Proceeding of the 11th World Congress on Intelligent Control and Automation
Shenyang, China, June 29 - July 4 2014

Research on the security mechanism for interconnection between PROFIBUS and Internet

Yuan Zhou, Dan Chai, Mingshan Liu[1†], Fengxue Lin,Wendong Shang

College of Communication Engineering
Jilin University
Changchun, China

Liang Wang

Armoured Force Military Representive Office
in Changchun Region
Changchun, China

***Abstract*—The connection between PROFIBUS network and Internet can realize remote real-time monitoring device on the fieldbus. This paper conducts detailed analysis and research advance on network security based on the interconnection methods between PROFIBUS and Internet, and proposes a PROFIBUS industrial network security model. An embedded gateway is developed especially for meeting the security requirement in this research work. With compact structure and low cost, it paves the way to realize real-time monitoring PROFIBUS device safely via Internet.**

***Index Terms*—PROFIBUS, Embedded Gateway, Security**

I. INTRODUCTION

PROFIBUS is the most popular fieldbus in manufacturing, process control and automation at present. How to make the fieldbus network access to Internet and enable the enterprise's information network and control network interconnect has become a research hotspot of industrial network technology.

The industrial network is different from other commercial networks due to its service environment and purpose. Generally, the industrial network in enterprise is structured by two parts, information network and control network. The information network is used to enterprise management. The control network connects the production devices and equipments together and makes the production process control and monitor centralized. In this research, the control network is based on PROFIBUS. As an independent unit, the business information confidentiality and preventing hacker invasion is crucial to the enterprise internal network. To realize remote control and management to production process, status and parameters of production equipment should be real-time provided. In other words, the control system based on PROFIBUS should be accessed via the industrial network and Internet. Therefore, reliable and effective security method should be taken when the network interconnect. Currently there is no unified solution to solve the network security problems when embedded gateway is used to connect to Internet. Because of the limited embedded resources, the existing security policy for PC could not be put to use directly. It is necessary to design a compact security strategy according to the practical application scenario for PROFIBUS. In this research, a method based on embedded Web gateway is proposed to realize the interconnection between PROFIBUS-DP network and Internet and some compact security methods are proposed to provide security assurance when user access to the PROFIBUS device via Internet.

II. Method of PROFIBUS accessing to Internet

PROFIBUS-DP protocol structure adopts three layers structure model based on ISO7498, including the physical layer, data link layer and user interface layer. While TCP/IP adopts four layers structure model, including the network interface layer, network layer, transport layer and application layer. To realize the interconnection and communication between two kinds of heterogeneous networks, a suitable method must be taken to connect the PROFIBUS network with the Internet.

At present there are four kinds of devices for network interconnection, including repeater, Bridge, router and gateway. Gateway is also known as network protocol converter, it is used to implement interconnection and communication between heterogeneous networks. So an embedded gateway is used to realize the interconnection between PROFIBUS network and Internet in this research. Configuring like this, heterogeneous networks might communicate each other without changing the original network structure and is beneficial to preserve existing investment. Figure 1 illustrates the interconnection between PROFIBUS-DP and Internet using a gateway.

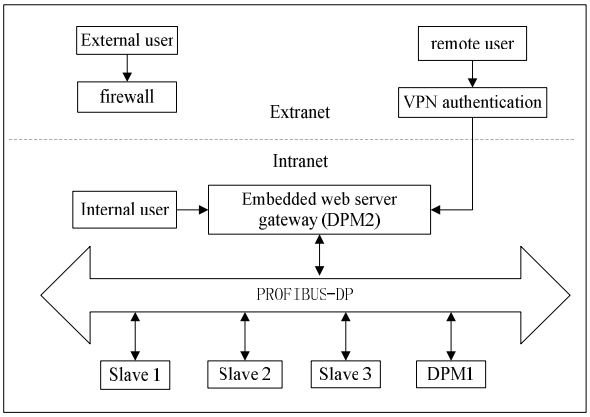

Figure 1. Illustration of interconnection between PROFIBUS and Internet

In PROFIBUS-DP, up to 127 devices, masters or slaves, can be connected to one bus. PROFIBUS-DP system differentiate between the following device types: DP slave, DP

† *Corresponding Author: Mingshan Liu, Associate Professor, College of Communication Engineering, Jilin University*

978-1-4799-5825-2/14/$31.00 ©2014 IEEE

class 1 master (DPM1) and DP class 2 master (DPM2). The embedded Web server gateway is as a DPM2 in Figure 1.

