A Design and Implementation Method of IPSec Security Chip for Power Distribution Network System Based on National Cryptographic Algorithms

Wei Xi[1], Siliang Suo[1], Tiantian Cai[1], Ganyang Jian[1], Hao Yao[1], Lin Fan[2,3]

1. Electric Power Research Institute, CSG. , Guangdong, 510663,China

2.State Grid Key Laboratory of Power Industrial Chip Design and Analysis Technology, Beijing Smart-Chip Microelectronics Technology Co.,Ltd.Beijing 100192,China

3.Beijing Engineering Research Center of High-reliability IC with Power Industrial Grade, Beijing Smart-Chip Microelectronics Technology Co.,Ltd.Beijing 100192,China

xiwei@csg.cn, suosl@csg.cn, caitt@csg.cn, jiangy@csg.cn, yaohao@csg.cn, fanlin1224@163.com

Abstract*—The target of security protection of the power distribution automation system (the distribution system for short) is to ensure the security of communication between the distribution terminal (terminal for short) and the distribution master station (master system for short). The encryption and authentication gateway (VPN gateway for short) for distribution system enhances the network layer communication security between the terminal and the VPN gateway. The distribution application layer encryption authentication device (master cipher machine for short) ensures the confidentiality and integrity of data transmission in application layer, and realizes the identity authentication between the master station and the terminal. All these measures are used to prevent malicious damage and attack to the master system by forging terminal identity, replay attack and other illegal operations, in order to prevent the resulting distribution network system accidents. Based on the security protection scheme of the power distribution automation system, this paper carries out the development of multi-chip encapsulation, develops IPSec Protocols software within the security chip, and realizes dual encryption and authentication function in IP layer and application layer supporting the national cryptographic algorithm.

***Keywords*—the power distribution automation system; network security; national cryptographic algorithm; sercurity chip; IPSec protocol**

I. INTRODUCTION

IPSec VPN technology has been widely used in electric power system, which based on national cryptographic algorithm is generally used in the distribution system to realize the "IP layer" security protection between the master station and the terminal. At present, the terminal side adopts the module or device of plug-in mode to realize the "IP layer" data security protection. Once the plug-in device is abnormal, the service data of distribution system is either blocked or transmitted in plaintext, and the "application layer" security protection of distribution system can't be guaranteed. In this paper, the security chip is used to realize the IPSec security protection of the terminal. The chip is directly welded on the terminal hardware, which has the advantages of lightweight, miniaturization, low cost, low power consumption and easy maintenance.

II. DESIGN AND IMPLEMENTATION OF SECURITY CHIP

A. The Composition Structure of Distribution Network Automation System

The target of security protection of the distribution system is to ensure the security of communication between the terminal and the master system. The VPN gateway for distribution system enhances the network layer communication security between the terminal and the VPN gateway. The master cipher machine ensures the confidentiality and integrity of data transmission in application layer, and realizes the identity authentication between the master station and the terminal. As shown in Fig.1, the structural diagram of security protection for the distribution system.

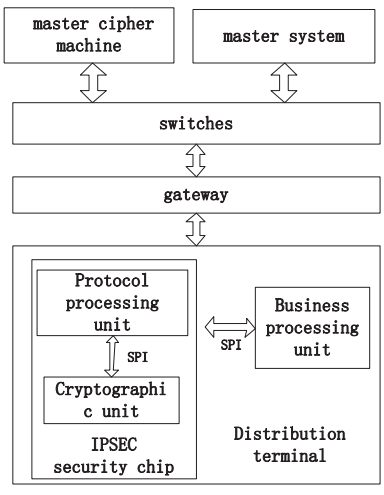

Fig. 1 the structural diagram of security protection for the distribution system

All these measures are used to prevent malicious damage and attack to the master system by forging terminal identity, replay attack and other illegal operations, in order to prevent the distribution system accidents.

B. The composition architecture of IPSec security chip

The IPSec security chip is an important part of security protection of the distribution automation system which is composed of the protocol processing unit and the cryptographic operation unit. The chip provides SPI interface and MAC interface for data interaction. The protocol processing unit is responsible for IPSec protocol processing and internal task scheduling of the security chip. The cryptographic operation unit is responsible for cryptographic operation services of protocol layer and application layer, and realizes the functions of national cryptographic algorithm SM1/SM2/SM3/SM4, certificate parsing, key storage and management. The IPSec security chip connects with the business processing unit through SPI interface to realize business processing with terminal, which includes calling cryptographic operation unit to perform cryptographic operation, configuring network parameters for IPSec security chip, and forwarding network data through IPSec security chip.

