Design and Implementation of 802.1x Authentication Module in Security Switch for Industrial Control System Based on FPGA

Yanan Zou
Department of Control Science and Engineering
Zhejiang University
Hangzhou, China，(86)18768163494
YNZou.Melinda@gmail.com

Dongqin Feng*
Department of Control Science and Engineering
Zhejiang University
Hangzhou, China，(86)13957166054
dqfeng@iipc.zju.edu.cn

***Abstract*—Aiming at the safety of the industrial control system, an authentication module based on 802.1x with dual authentication model in safety switch is proposed. The authentication mechanism of 802.1x is stated. The dual authentication model, namely the authentication between the safety switch and the server and the authentication between the client and the server, is raised. The EP4CGX75 chip of Altera company is chosen as the hardware developing platform. The design and realization in FPGA has been researched. The simulations indicate the correctness and validity of the model designed.**

Keywords-Safety of Industrial Control System; 802.1x; FPGA implementation

I. INTRODUCTION

With the development of the computer technology and control technology, the development trend of the industrial control system is digitization, networked and precision. The structure of the control system has been from the initial CCS (computer centralized control system) to the second generation of DCS (distributed control system), and now it's FCS (field bus control system) [1]. The data collection of the industrial control system is dispersive, and the system functions rely on the remote communication implementation. These lead to a lot of potential danger in the industrial control system.

In recent years the attacks aiming at the industrial control system emerge constantly. End in October 2011, there has been more than 200 attacks to the industrial control system in the global[1]. At present the industrial control system is widely used in electric power, water conservancy, oil and gas, and large manufacturing. According to incomplete statistics, more than 80% of the key infrastructures involved in the people's livelihood rely on the industrial control system to realize the automation work. Industrial control system has been an important component of the national security strategy[2]. The information security of the industry control system becomes particularly important.

As the important information interaction equipment of the industrial control system, the switches become an important role to ensure the information security. The security switches proposed in this paper have these functions, such as users' identity authentication, encryption and access control and so on. The data in the security switch network is encrypted to ensure the safety of network. The user authentication uses 802.1x protocol[3]. The 802.1x authentication module uses dual authentication mechanism to control the identity of the accessing switches and the identity of the accessing users.

This work is supported by the 863 national projects (No. 2012AA041102).

II. DESIGN OF THE 802.1X AUTHENTICATION MODULE

The 802.1x authentication for most Internet focuses on the authentication between the clients and the server, but this way only guarantees the legitimacy of the user's identity. If an attacker accesses the switch network with a switch, he can steal data from the net, and then to attack the network. In this kind of situation, this paper puts forward the dual authentication mode, namely the combination of the authentication between the safety switch and the server and the authentication between the client and the server. This method not only ensures the legitimacy of the user identity, but also can prevent illegal switches from accessing to the network effectively, so as to prevent network data from being stolen. Based on the design ideas, the 802.1x authentication module needs to realize two functions. One is the authentication between the safety switch and the server to ensure the safety of the network. The other one is the authentication between the clients and the server to ensure user's identity.

A. Authentication Mechanism of 802.1x Protocol

The 802.1x authentication is a kind of access control protocol based on port. It includes three parts: the authentication server, the authentication equipment and the client[4]. In this paper the authentication equipment is the security switch. The logic ports of 802.1x authentication are divided into the authentication ports and data ports. The authentication ports can transmit the authentication messages in either authenticated state or not-authenticated state, while the data ports can only transmit the data messages in authenticated state. In this way the 802.1x protocol can realize the access control. In this paper the authentication process includes two sub-parts: 1.The authentication between the security switch and the server, 2.The authentication between the clients and the server. Only when the authentication of security switches is

© 2012. The authors - Published by Atlantis Press

finished, the authentication between the client and the server begins.

1) Authentication Process between the Security Switches and the Server

Each security switch includes built-in legitimate user name and authentication password. It requests the authentication with the server when power is on. The whole communication process is shown in Fig.1.