A PROFIBUS-DP system configured with 1 DPM1, 3 slaves and 1 DPM2 (embedded gateway) is adopted in this research. Structure of PROFIBUS-DP system with more devices is similarly and method of connection is consistent. According to the PROFIBUS addressing principle, the address of the DPM1 is 1, the address of the DPM2 is 3, the addresses of slave 1、 slave 2、 slave 3 are 4、 5、 6 respectively. The embedded Web Gateway here is mainly used to perform protocol conversion between PROFIBUS protocol and TCP/IP protocol and authenticate users who get access to PROFIBUS-DP system from either intranet or external network. In this case, all of network access requests must go through the gateway. It adopts B/S (Browser/Server) mode to achieve the user's visit to the embedded server.

Client sends access request to the PROFIBUS-DP bus device from a browser via Internet to the embedded Web gateway. After authentication, the embedded Web gateway sends query request or control request according the client to the slave device which is as the client's access object. Slave device responds the request and transmits data to the gateway. During this process, the gateway performs protocol conversion between PROFIBUS protocol and TCP/IP protocol, data processing, as well as releasing the equipment information in the form of Web pages with the help of Web server.

In terms of security policy, firstly, firewall should be used to isolate the extranet and intranet to ensure the security of intranet. Secondly, for the remote user, they are permitted to operate the devices only after checking VPN password and authentication of identity and authorization[1]. Thirdly, in the intranet, the identity authentication and data encryption technology are used to prevent part of the intranet users eavesdropping other users' information, accessing unauthorized resources, and even modifying system files illegally. In this paper, the third security policy is mainly analysed and designed.

III. Analysis and design of security mechanism

For industrial Ethernet, the security threats mainly come from two aspects. First kind of threat is mainly caused by attackers' visiting the network resources or accessing the control system without authorization. This can lead to loss and misusing the confidential information and endangering system safety. Second kind of threat is mainly caused by attackers' eavesdropping, tampering and pretending confidential information, it is mainly reflected in the process of data communication between Internet and control network.

In this research, the embedded Web gateway is adopted as communication platform and it is the hub of the PROFIBUS network monitoring system. It connects several master devices and slave devices via PROFIBUS-DP inward and connects Internet via LAN or Modem outward. Data transmission and communication between Internet and PROFIBUS-DP is controlled by the embedded Web gateway. Due to the embedded Web gateway is as the "hub" for user on the Internet accessing to the device, it is the key point of network security in the PROFIBUS network monitoring system.

According to application of the embedded Web gateway in PROFIBUS-DP, network security mechanism introduced in this paper is mainly from three aspects. Firstly, the security of embedded platform itself is the basis. That is to say the gateway itself must ensure the protocol conversion is correct, this is the basis of correct transmission of information between user and PROFIBUS-DP device. Secondly, access control mechanism should be adopted to prohibit illegal user access to the unauthorized resource. Thirdly, security technology for data transmission should be taken to prevent the attackers decoding the system confidential information[2]. It should make sure that the data is reliable by authentication, and protect from network active attack, such as tampering and pretending.

