Advances in Engineering Research, volume 127
3rd International Conference on Electrical, Automation and Mechanical Engineering (EAME 2018)

# Research on Safety Communication Technology between Expressway Front-end Equipment and Background Based on PSAM Technology and Private Communication Protocol

Zhanbin Wang[1], Jie Wu[1,2,*], Haibo Zhang[1] and Yi Xu[1]
[1]The Third Research Institute of The Ministry of Public, Security of P. R. C., Bisheng Road 339, Shanghai, China, 201204
[2]East China Normal University, Shanghai, China, 200062
[*]Corresponding author

***Abstract*—When wireless communication technology is applied between Front-end Equipment and Background on expressway, the security is always an important point to be considered. The paper put forward a kind of reliable communication with the PSAM Technology and private communication protocol. The PSAM technology is used to encrypt the plain text. The private communication is formulated to achieve a high reliability of communication mode based on 4G transmission equipment. In the end, the experiment was conducted to demonstrate its feasibility and really high security.**

***Keywords—expressway communication; pivate protocol; session layer; PSAM***

## I. INTRODUCTION

Currently in a variety of wireless communication based technologies, 4G technology is constantly favored for its high signal coverage and high transfer rate. Through the 4G network system, the Internet communication standards and server can be used for the device to exchange data, achieved the connection with international Internet connections [1]. Traditional industry requirements for communication and data exchange has been changed from a fixed, time-limited mode into a mode without geographical, no time constraints. The wireless access network is used to replace wired way has become an inevitable trend. With the TCP/IP network protocol, 4G technology provides a link between the mobile user and the data network; the mobile users can enjoy the high speed wireless IP and X.25 services. 4G communication obtains the characteristics of always online, expenses is calculated by flow, flexible networking, and easy maintenance. Without changing the user's original network architecture, networking costs and operating costs can be significant saved [2]. Although 4G accesses greatly extend the space-time domain of office automation, the security issues of private networks connecting with wireless internet are also becoming increasingly prominent [3].

Traditional wired communication technologies on highway usually use data encryption and other methods to ensure communication security. Although these methods are still feasible in wireless communication, none of them fully compensates for the security gap caused by the openness of wireless channels [4]. Public security areas are related to the use of sensitive and transmission of classified information, which requires high-security communication means, considering the complexity of terrain in the police field and the instability of wireless networks in those areas. 4G communication has been widely used as a communication mean. However, as a public transmission route, 4G itself is not a reliable method for secure transmission. Many papers describe the reliability design of 4G, but when it comes to security on highway, especially in the field of public security, the discussion is very limited.

The main design idea of the 4G-based trusted system designed in this paper is to increase the communication protection of the session layer according to the ISO seven-layer network protocol. The private communication is formulated in the session layer to achieve a high reliability of communication. The implement is divided into hardware design and software design. The hardware part uses the ARM chip with the Contex-M4 series as its core. Software is divided into three parts, embedded COS software, data communication background and device management background, the main session layer protocol is implemented in embedded software. This design has the characteristics like simple on-site installation, convenient use of engineering personnel, and stability of the device, etc. At the same time, it also proves that the system can achieve high-confidence data transmission of 4G through a large number of experiments and use.

## II. METHODOLGOY

### *A. The Session Layer and PSAM Technology*

In the system reliability design, this paper uses the ISO standard seven-layer protocol architecture [5], as shown in Figure I. During the communication between the for-end device and the background, the strategy is needed to achieve a trusted session layer transmission, in particular at the physical layer using a data link communication, the network layer using the TCP / IP communication protocol, session layer implements data encryption while both ends of the session

layer implements authentication data terminal device, which in addition to the original Ethernet protocol layers comprising the original header information, further encapsulating layer This layer includes an encrypted ID information used as a session layer communication and device authentication and is compatible with the upper layer.

