Fig. 4 shows the digital certificate generated by the server. The certificate includes the version number, user's name, validity, signature algorithm (sha256 was adopted in this experience) and public key, etc. The client validated the content after receiving the certificate. Only if the authentication is successful, the communication session can be continued, otherwise the session will be interrupted.

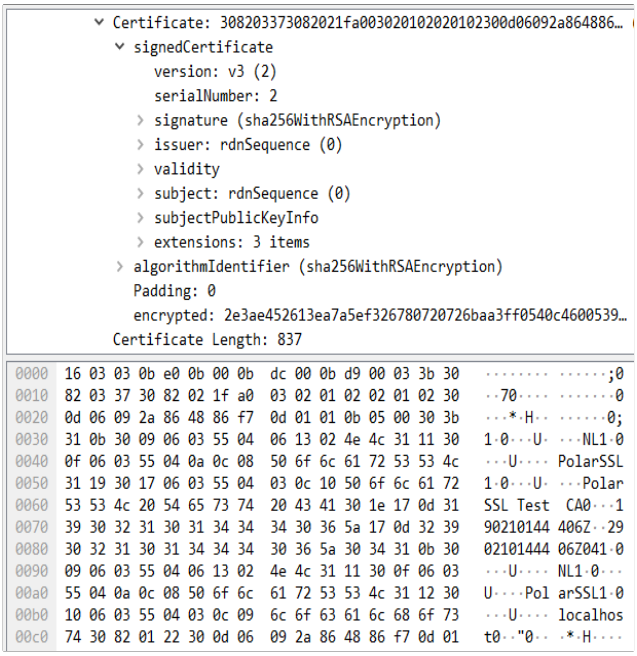

Fig. 4 digital certificate

Figure 5 shows the information exchange process captured during the handshake phase by using the Wireshark software. Multiple pieces of information were exchanged by the communication parties during the handshake process. The imformation was utilized for identity authentication and negotiating the meassage(e.g. the session key) used for next secure communication.

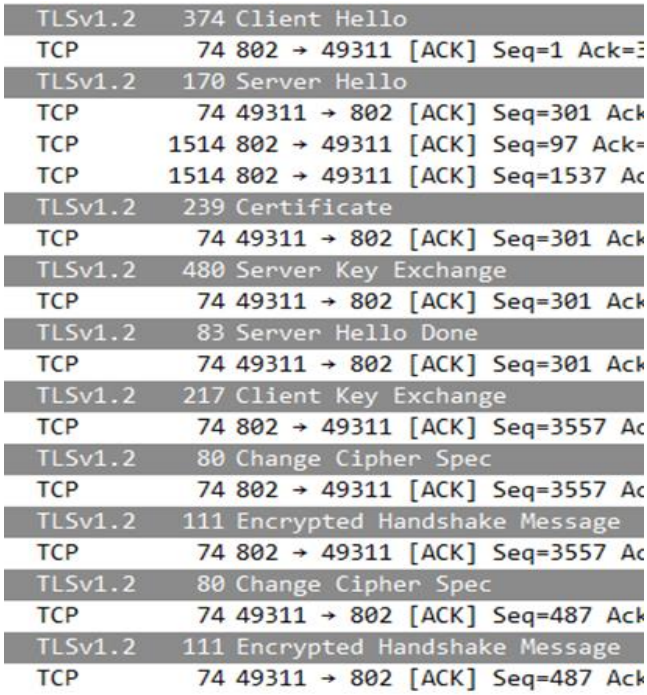

Fig. 5 Handshake process

B. Implementation of Data Encryption

The implementation of data encryption is based on the TLS record protocol. Modbus/TCP datas encrypted transmission is performed after the two parties handshake successfully. In this paper, the Modbus 04 function code (read input coils) was taken as an example to write datas to 10 coils, and the encrypted transmission was performed on the basis of the original Modbus/TCP data frame.

Fig. 6 shows an example of the data frame structure (hexadecimal) of Modbus/TCP in this experiment. 06BC stands for protocol identifier, 0000 stands for Modbus protocol, 0017 stands for data length, 01 stands for slave address, 04 stands for function code, 14 stands for data segment length, and the rest stands for Modbus/TCP data segment.

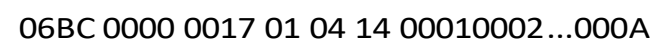

Fig. 6 Modbus/TCP frame structure

The data frame above was encrypted and transmitted to the client through the encrypted channel , and the secret key used for encryption was negotiated while the TLS handshake phase. Fig. 7 shows the encrypted Modbus/TCP datas captured while transmisson. In this experience, taking real-time issues into consideration, chacha20-ploy1305 encryption algorithm was chose for data encryption. Chacha20-ploy1305 algorithm is a new stream encryption algorithm that Google optimized for mobile CPU. It can reduce the amount of encrypted and decrypted datas, and its performance is obviously improved compared to ordinary algorithms.