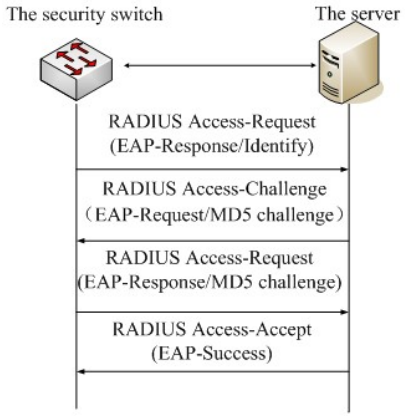

Figure 1. Authentication process between the secutity switch and the server

- The security switch will package EAP-Response/Identity message containing user name to the RADIUS Access-Request message, and send it to the authentication server.
- The authentication server produces a Challenge and sends the security switch RADIUS Access-Challenge message, including EAP-Request/MD5 Challenge, requesting to the response of the security switch.
- After receiving EAP-Request/MD5 challenge message, the security switch does the MD5 algorithm with the password and challenge. The result is called Challenged-Password. Then the security switch sends Challenged-Password, Challenge and user name to the server together.
- The server does MD5 algorithm according to the user information, judging if the switch is legal. Then the server responds the authentication success/failure message to the switch.

2) Authentication Process between the Client and the Server

The authentication process between the client and the server is shown in Fig.2.

The 802.1x authentication process is as follows[5]:

- The client sends an EAPOL-Start message to the security switch requesting the authentication.
- After receiving the client authentication message, the security switch responds an EAP-Request/Identity message to ask the client to send the authentication information.
- The client responds EAP-Response/Identity message to

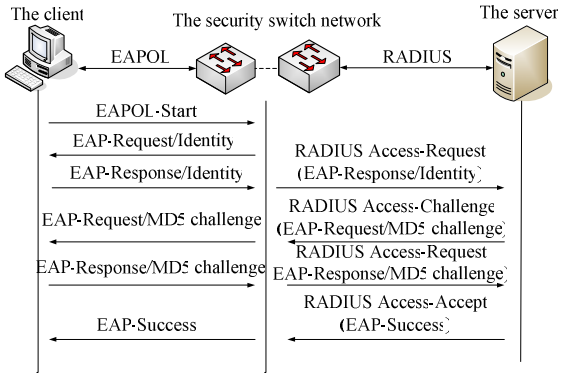

Figure 2. Authentication Process between the Client and the Server

the security switch, which contains the user name and other information.

- The security switch will package EAP-Response/Identity message to the RADIUS Access-Request message, and send it to the authentication server.
- After receiving the user name from the security switch, the server compares it with the user name table in the database to find the corresponding information of user password. Then the sever generates a random encryption word with MD5 encryption.
- After receiving EAP-Request/MD5 challenge message, the client does the MD5 algorithm with the password and challenge. The result is called Challenged-Password. Then the client sends Challenged-Password in the EAP-Response/MD5-Challenge to the security switch.
- The security switch returns RADIUS Access-Request message to the server.
- The authentication server compares the received encrypted authentication information with its own authentication information after encryption operation. If they're the same, the user is through the authentication and the server sends RADIUS Access-Accept message authentication to the security switch. The security switch sets the port state to Authorized Port, and sends EAP-Success message to the client to inform the client that the data port is already open. If they're different, the authentication is failed. The server sends authentication failure message to the security switch. The security switch port keeps an Unauthorized Port[6].

B. Design and Implementation of the 802.1x Authentication Module

Quartus of Altera company is adopted as design software in this paper. EP4CGX75 chip of a series of Cyclone4 of Altera company is adopted as hardware development platform, including 73,920 logic elements and 24,500,000 bits data.

The structure diagram of 802.1x authentication module is as shown in Fig.3, including the input control module, the switch authentication module, the user authentication messages conversion module and the arbitration and send module.