A. Protocol conversion

Structure of PROFIBUS protocol and TCP/IP protocol are different. The correct protocol conversion is the basis to realize safety remote operation of device on PROFIBUS-DP via Internet. As DP class 2 master, the gateway designed in this paper has its own independent PROFIBUS address. At the same time, it is connected to the Internet, so it also has its own IP address. The address conversion diagram is as shown in Figure 2. When user on the Internet want to access and control PROFIBUS device, browser sends a frame of TCP/IP protocol to the gateway, source address of the frame is PC's IP address, and destination address is gateway's IP address, device's address and manipulating information are stored in the data items of the frame. When the gateway receives the frame of TCP/IP protocol, it unpacks the packets according to TCP/IP protocol format and gets the application layer data. Then the gateway packs this data in accordance with the PROFIBUS protocol format. Now source address of the PROFIBUS protocol frame is gateway's PROFIBUS address, destination address is the device's PROFIBUS address. Then the data that packed by PROFIBUS protocol format can be transmitted on the PROFIBUS. On the contrary, when the device response to the request of the gateway, the device sends data in PROFIBUS protocol frame to the gateway, source address of the frame is the device's PROFIBUS address, destination address is the gateway's PROFIBUS address, the gateway unpacks packets according to PROFIBUS protocol format, and then pack the data according to the TCP/IP protocol format. Source address of the packed frame is the gateway's IP address, destination address is PC's IP address. Then the data that packed by TCP/IP protocol format can be transmitted on the Internet. Protocol conversion principle diagram is as shown in Figure 3[3].

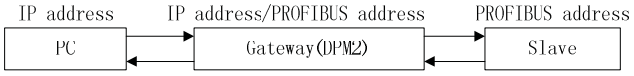

Figure 2. The address conversion

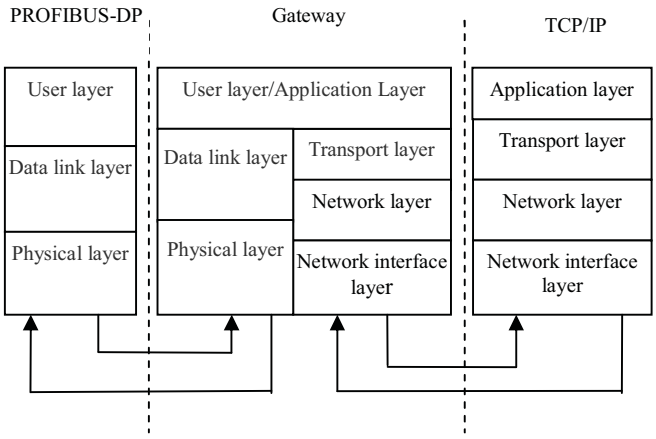

Figure 3. Protocol conversion principle of PROFIBUS and TCP/IP

B. Identity authentication and mandatory access control

To ensure security of PROFIBUS network, the first thing that should be taken into account is to prevent illegal access. Only the authorized users can be allowed to access to PROFIBUS system. This paper adopts the idea of mandatory access control. The user's authorization of remote access is not determined by themselves. The whole system has a top administrator. The top administrator set authorizations for all resources uniformly and allocate a label for all resources and users. The labels comprise authorizations of administrator and ordinary user. The administrator is allowed to view the device's state and control device, the ordinary user only can view the device's state. In this paper the embedded database technology and dynamic Web page technology – CGI are used to realize identity authentication and access control.

Data information is the most important information in the industrial control network. And database technology is widely used to organize and store data, as well as retrieve and process data with high-speed. The role of the database in this design mainly has two aspects. Firstly it is used to manage user information. Secondly it is used to maintain a large number of shared data of devices. In order to ensure the real-time performance, the control information can be issued directly to the devices rather than via the database. With the development of embedded technology, embedded database technology also steps into wide application stage from research stage. SQLite is a light embedded database, it occupies less resources and supports Linux operating system and C programming language. At the same time it has high processing speed. SQLite is used in this design to create an authorization database, the database contains user's name, the corresponding password and user's authorization. While the designed login interface does not display user's authorization, only shows the input area of user's name and password. This guarantees confidentiality of information and prevents illegal users to sabotage the system. For example, when the illegal users become aware of that the system has administrator authority through the login page, they might carry out brute force attack to login the system. Once they login successfully and operate equipment illegally, it will disrupt the normal operation of equipment and even cause a fatal damage to equipment. The created authorization database is as shown in Figure 4.

```
sqlite> .mode column
sqlite> .header on
sqlite> select *from tb1;
username    password    authority
----------  ----------  ----------
chaidan     3141846     guanliyuan
liming      2354321     putongyong
wanglong    1234567     putongyong
sqlite>
```

Figure 4. Authorization database

Common Gateway Interface (CGI) is a standard interface for external extension program's interaction with the Web server. When the Web server identifies the request sent by the client browser is a CGI program rather than a normal static HTML page, the Web server will activate the CGI program[4]. In the process of industrial equipment monitoring, the corresponding CGI application program is used to read user information that inputted in the browser by the user. At the same time the CGI program operates the authorization database and determines the authority and access level of the user. If the user is not authorized, the gateway forbids the user to access to the system. While if the user is legitimate, CGI program determine whether the user is an administrator or an ordinary user, and then return to the corresponding user interface according to the user's authorization. Figure 5 is the identity authentication flow chart.