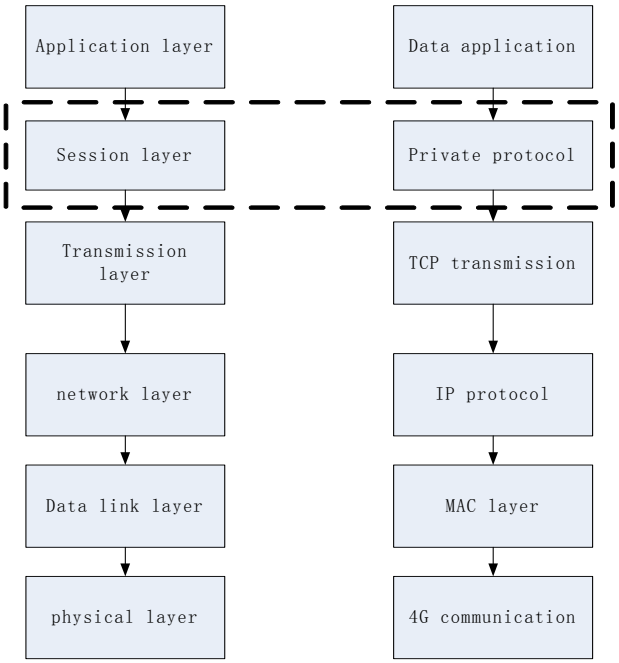


FIGURE I. DIAGRAM OF ISO STANDARD SEVEN-LAYER PROTOCOL

Device authentication is interactive through cipher text. The authenticated device has an encrypted device ID. When the authentication starts, the device connects to the platform and sends an authentication command, which includes the cipher-text obtained by encrypting the device ID number in the PSAM chip. When the platform receives the authentication application, the platform decrypts the device ID and sends it to the database for comparison. If the ID number is already authorized, the authentication succeeds. Otherwise, the system will take the initiative to disconnect the device up, , and recording to the wrong ID number and hardware serial number to ensure that the same number cannot be authenticated more than three times per day.

### *B. Private Transmission Protocol*

The security of information flow is guaranteed in two places. As shown in Figure II, The first one is PSAM encryption and authentication to ensure the effective information will not be intercepted and illegal decrypted during the collection and transmission [7]. The second one is after the device turned on, it will send the running parameters to the background and after receiving the operating parameters, the background will start ID authentication, the process is shown in Figure III. If the authentication succeeds, it means that the device is a legitimate device. If the authentication fails, it is considered to be an illegally accessed device.

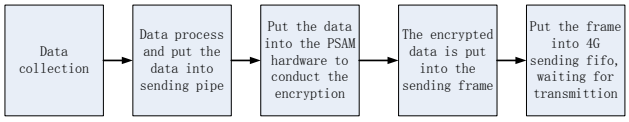


FIGURE II. THE TRANSMISSION PROCESS

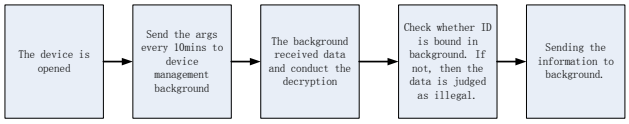


FIGURE III. THE CERTIFICATION PROCESS

The protocol between the device and device management background consists of a short TCP connection. The server sends one CLOSE byte to the client protocol. This byte is used to send the information to the device whether there are other bytes need to be transmitted. If not, CLOSE=0. After the device receives the CLOSE byte instruction, it will actively send the FIN signal and close the network connection. The Table I and Table II show the uplink communication protocol and downstream communication protocol especially.

TABLE I. THE UPLINK COMMNUCATION PROTOCOL

| Frame head | CMD | Frame length | Frame data | SUM |
|---|---|---|---|---|
| 0xEE | 0x01 | 2bytes | N bytes | 1 bytes |

TABLE II. THE DOWNSTREAM COMMNUCATION PROTOCOL

| Frame head | CMD | Frame length | Frame data | CLOSE | SUM |
|---|---|---|---|---|---|
| 0xEE | 0x01 | 2bytes | N bytes | 1 bytes | 1 bytes |

## III. HARDWARE IMPLEMENTS FOR SYSTEM

This system uses STM32F407 as the processor, uses the FreeRTOS operating system, communication means is a wireless network communication using the SIM900A GSM communication module. The personnel and license plate information sent by the active RFID are processed and encrypted then sent to the rear platform according to the agreement for monitoring the real-time flow conditions of people and vehicles in a certain area. Figure IV shows the hardware system block diagram of this system. The core is STM32F407, including its supported NAND FLASH and external SRAM. PSAM (purchase secure access module) support is composed of two parts, using the PSAM driver chip M505A. Use serial port and core module communication, support 115200 baud, 38400 baud two kinds of baud rate, use two PSAM slots, use as master and backup PSAM card. 4G communication adopts ME909s-821 module to realize communication through serial port. The whole system is shown in Figure V.