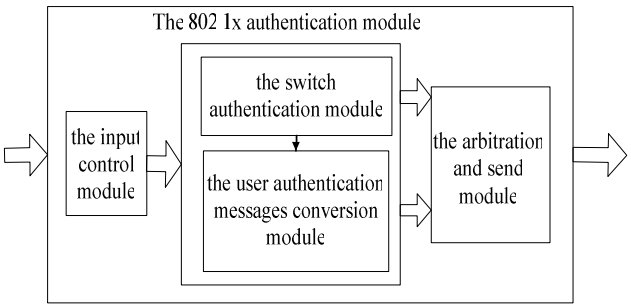

Figure 3. Structure diagram of 802.1x authentication module

The function of each module is: (1) the input control module: to control the timing of messages sent to the switch authentication module and user authentication messages conversion module, to ensure the two modules above can correctly receive all messages. (2) the switch authentication module: to complete the authentication of switches. (3) the user authentication messages conversion module: to complete the protocol conversion of the user authentication messages. (4) the arbitration and send module: to decide to send which authentication messages and control output timing.[7]

1) The input control module

The 802.1x authentication module needs to convert the timing of received messages to its own timing, and then send messages to the switch authentication module and the user authentication messages conversion module for processing. So it is necessary to design the input control module so as to avoid messages being discarded.

2) The switch authentication module

The switch authentication module proposes the switch authentication request to the server, and judges whether the authentication is successful according to the response message from the server. If this process succeeds, the switch authentication is over. The user authentication module starts to trigger the transformation of the user authentication messages. If the server has not responded in a certain period of time, send the request message again.

3) The user authentication messages conversion module

This module judges the received messages' protocol. Then convert the EAPOL message from the client to the RADIUS message which can be distinguished by the server. And convert the RADIUS message from the server to the EAPOL message which can be distinguished by the client.

4) The arbitration and send module

Before the switch authentication is completed, this module sends the switch authentication messages only. When the switch authentication is completed, send the user authentication messages and judge whether there is a complete message in the register. If there is, this module reads the message from the packet cache, and sends it according to the timing sequence.

The design flow chart of 802.1x authentication module is shown in Fig.4.

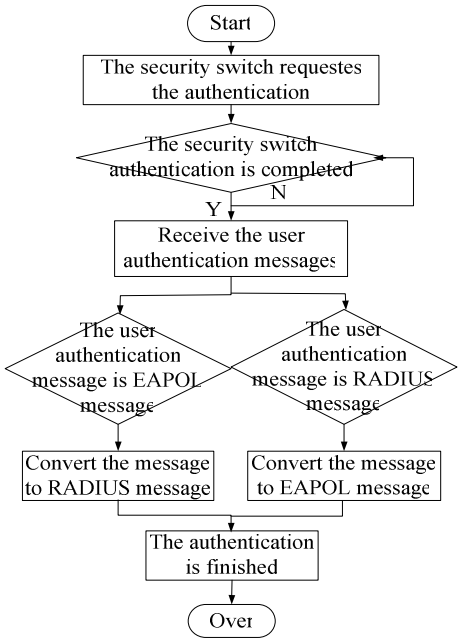

Figure 4. Flow chart of 802.1x authentication module design

III. Simulation Results of FPGA Realization

Fig.5 is the modelsim simulation figure of the security switch authentication. Among them clk_125 is 125 M clock. Rst_n is reset signal. Switch_MAC is the MAC address of the security switch. Switch_ip is the IP address of the security switch. Auth_success is the authentication complete signal of the security switch.

