Design of remote security control system based on 4G

Xiao Liu¹,*, Guozhen Shi¹, Jinpo Fan²

¹Department of Computer Science and Technology, Beijing Electronic Science and Technology Institute, Beijing, China
²Department of Electronics and communication engineering, Beijing Electronic Science and Technology Institute, Beijing, China

*Corresponding author e-mail: 3408355302@qq.com

Abstract. With the rise of the concept of "smart earth", the new generation of information technology has changed the way information interacts. The combination of things, intelligence and interconnection has made people's daily life more convenient. However, while enjoying convenience, information security has become a bottleneck restricting comprehensive interconnection. A variety of devices can be remotely controlled through public networks and sensor networks, but a large number of facts show that in an open network environment, information is easily stolen and tampered, and the resulting security problems are becoming more serious. The 4G (the 4 Generation mobile communication technology) remote security control system implemented in this paper consists of a main controller, a cloud server and an Android client. The information of the main controller and the client is encrypted by the national secret algorithms SM2 and SM4, the information exchange is performed by the cloud server, and the main controller establishes a connection with the terminal device through the short-range wireless network. Compared with the remote control system that usually uses international algorithms, this system has advantages in terms of ensuring the security and control on the basis of satisfying convenience and intelligence.

1. Introduction

Application scenarios such as smart home, intelligent transportation, and smart city all involve remote security control issues. At the end of 2016, the Mari botnet attacked the domain name service provider Dyn with a maximum of 620G of DDoS traffic, resulting in a large number of websites being inaccessible. At the end of 2017, the “small droplets” video live event caused people to worry about the security of the terminal equipment. Configuration and security vulnerabilities are hidden dangers of information security problems, but fundamentally, because the information is not cipher protected during transmission, the attacker obtains remote control rights of the device and this has led to a series of security threats and privacy leaks.

The development of communication technology has brought more convenient and high-quality network access experience. Compared with traditional networks, 4G adapts to mobile data communication, its speed is faster, network spectrum is wider, and communication billing More economical, able to meet high-quality multimedia communication needs. The wide application of 4G technology makes the communication terminal equipment more intelligent, which is characterized by
higher speed computing power, lower power consumption chip integration and more friendly human-machine interface. The high-speed and stable mobile network and intelligent terminal enable users to use a abundant application for data interaction. At the same time, applications with dedicated functions can be developed based on different operating systems.

The cloud is a concentrated expression of information technology development and service model innovation. In the era of the Internet of Everything, with the cloud platform, data sharing between enterprises, users and governments has become more convenient. The cloud can meet the computing power requirements and flexibility of digital services. Through dynamic resource allocation, it saves a lot of repetitive construction costs and avoids the risk of data loss. But the cloud is also facing the security problems and the resulting risk of privacy breaches. According to Gartner, by 2022, at least 95% of cloud security failures will become an important issue for enterprises and organizations to consider. [1]

In order to solve the security problem on the cloud, a feasible solution is to protect the cloud data through cryptography. In the context of autonomous and controllable information security, the use of international algorithms for data protection increases the risk of data breaches and information systems being attacked. With the national secret algorithm combined with the Internet of Things cloud platform, a relatively complete data security mechanism can be established to effectively prevent users from leaking private data. In this paper, we use remote control for wireless sensor networks, and propose a new remote control system design that uses national secret algorithm to protect communication security. The system can provide an effective solution to the security problems that constrain the development of the Internet of Things.

2. System structure

![Figure1 Schematic diagram of the system architecture](image)

The 4G-based remote security control system consists of a client, a cloud server and a main controller on the mobile phone. The information exchange between the mobile terminal and the terminal device needs to be performed by the 4G network and the main controller. The cloud server is equivalent to the transfer of data transfer. The data is separated from the mobile terminal and the host controller, but the encryption is only for control signaling or Device status data does not encrypt the device name, which makes it easier to query data from the database. The main controller sends the device status to the cloud server every 300 ms. If the device is abnormal, the alarm is sent through the short message module while updating the status. The main controller sends an encrypted control command to the cloud server user on the client, and transmits the data to the cloud server through the 4G network. The cloud server interacts with the main controller to perform remote security control on the device, and at the same time, different terminal devices pass the wireless sensor network. The device status is sent back to the main controller, and the main controller encrypts and uploads it to the cloud server to implement remote and secure information interaction.
Figure 2: Architecture design of the main controller

The main controller uses the embedded system platform and adopts an open system architecture and module design to uniformly encrypt and transmit information exchanges of different devices. The overall architecture of the main controller is shown in the figure. The system is divided into three levels: functional layer, component layer and network layer.