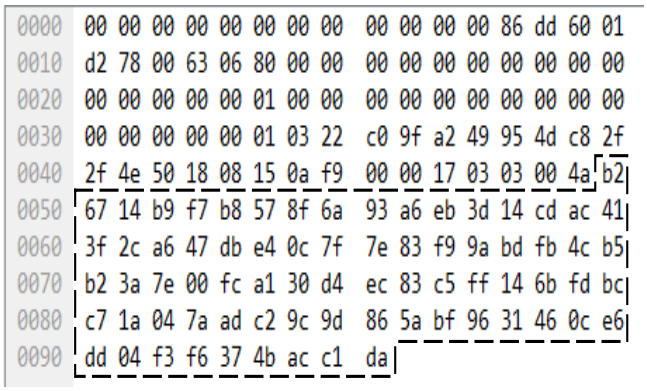

Fig. 7 encrypted Modbus/TCP datas

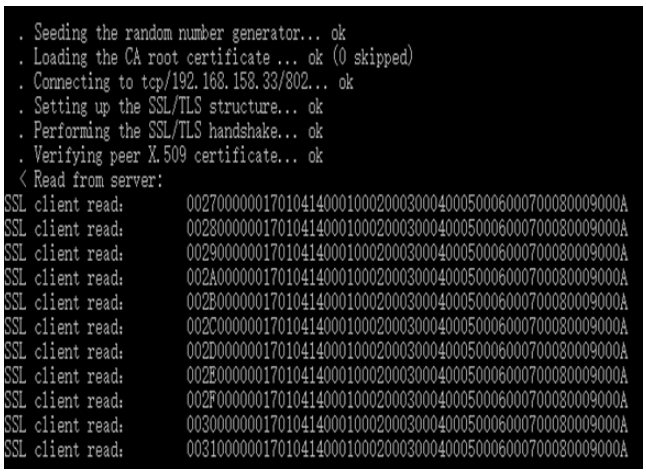

Fig. 8 Client secure communication process

Fig. 8 shows the entire communication process performed by the client during the transmission of the secure communication protocol. First, the client and the server performed a handshake process to establish a secure transmission channel. After the channel was built

successfully, the server sent the encrypted datas to the client. The Modbus/TCP protocol uses the polling mechanism so the client will continuously receive the datas sent by the server after the protocol is turned on. The datas showed in the figure below has been decrypted by the client.

VI. Conclusion

This paper analyzed the security problems existing in industrial communication protocols and protected the protocol datas by adding an external security protocol (TLS). The Modbus/TCP protocol was taken as an example to develop the secure protocol, and realized the end-to-end identity authentication and data encryption transmission of the industrial control networks. By adding the secure mechanism to the protocol, we improved the security of industrial datas in the transmission process.

This experiment has now completed the development of a secure communication protocol on the PC platform. It will be applied to embedded systems in the next plan. Considering of the real-time requirements and data processing capability of the ICS, the handshake process will be simplified to minimize the number of information exchanges. At the same time, encryption is a little bit heavy for ICS, so appropriate password length and password groups will be selected to ensure secure communications without affecting the normal operation of the system.

Acknowledgment

This work is supported by Research on Multi-Controller Cooperative Trusted Interconnection and Service Protocol for Distributed Control No. 2018YFB1702202.

References

[1] S. Al-Rabiaah, "The “Stuxnet” Virus of 2010 As an Example of A “APT” and Its “Recent” Variances," 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, 2018:1-5.

[2] Yu Yao, Liehuang Zhu, Chuankun Wu. Industrial Control Network Security Technology and Practice[M]. Beijing:Mechanical Industry Press, 2017

[3] Tao Feng, Wei Lu, Junli Fang. Overview of Vulnerability and Security Protection Technology of Industrial Ethernet Protocol[J]. Transactions of Communications, 2017, 38(365):189-200.

[4] Mclaughlin S , Konstantinou C , Wang X , et al. The Cybersecurity Landscape in Industrial Control Systems[J]. Proceedings of the IEEE, 2016:1-19.

[5] Fei Liu, Renbin Zhang, Gang Li, et al. Modbus/TCP security authentication protocol based on hash chain and synchronization mechanism[J]. Journal of Computer Applications, 2018, 35(318):215-232.

[6] Weixuan Gao. Design and implementation of information security active defense system for industrial control system based on Modbus protocol [D].

[7] Tianmu Li. Security Analysis and Improvement of SSL/TLS Protocol [J]. Information Network Security (01): 49-52.

[8] Turner S . Transport Layer Security[J]. IEEE Internet Computing, 2014, 18(6):60-63