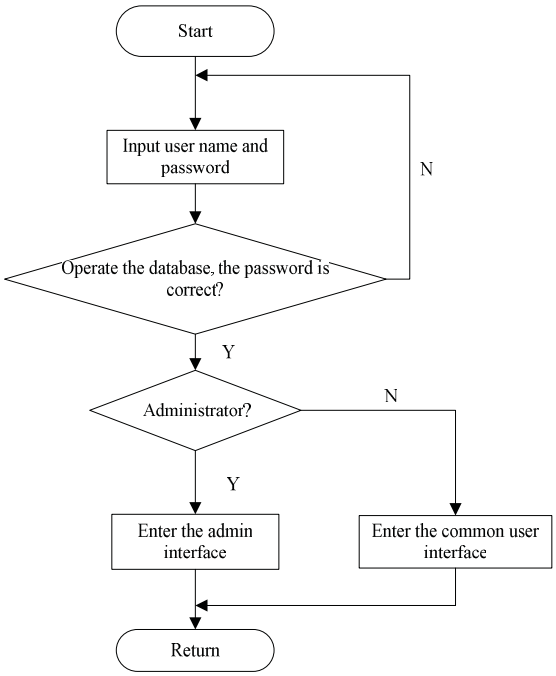

Figure 5. Identity authentication flow chart

C. Security of data transmission

User information and equipment information are transmitted in plaintext in the network if no data encryption processing operations is adopted. The illegal users might intercept user information and equipment information by using

Network capture software, even tamper with the equipment data, it is also a fatal security problem, so the user information and equipment information must be encrypted before transmission.

SSL (Secure Socket Layer) protocol is a kind of safety protocol that provides confidential service based on Internet, and it works between the transport layer and application layer. It provides the safe channel with three characteristics: confidentiality, certainty, reliability[5]. In this paper, the embedded Web technology is used to realize the interaction between client and devices, and the application layer protocol is HTTP protocol. The current mainstream browsers such as Internet explorer and Firefox support SSL. The Appweb server selected in this paper also supports SSL. So we just need to transplant the embedded SSL protocol in the embedded gateway and enable SSL in the Appweb server configuration file. When HTTP is used to communicate based on SSL protocol, user name, password, and control data have become a part of encrypted SSL data flow, the packets transmitted on the Internet will not be leaked, eavesdropped, intercepted or forged. Obviously this method greatly simplifies the development process, reduces the development cycle, at the same time ensures the safety of data transmission.

IV. Realization of the embedded secure Web gateway

A. *Design of hardware*

The hardware structure of Embedded Web gateway is as shown in Figure 6[3]. The packets from Internet are transferred to the ARM processor S3C2440 via RJ45, network isolation transformer and network chip DM9000. The packets from the PROFIBUS-DP are transferred to the ARM processor S3C2440 through RS-485 bus driver. The S3C2440 processor is responsible for processing data transmitted between Internet and PROFIBUS-DP.

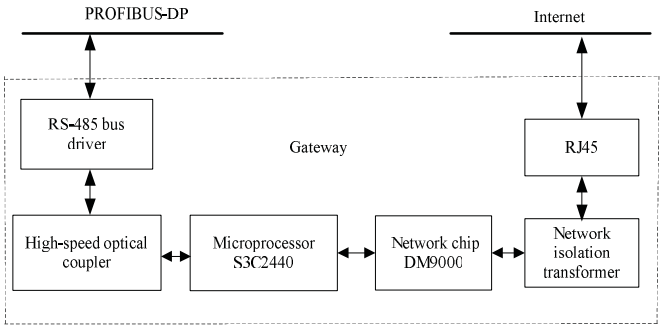

Figure 6. Structure of Embedded Web gateway

B. *Implementation of software*

The embedded Linux operating system is transplanted on the embedded gateway platform. To provide security protection, the embedded Appweb server, embedded database SQLite and embedded SSL protocol Matrixssl are transplanted to it also. The software architecture of embedded Web gateway is as shown in Figure 7.