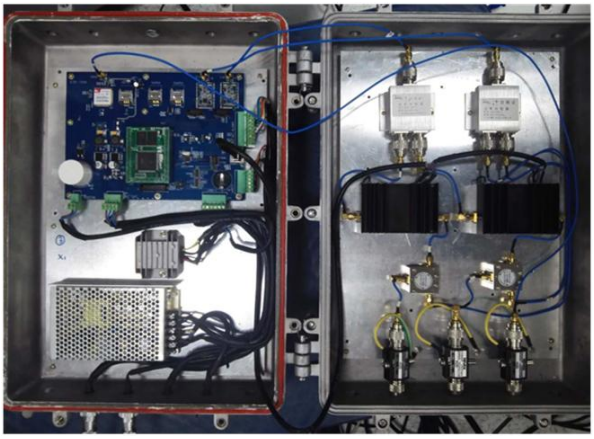

FIGURE IV. THE PHOTO OF DESIGNED HARDWARE

The SAM card is generally installed on a smart card terminal device as a security control of the smart card terminal to achieve the legality authentication between the terminal and the card [6]. For civil servants, different keys should be granted at any time, for they can register into the system, bind the hardware SN number of the device and the different key to be granted at any time. After the task is executed, the device and key are recycled. This process ensures the security of device communication at different times. The public security internal platform agreement which is customized and personalized depending on each region's public security system platform, this requires that when the mission is performed, it must be ensured that the message can only be known by the person in the execution group without being leaked out, therefore, the PSAM key card is allocated before execution to ensure the reliability of the message and the security of the task.

FIGURE V. THE PHOTO OF DESIGNED SYSTEM

## IV. SOFTWARE IMPLEMENTS FOR SYSTEM

### A. *Front-End Software Implement*

Five parallel threads are designed in the system after the system is powered on, hardware initialization and network interface initialization are performed first, and the next step is self-checking system. If the self-checking system passes, five threads will run separately after reading the system configuration. The five threads are thread data acquisition and processing, the data transmission to the information management background thread, the data transmission to the device management background thread, local setting thread, and the last is device monitoring, which can monitor the operating status of each device component in real time.

### B. *Background Software Implement*

The server used to transmit the device-specific monitoring platform protocol is placed in the research institute ministry of public Security. The browsing mode can have two modes, an engineer browsing mode and a device buyer browsing mode, which can facilitate system maintenance, while monitoring whether the monitoring system has been threatened by security threats such as movement, destruction, or vibration, or whether subjected to illegal device access, etc.

After the device starts working, it will connect to the dedicated monitoring background IP address and port number, which is already preset. When the connection is success, the device will send an authentication command to the background, if the system passes the device authentication, it will send an authentication return and begin to send parameter status. Otherwise, it will send an unsuccessful reply and disconnect the connection. Device management background mainly consists of the background processing protocol and web display, wherein the device management algorithm is divided into three main functions, the first is to receive various status parameters of the remotely transmitted device, as well as software and hardware version numbers, and displays the page above. This algorithm can notify relevant person at any time when abnormal conditions occur in the parameters; the second is to remotely set the threshold for each device, restart the system, and change the system SN number, etc.; the third is the device remote system update, remote system maintenance, avoid relevant person to go to the local area to perform program maintenance.

The different users can be implemented with different functions. For example, the program can be upgraded remotely through the background for the device providers. However, this function is not open to the device user. As for the threshold setting, IP setting and other functions, they are not open to the device provider but open to the device user. Through these functions, corresponding users can set the device remotely. Equipment and background use TCP short connection to communicate. The advantage of this communication is that the device does not need to maintain connection with the background, which can minimize the occupation of system resources. When the number of devices that connect to the background is increasing, the background can also effectively manage the devices, and the load will not increase too much.

## V. CONCLUSIONS

This article mainly describes two kinds of high-security communication methods used in the public security application to prevent leakage and illegal device invasion when using 4G communication devices. The two methods are PSAM encryption, private protocol implement on the session layer. The two methods ensure the high reliability of the implementation and increase the credibility of the system

communication process. The proposed method is applied in the intelligent terminal and has significantly improved the system security. It further verifies the realization of this method with no significant increase in system cost.

## REFERENCES

[1] Sun Zhongfu, Cao Hongtai,Li Hongliang, et al. 4G and Web based data acquisition system for greenhouse environment[J].

[2] REGID,J. General wireless grouping service (4G) technology and application[M]. ZHU Hongbo,SHEN Yuehong,CAI Yueming, et al. Beijing: The People's Posts and Telecommunications Press,2002.

[3] Tang Danl Kuang Xiaohong A 4G ACCESS SYSTEM AND ITS SECURITY SOLUTION, 2010:133-136)

[4] MU Pengcheng, YIN Qinye, WANG Wenjie A Security Method of Physical Layer Transmission Using Random Antenna Arrays in Wireless Communication LU Shiwen. Computer network protocols and implementation technology [M]. Beijing: tsinghua university press, 2000:30-31

[5] SHAO Jianping. Smart card developer guide [M]. Beijing: electronic industry press, 2000:25-29

[6] YANG Yixian. Smart card security and application: second edition [M]. Beijing: people's posts and telecommunications publishing house, 2002:10-13.