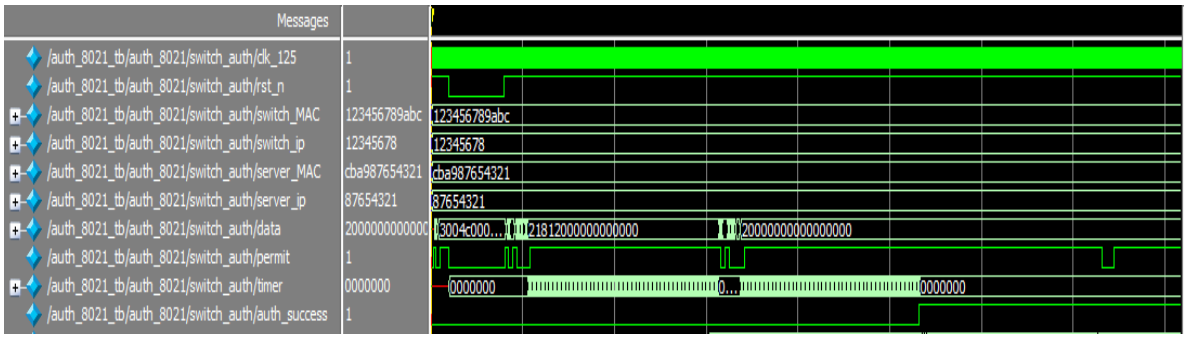

Figure 5. Modelsim simulation figure of the security switch authentication

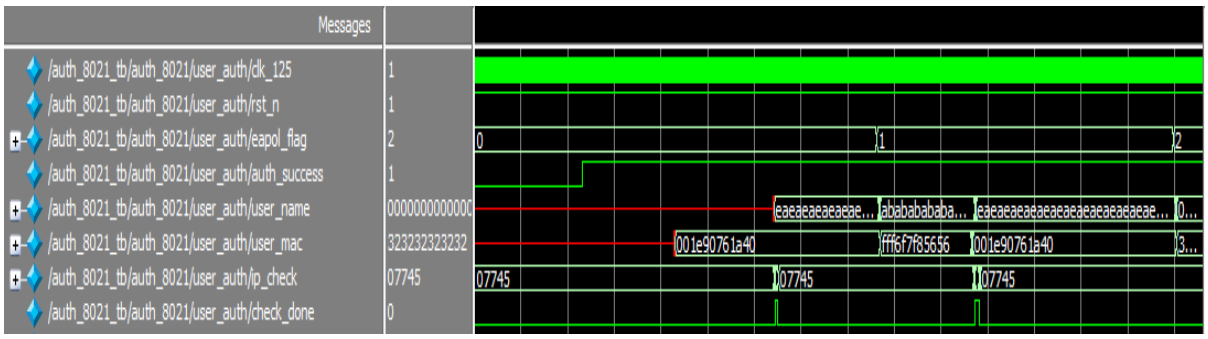

Figure 6. Modelsim simulation diagram of the client authentication

Fig.6 is the Modelsim simulation diagram of the client authentication. Among them clk_125 is 125 M clock. Rst_n is reset signal. Eapol_flag is to judge the message type is EAPOL or RADIUS. Auth_success is the authentication complete signal of the security switch. User_name is user name. User_mac is the client MAC address. Ip_check is the authentication for IP address. Check_done is the authentication complete signal.

The figures show that the dual authentication model proposed in this paper has been effectively realized. The 802.1x authentication module realizes the authentication between the security switch and the server and the authentication between the client and the server. The design ensures the security switch network's security and the user identity effectively and improves the security switch's security of the industrial control system.

IV. CONCLUSION

This paper discusses the importance of 802.1x authentication module in industry control system, and analyzes the protocol mechanism. This paper proposes a dual authentication model: the authentication between the security switch and the server and the authentication between the client and the server. The design process of the proposed authentication module is also introduced in this paper. This work has been realized in an FGPA chip of Altera company. The security switches realize the control the identity of the switches in the network and the control of the users' identity, ensuring the security of the industrial control system.

ACKNOWLEDGMENT

We would like to thank our respected teachers and colleagues for their guidance and support. At the same time we'd like to thank the rigorous learning style of Zhejiang University. And we are also thankful to SUPCON company for providing us the facility and research environment.

REFERENCES

[1] Xiaobo Han, "Discussion and Implementation of Networks Security Technology for Industrial Control in Enterprisesj," Control and Instruments in Chemical Industry, vol.39(4), pp. 498-503, 2012.

[2] DU Wei-qi, WANG Ping, WANG Hao, "Security threat analysis and strategy in industrial control system," Journal of Chongqing University of Posts and Telecommunications(Natural Science),vol. 17, pp. 594-598, 2005.

[3] IEEE 802.1x,Standards for Local and Metropolitan Area Networks: Prot-Based Access Control[S]. 2001.

[4] LUO Han-yun, SONG Yong, "802.1x Authentication Technology Analyse," Journal of Anqing Teachers College(Natural Science), vol. 15, pp. 52-54, 2009.

[5] Edwin Lyle Brown.802.1x Port-based Authentication[M]. New York : Auerbach Publications. 2006.

[6] BAI wan-jian, LIU bing, "Research and implementation of 802.1x authentication in LAN," Computer System & Applications, issue. 7, pp.71-74, 2006.

[7] XIA yu-wen, Verilog digital system design tutorial. Beihang University Press, 2009.