In the functional layer, the design selects four functions of control command, status transfer, encryption and decryption service and device alarm. The information exchange between the main controller and the cloud needs to be performed through the encryption and decryption service, so that the data is transmitted in a dense state in the common channel and the cloud server. On the basis of the encryption and decryption function, the local data communication method is not changed. The control command function receives the setting state of the cloud and controls the local terminal device. The status transfer function displays the current working status of the device and encrypts the status information and transmits it to the cloud. The alarm function is used to send an alarm message to the user through SMS or dial-up when the device is abnormal.

The main controller mainly includes two types of modules, one of which is a 4G module, which can be connected and communicated with a public network, and further includes a short message module for sending an alarm message to a preset number when a device abnormal condition occurs; It is a wireless sensor module, including but not limited to Bluetooth, infrared, ZigBee modules, for implementing data communication in a wireless sensor network.

3. Cryptographic module design

In the design of the remote security control system, the security of the data is mainly guaranteed by the security of the key. The security of the key is reflected in the generation, distribution and storage of the key. Destroy various stages of the life cycle. The distribution of the key is to transfer the key to the authorized entity in a secure manner, which can be done in a digital envelope. Digital envelope technology combines asymmetric encryption with symmetric encryption to provide secure delivery of session keys. However, the cryptographic algorithm used is generally an international cryptographic algorithm, which increases the risk of information leakage and system attack. Therefore, a national secret algorithm module is designed for the security protection of communication data. The process of transmitting information using the national secret algorithm is as follows:

Figure 3: Flow chart of secure information transmission using national secret algorithm

The design of the cryptographic module in Figure 3 includes the design of the asymmetric algorithm SM2[2] and the design of the symmetric algorithm SM4. The message is encrypted with the session
key using the SM4 algorithm, and the session key is encrypted with the recipient public key using the SM2 algorithm, and the encrypted message is sent together with the session key. After receiving the information, the receiver uses the SM2 algorithm to decrypt the session key with its own private key, and then decrypts the received message with the session key.

4. Software design

4.1 Introduction to the Android platform

Android is an open source operating system based on Linux. It is mainly used for mobile devices and is continuously developed and led by Google and the Open Handheld Alliance [3]. It uses a software stack (aka software stack) architecture, which is divided into three parts. The underlying layer is based on the work of the Linux kernel and provides only basic functionality. Other applications are developed by each company and are part of the programming process in Java. The kernel of the Android system belongs to a branch of the Linux system kernel, with typical Linux features and functions. In addition, Google has modified and customized Android to make it work well on mobile devices. The advantage of Android is that the system is open source, so that more hardware manufacturers and developers can invest in it and continue to promote its growth. On the other hand, the ecosystem disorder caused by open source has also caused the system to be mixed, resulting in many problems in compatibility.

Its main features include: (1) openness. Through in-depth cooperation with operators, equipment manufacturers and other related parties, Google takes the open source Android system as the core and builds a standard and open mobile software platform to form an open ecosystem within the industry. (2) Application interoperability. Applications installed on Android devices can access the system features of the device using the interfaces provided by the system. Applications can use configuration files to indicate that their functionality can be opened to other applications. (3) Unrestricted developers. Due to the compatibility of the Android system, the selectivity of the hardware platform is also a lot richer. In addition, based on the open principle of the Android operating platform, many hardware manufacturers are gradually getting rid of the shackles of hardware devices, and also made a lot of breakthroughs in the innovation research of many developers, and then designed a lot of innovative application software.