C. Protocol implementation principle of the IPSec security chip

The paper designs and implements IPSec protocol on security chip refers to <<GM-T 0022-2014_IPSec VPN Technical Specification>>. The cryptographic algorithm uses symmetric, asymmetric, hash and random number generation algorithms. The IKE process negotiation and the ESP data encapsulation process are implemented by using embedded real-time operating system rt-thread, open source protocol stack LWIP. The data processing flow of the IPSec security chip is shown in Figure 2. The chip implements LwIP (light weight IP) and IPSec protocol stack, adds IPSec processing layer between IP layer and physical layer of the original TCP/IP protocol stack four-layer network model, and processes incoming and outgoing IP layer data packets.

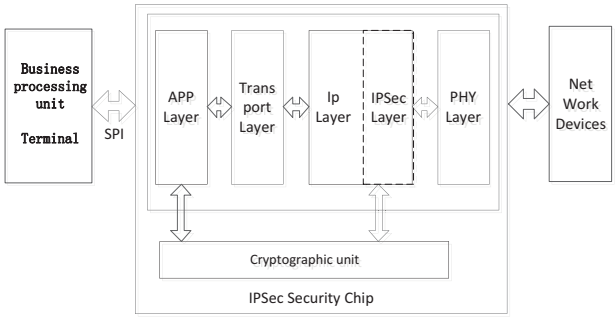

Fig.2 The data processing flow of the IPSec security chip

The IPSec procotol provides a complete set of security services based on cryptography for IP, including access control, data source verification, anti-replay attack, etc. It provides protection for IP and upper protocols. IPSec defines IKE (Internet key exchange) protocol for key distribution and SA management in automatic mode. The process of key distribution and SA (Security Association) management in IKE is divided into two stages. The first stage is to establish a trusted and secure channel between the two parties to protect the second stage key negotiation process. The second stage completes the negotiation actually used in IPSec SA, and determines the security policy of both sides and the session key. The IKE negotiation protects data exchanging by calling cryptographic units in application layer, and the ESP data transmission process through the IP layer by calling cryptographic unit. The Device key (signature key pair and encryption key pair) and certificate are stored in cryptographic operation unit

D. Security Business Processing Flow

IPSec security chip supports the dual security protection in IP layer and application layer .The security business processing Flow as shown in Fig.3.

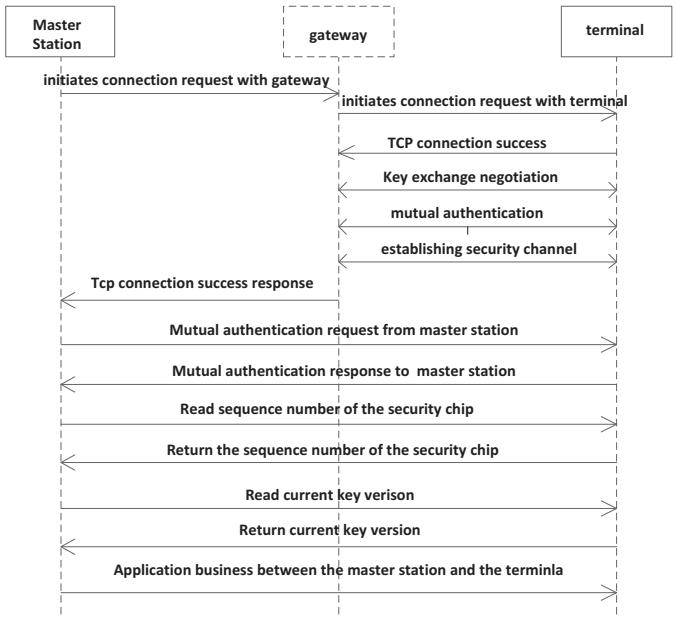

Fig.3 Security Business Processing Flow

(1) The master station initiates a connection request to the gateway and requests a connection with the terminal;

(2) The gateway initiates a connection with the terminal;

(3) After successful TCP connection, key exchange and negotiation between the gateway and the terminal;

(4) Mutual authentication between gateway and terminal based on digital certificate technology;

(5) when the Mutual authentication between gateway and terminal is passed, the two sides establish a security channel;

(6) The master station initiates mutual authentication with the terminal;

(7) After successful authentication, the master station reads the sequence number and key version of the security chip in the terminal;

(8) Then Application business between the master station and the terminal start transmission.

E. Data Processing Flow of the IPSec Layer

In this design, the security policy database SPD and the security association database SAD are constructed, and the corresponding IP and port are configured to set up the whitelist of the access devices, while the negotiated SAD is maintained. The IPSec security chip has two working modes: APPLY and BYPASS. When selecting PYPASS mode, the chip only serves as a security chip to realize mutual authentication and application business protection between the terminal and the master station. When choosing APPLY mode, it can also realize identity authentication between the terminal and the encryption authentication gateway data encryption protection in IP layer.

The inbound data processing flow is as shown in Fig 4.