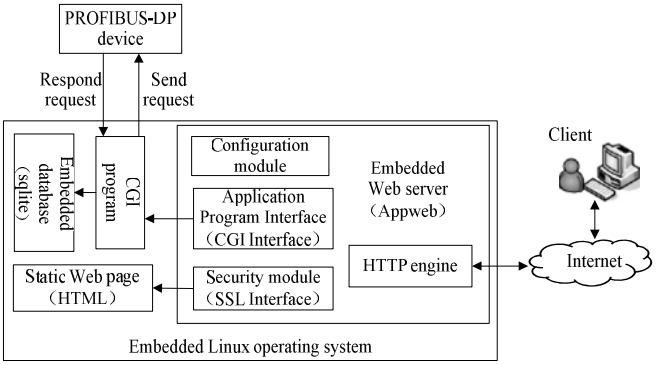

Figure 7. Software architecture of embedded Web gateway

1) Implementation of the identity authentication and access control.

The login page is written in HTML language and stored in the directory /www of file system. Set the default access path /www in server configuration file. When users enter IP address of the gateway in the browser the login interface will be displayed. Users input the user's name and password in the login page, the CGI interface of server will call CGI program of user identity authentication. Enter the gateway's IP address 192.168.1.230 in the browser, the login page appears, as show in figure 8.

Figure 8. The login page

2) Realization of data transmission security.

In order to test the validity of SSL protocol designed in the security module, the Iris Network capture software is used to intercept packets.

Add statements to enable the SSL module in the Appweb server configuration file, and access the Web server's port 443 in a safe way, input "https://192.168.1.230" in the browser, intercept packets by Iris. As shown in Figure 9, we can see the data is encrypted, just some gibberish, and can't find any useful information.

Figure 9. Captured packet with using SSL protocol

V. Conclusion

To realize remote monitoring, an interconnection method between Internet and PROFIBUS-DP network based on the embedded Web gateway is put forward in this paper. For the security requirement of industrial network based on PROFIBUS, several security measures are proposed when the PROFIBUS network access to the Internet in this research. Analyzing the security mechanism and implementation method, the protocol conversion method between PROFIBUS and TCP/IP is designed, and it is the basis of secure operation of PROFIBUS-DP device via Internet. Secure mandatory access control mechanism of the user identity authentication is designed and implemented. It can guarantee that only the authorized users can access to the authorized system resources. The embedded SSL security technology is also adopted especially for security requirement and transplanted to the embedded web gateway. Using this method, the secrecy and safety of the data of user information and equipment data can be protected effectively when PROFIBUS-DP is accessed via Internet. With the embedded secure Web gateway, the managers and engineers can control and manage the equipment and production process in time remotely, safely and effectively via Internet. The achievement has great significance for enterprise in reducing production cost and speeding up development of industrial informatization and network, and is helpful in configuring the integrative and secure industrial enterprise network.

REFERENCES

[1] GUO Meng,, QIAN Jiang, "A Design of Security Model for Control Network of Industrial Ethernet", Microcomputer Information, 2008(11-3),pp.53-55.

[2] ZHAO Yuehua, DU Yunhai, BAO Mingguo, "Implementation of Security in Embedded Web Gate Based on Authentication", Computer Engineering,2004(23),pp.111-113.

[3] LiTing, "Research and Implementation of Remote Monitoring Methods Based on IPv6 and PROFIBUS",[D], Jilin University, 2013.

[4] CHEN Tian-huang, HUANG Jia-xi, " Design and Realization of CGI in Embedded Dynamic Web Technology", 2007 IFIP International Conference on Network and Parallel Computing – Workshops,2007,pp. 774-777.

[5] SHEN Yong, ZHU Chao, "Design and Implementation of Embedded Web Server Security Based on SSL", Computing Technology and Automation, 2012(7),pp. 160-162.