4.2 Functional module design

![Android software design of remote control system](image)

The remote control system software not only enables secure remote control but also the current and historical status of the device. In order to facilitate the user's use, the intuitive and convenient operation interface is designed, and the status check and log query are realized through timely data update. Figure4 is the components of the Android terminal of the remote control system. It can be seen from Fig. 4 that the remote control system consists of five parts: information storage module, data
encryption and decryption module, data display module, human-machine interface module and equipment management module.

(1) Data storage module
The various device operating parameters obtained need to be stored in the database for querying and for other functions.

(2) Data encryption and decryption module
When the user logs in successfully, the control terminal starts to receive the data transmitted from the server, and saves it to the corresponding file buffer, and then the data encryption and decryption module decrypts the data in the buffer.

(3) Data display module
Users can view and control devices in real time through the cloud platform, and the system is based.

(4) Human machine interface module
The Android client uses different interfaces for data transfer and command requests to facilitate database storage and query. Users do not need to know the underlying communication commands, just click the button to complete the acquisition of device status and the transmission of control signaling.

(5) Device Management Module
The appliances and sensors in the user's home are constantly changing in actual operation. The system should support this dynamic change and make modifications according to the content of different rights.

4.3 Cloud Server Design
Cloud storage is a new type of storage service. Service providers provide storage capacity and data storage services to customers through the network. At the same time, customers do not know the specific implementation details and underlying mechanisms. Compared with traditional storage devices, cloud storage is more than just a piece of hardware, but a complex system consisting of multiple parts such as network devices, storage devices, servers, application software, public access interfaces, access networks, and client programs. Each part takes the storage device as the core and provides data storage and service access services through application software [4]. All devices in the cloud storage system are completely transparent to the user, and the user only needs to connect to the cloud through the network to access the data. Users who need storage services no longer need to set up their own data centers, only need to apply for storage services to SSP (storage service provider), which saves expensive software and hardware infrastructure investment. Compared with the traditional data centralized storage solution, the efficient clustered cloud storage system has the advantages of easy expansion (including bandwidth), lower cost, more secure data, and uninterrupted service. The cloud server of this system is designed with PHP and MYSQL language. It mainly handles connection requests initiated by the Android terminal and the main controller, and extracts information and stores data.

5. Main controller design
The wireless aggregation-4G main controller is designed as follows: the main controller ARM is connected to the 4G module, and the DC power supply provides the 9V-1A power output, which is respectively connected to the PWR and GND of the UNV-SIM7600CE module, and the ARM serial port and the UNV-SIM7600CE module. The TTL level serial port is connected, and the controller sends an AT command to the UNV-SIM7600CE module through the serial port to perform operations such as sending short messages and network data transmission, and the main controller waits for the 4G module to respond, and when receiving the short message or receiving the network data, the completion is completed. The corresponding control operation. The system hardware connections are as shown.
5.1 Introduction to ARM

The embedded system is a tailored real-time Linux system, which has the advantages of small space, reliability, low power consumption, strong specificity and high real-time performance [5], which makes it have a wide range of vitality. By estimating the utilization of the solution resources, the AM335x-based development board is selected. The AM335x is based on the ARM Cortex-A8 processor and its speed ranges from 600MHz to over 1GHz, meeting the requirements of most low-power devices.

The AM335x used in this article is the core development board. The hardware size is much smaller than that of the PC. By cutting and modifying the kernel, many unnecessary modules are removed, and some necessary driver support is retained. The operating system is changed from a general-purpose Linux system to a real-time operating system, which saves space, improves convenience, and greatly improves system performance.

5.2 Sensor Network

Wireless sensor networks offer a high degree of flexibility, including self-organizing, fast cabling, and intelligent processing, while dramatically reducing wiring costs. Wireless sensor network nodes are generally embedded in the device to convert device data and wireless data. The wireless sensor network node has a wireless relay function and constitutes a multi-hop Mesh network. The wireless access point AP on the primary controller implements aggregation of data of the wireless sensor network node.