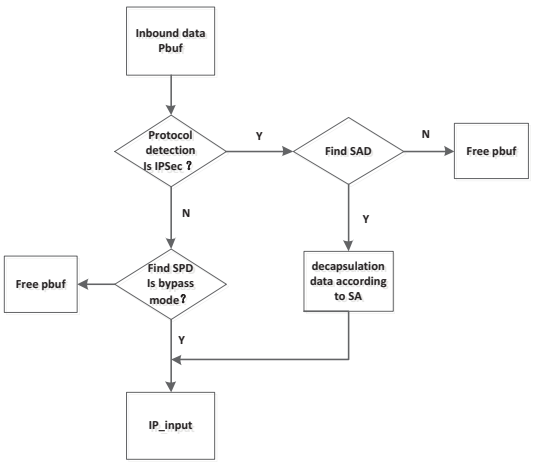

Fig.4 inbound data processing

(1) When the physical layer receives the Ethernet data frame, forwards the frame to the IPSec layer after removing the Ethernet header, and judges the protocol type according to the IP header;

(2) The IPSec packet is detected in the SAD library to find the corresponding SA. According to the corresponding SA, the IP packet is unpackaged and replay-resistant. After confirming that the data is correct, the original IP packet is transferred to the ip_input;

(3) While the Non-IPSec packages , search the SPD library to determine the mode , with the bypass mode sends data to ip_input, otherwise, pbuf is released.

The outbound data processing flow is as shown in Fig 5.

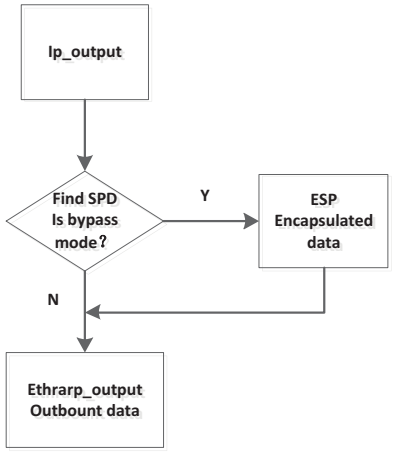

Fig.5 outbound data processing

(1) 1Obtain the ip_output data packet and find the working mode of the data packet through the SPD Library;

(2) Bypass mode IP packets are forwarded to etharp_output;

(3) In application mode, the original IP packet is encapsulated and forwarded to etharp_output with a new IP header.

III. SAFETY ANALYSIS

The IPSec security chip is implemented by BGA package, which includes the control chip, the security chip and the switch circuit. The control chip and security chip are two different chips, so they have less physical coupling and stronger anti-interference ability. The IPSec security chip supporting national cryptographic algorithm is adopted to realize identity authentication and data encryption between the terminal, the gateway, and the master station.

The paper adopts an IPSec security chip to realize the terminal side security protection. The chip is directly welded on the terminal hardware, which has the advantages of lightweight, miniaturization, low cost, low power consumption and easy maintenance. The IPSec security chip has both protocol processing unit and cryptographic operation unit. The IPSec security chip based on national cryptographic algorithm is designed and implemented by Reference to the IPSec VPN technical specification. By cooperating with cipher management system, double encryption technology based on "network layer & application layer" is realized. The gateway for distribution system enhances the network layer communication security between the terminal and the gateway.

The master cipher machine ensures the confidentiality and integrity of data transmission in application layer, and realizes the identity authentication between the master station and the terminal. All these measures are used to prevent malicious damage and attack to the master system by forging terminal identity, replay attack and other illegal operations.

REFERENCES

[1] Sun Weifeng, Zhang Lin, Lin Shaofeng. et al. A design and and implementation of an enhanced VPN security isolation gateway[J] Journal of China Academy of Electronics and Information Technology, 2015,06:628-631+651.

[2] Zhang Qing. Systematic analysis of network security isolation and information exchange technology[J]. Network Security Technology & Application 2014,04:77-78.

[3] Li Xuan, Wu Qicong. Research on Application of digital signature and encryption in network isolation[J]. Netinfo Security,2013,10: 178-180.

[4] Application Research of data security encryption technology in computer network security Network Security[J].Technology & Application,2018,02: 45-46.

[5] Xiao Nan, Dai Zibin, Wu Zaihe et al. Design of security transmission system for the internet. Innovation Management&Industrial Engineering . 2012

[6] Shanshan Liu,Peng Wang,Lei Luo et al. Security Module in Information Unilateral Transmission System among Networks[J] . AASRI Procedia . 2012.

[7] 《GM/Z 0001-2013 Definition of cipher terminology》

[8] 《GM/T 0002-2012 SM4 block cipher algorithm》

[9] 《GM/T 0003-2012 SM2 elliptic curve cryptography algorithm》

[10] 《GM/T 0004-2012 SM3 cipher hash algorithm》

[11] 《GM/T 0005-2012 Randomicity testing specification》

[12] 《GM/T 0006-2012 Code application identifier specification》

[13] 《GM/T 0022-2014 Code application identifier specification》