5.3 Introduction to 4G Module

UNV-SIM7600CE V1.2 is a high-performance industrial 4G development board launched by Global Eagle. Support mobile, China Unicom, Telecom 4G, 3G and 2G. Rich in function interface, especially suitable for SMS, MMS, 4G wireless transmission of data in various fields. This module can be controlled by AT commands. In the system, you first need to send the AT to initialize the 4G module, then send AT+CREG=1 to register the network, and use AT+COPS to confirm the registration information. In the short message module processing, use AT+CMGF to select the short message format, use AT+CSCS to select the character set, use AT+CSCA SMS to set the SMS service center address, use AT+CSMP to set the text mode parameter, AT+CNMI will set the new message. Pass to TE. At the same time, the judgment is made in the code, and if the return prompt does not match the normal prompt, an error message is returned.

5.4 Function module call

The main controller has the same wireless communication module as the wireless sensor network node device, and also connects the 4G module through the serial port, which is the aggregation node of the wireless sensor network, and also the gateway node between the wireless sensor network and the 4G network. The wireless aggregation-4G main controller uses the ARM processor and the wireless communication module in the 2.4 GHz band. In addition, the UNV-SIM7600CE module and
the user card (USIM) support 4G access. The node device sensing information in the wireless sensor network is transmitted to the wireless convergence-4G main controller through the wireless ad hoc network. The main controller encrypts the sensing data of the wireless sensor network node device and sends it to the cloud server, and forwards commands for querying, controlling, and managing the sensing node to the wireless sensor network.

The main controller needs to support the three services of listening, requesting and configuring concurrently [6], so three modules are designed to satisfy different function calls. The listening service is a periodic event. The listening module sends a broadcast request every 300ms, and all the devices that receive the request reply to its working state; the requesting service is an emergency, and the main controller makes a sudden request to a device, and the device responds to it. The detailed working status of the user, the configuration service is also an emergency, the main controller bursts the configuration command to a certain device, and the device modifies the configuration and replies to the main controller.

6. Conclusion

For remote security control systems, the constant integration of various wireless communication technologies and network structures makes the system face greater network security threats. At present, there are relatively few studies on the security of remote control systems. Generally, they are commonly used in the smart home field. The devices that receive control commands are relatively single. The device status and control commands are usually transmitted through the public network. It is easy for hackers to obtain device rights and use them. Illegal purpose. In remote control systems that use cryptographic techniques for protection, their security generally relies on international algorithms for protection, which increases the risk of information systems being attacked.

This paper studies Android platform software development, embedded system development and cloud server design, and analyzes the existing remote control system problems. A security scheme for 4G access is proposed, and a 4G-based remote security control system is designed. Using the security architecture for 4G access proposed in this paper, the integrated sensor network technologies such as mobile vehicle network, RFID system and ZigBee networking, on the basis of this, the remote security control across the terminal platform is studied. Because wireless sensor networks sense nodes with simple functions and low carrying capacity, they cannot have complex security protection capabilities [7]. In the next step, research on the security protection mechanism of the wireless sensor network is also needed.

References
[1] http://news.west.cn/42658.html
[2] GM/T 0003-2012, SM2 elliptic curve public key cryptography algorithm [S].
[3] Liang Guocheng. Design and implementation of Android mobile learning system [D]. University of Electronic Science and Technology, 2015.
[4] He Teng. Discussion on cloud storage technology and application [A]. Tianjin Institute of Electronics. The 29th China (Tianjin) 2015 'Proceedings of IT, Network, Information Technology, Electronics, Instrumentation Innovation Conference [C]. Tianjin Institute of Electronics;, 2015: 4.
[5] Xie Huajing. Research on SM2 Encryption Technology in Embedded System Communication [D]. Suzhou University, 2014.
[6] YANG Dong, MA Jian, ZHANG Hongke. Smart Collaborative Industrial Wireless Sensor
[7] Sun Onqiang. Design and Implementation of IoT Secure Access Gateway [A]. Computer Security Professional Committee of China Computer Society. Proceedings of the 26th National Computer Security Academic Exchange Conference [C]. Computer Security Major of China Computer Society Committee: 2011: 3.